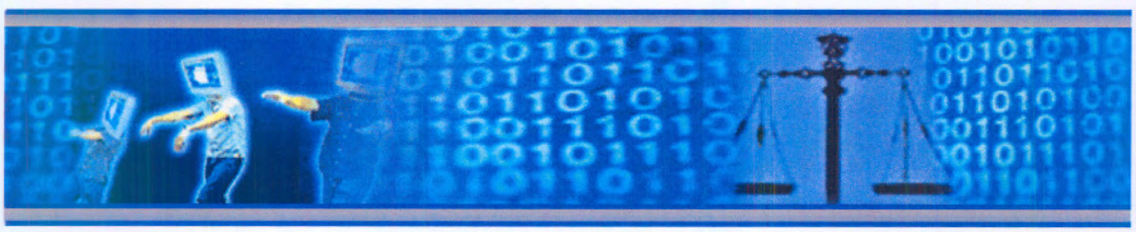
SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION OF ELECTRONIC EVIDENCE



SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION OF ELECTRONIC EVIDENCE

by

ANNAMART
NIEMAN

submitted in accordance with the requirements for the degree
DOCTOR OF LAWS

at the

NORTH-WEST UNIVERSITY

Promoter:	Prof C Rautenbach
Assistant Promoter:	Prof MM Watney

May 2006

Potchefstroom

The research for this thesis was concluded on 30 April 2006. Only exceptionally important literature since this date has been included.

SOLI DEO GLORIA

A Nieman

ACKNOWLEDGEMENTS

My husband	For lifting me onto your shoulders in pursuit of one of our dreams; for loving me as much as I know you do and for letting me love you as much as you know I do; and for being the single most important person in my life: my God-sent gift.
My father and mother	I am deeply indebted to you for a lifetime of unselfish giving and, not least, for giving me backbone and wings – I am proud to be a child of two truly exceptional "walking tall" individuals.
My promoters	Professors Christa Rautenbach and Murdoch Watney – in the final analysis, this all-female effort was propelled by the Mothership-*Sputnik* combo. Without you, the realisation of this ideal would simply not have been possible – I have been both blessed and enriched by our association.
AnnaMartha (The Original)	For clearing the way, cleaning up afterwards and keeping everything together (including the overall management of the sources, proofreading and tidying up the footnotes and bibliography) – essentially, for being not only the official "team-leader" but also the chief, cook and bottlewasher-*grande* of this project; an awesomely strong woman in real life; and for being the greatest cheerleader in my life.
Dorette	For constituting "the (whole of the) team"; for being such an all-encompassing resourceful bonus and for subscribing to this project (and my family) with endless commitment and incredible lightness of being.
Christine	"A capable, intelligent and virtuous woman ..." [Prov 31:10] – the most dedicated and inspired information specialist in the industry! Thank you also to all her colleagues at the Ferdinand Postma library who had to lend her a frequent helping hand and/or sympathetic ear (I imagine).
Ingrid	For coaching us through the rush hour(s); for amplifying your contribution to humankind and for being a dear friend.
Hannes and Coba	For being my prayer and support groupies in the back office (as always).

Anton	For patience, humour and important finishing touches embedded in the metatags of this thesis.
Idette	For painstaking editing and grace in the heat of the beat.
Online Intelligence	For financial and technical support and for having and keeping the F/faith.
Magnifying Solutions (Charl)	For meticulous IT support and for showing a sincere interest.
The CSIR	For financial support. A special word of thanks to Cobus and Barend for their votes of confidence.
North-West University	For financial support. The remarkable absence of bureaucracy has been overwhelmingly welcoming.
Deloitte	Peter, Corné and Jaco – for hearing me out and for letting me be.
Liezel	For your very precious presence in my life and for being the greatest girl friend anybody can wish for – I look forward to strip poker "under the boardwalk" when we get to the old age home.
My family	Anri – for being my daughter in the bravest way we both know how (and for being a supercool teenager/ young woman); Herman, Susan, Deon and the boys – for being my loved ones and not in-laws; Nellie, Maxie, Flora, Coba, Helena – for being my beautiful "sistas" and for being the ones that I *count on*; Hannes – for being a brother that I am so very proud of; the husbands in the family – for hanging in there (...); all my godchildren and the *UnterarmClub* (veterans and aspirants inclusive) – we will see each other soon ...
Jan and Dewald	For not only being my partners, but also for being my very dear and special friends – that "5%" surely was the best investment I ever made.
Torie	For endless philosophical cups of coffee, a cherished friendship and "walk for my life".

Jacques	For sharing your passion(s) with me – I look forward to a journey together.
Louise	For your invaluable contribution to my life.
Wilma, Gerhard, Zaais, Estie, Willie, Corné, Willem, John, Maritha, AJ, Magda, Annalize, Elmari, Marika, Daleen and Christiaan	For your treasured support in this effort and in my life.
The techies in my life	For entertaining my endless query strings and keyword searches and for spicing up my professional life.
My (former) colleagues in the DSO/NPA/SAPS	For keeping the fire aflame.

ABBREVIATIONS

A	
APPN	Advanced Peer-to-Peer Networking
ASCII	American Standard Code of Information Exchange
ATM	Asynchronous Transfer Mode
B	
BCCs	Blind Carbon Copies
BIOS	Basic Input and Output System
Bit	Binary Digit
C	
CCIPS	Computer Crime and Intellectual Property Section
CD	Compact Disk
CD ROM	Compact Disk Read-Only Memory
CDF	Microsoft Channel Definition Format
CDPC	European Committee on Crime Problems
CD-R	Compact Disc-Recordable
CD-RW	Compact Disk-Rewritable
CERD	International Convention on the Elimination of All Forms of Racial Discrimination of 1965
CERT	Computer Emergency Readiness Team
CMOS	Complementary Metal-Oxide Semiconductor Memory
COM	Computer Output Microfilm
CPU	Central Processing Unit
CRCs	Cyclic Redundancy Checks
D	
DHCP	Dynamic Host Configuration Protocol
DNA	Deoxyribonucleic Acid
DNS	Domain Name System
DOS	Disk Operating System
DPP	Director of Public Prosecutions
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Line
DSN	Data Source Name
DSO	Directorate of Special Operations
DVD	Digital Versatile/Video Disks

DVD+RW	Digital Versatile/Video Disks Rewritable
DVD-R	Digital Versatile/Video Recordable
DVD-ROM	Digital Versatile/Video Disc – Read-Only Memory
DVI	Digital Video Interface
E	
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950
ECPA	Electronic Communications Privacy Act of 1986
ECT Bill	Electronic Communications and Transactions Bill
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIDE Controller	Enhanced Integrated Drive Electronics Controller
Email	Electronic Mail
EMS	Enhanced Messaging Service
EPROM	Erasable Programmable Read-Only Memory
ETS No	European Treaty Series Number
EXIF	Exchangeable Image File Format
F	
FBI	Federal Bureau of Investigation
FDD	Floppy Disk Drive
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
G	
G8	Group of Eight Nations
GB	Gigabyte
GUI	Graphical User Interface
GSM	Global System for Mobile Communication
H	
HDC	Hard Disk Controller
HDD	Hard Disk Drive
Hex	Hexadecimal
HomePLC	Home Powerline Network
HomeRF	Home Radio Frequency Network
HRA	Human Rights Act of 1998
HTTP	Hypertext Transfer Protocol
I	

ICASA	Independent Communications Authority of South Africa
ID	Identification
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
Interpol	International Criminal Police Organisation
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
ITU-T	International Telecommunications Union, Telecommunications Standard Sector
J	
JPEG	Joint Photographic Experts Group
K	
L	
LAN	Local Area Network
M	
MAC Address	Media Access Control Address
MAN	Metropolitan Area Network
MD5	Message Digest 5
MG	Megabyte
MMS	Multimedia Messaging Service
MO	Magnetico-Optical
N	
NAS	Network-Attached Storage
NICs	Network Interface Cards
NSF	National Science Foundation
NTI	New Technology Incorporated
O	
OECD	Organisation for Economic Cooperation and Development
OSI	Open Systems Interconnect
P	
P2P	Peer-to-peer
PACE	Police and Criminal Evidence Act of 1984

PC	Personal Computer
PC-CY	Committee of Experts on Crime in Cyberspace
PCMCIA	Personal Computer Memory Card International Association
PC-RX	Committee of Experts on the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems
PDA	Personal Digital Assistant
POP	Post Office Protocol
PROM	Programmable Read-Only Memory
PSTN	Public-Switched Telephone Network
Q	
R	
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RICPCIA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
RIPA	Regulation of Investigatory Powers Act of 2000
ROM	Read-Only Memory
ROT-13 Decoders	Rotate-13 Decoders
S	
SACJ	South African Journal of Criminal Justice
SADC Protocol	South African Development Community Protocol
SAJCJ	South African Journal for Criminal Justice
SALC	South African Law Reform Commission
SALJ	South African Law Journal
SAN	Storage Area Network
SANAB	South African Narcotics Bureau
SAP	South African Police
SAPL	SA Publiekreg/SA Public law
SAPS	South African Police Service
SARPCCO	Southern African Regional Police Chiefs Cooperation Organisation
SCSI	Small Computer System Interface
SGML	Standard Generalised Markup Language
SHA 1	Secure Hash Algorithm 1
SIM	Subscriber Identity Module

SMS	Short Message Service
SPA	Software Publisher's Association
SRAM	Static Random Access Memory
T	
TB	Terrabyte
TCP/IP	Transmission Control Protocol/ Internet Protocol
THRHR	Journal of Contemporary Roman-Dutch Law/Tydskrif vir die Hedendaags Romeins-Hollandse Reg
TIFF	Tagged Image File Format
TSAR	Tydskrif vir Suid-Afrikaanse Reg/Journal for South African Law
U	
UNCITRAL	United Nations Commission on International Trade Law
UNTOC	United Nations Convention Against Transnational Organised Crime of 2000
URL	Uniform Resource Locator
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools, Required to Intercept and Obstruct Terrorism of 2001
USB	Universal Serial Bus
V	
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W	
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WWW	World Wide Web
X	
XML	Extensible Markup Language
3GPP	Third Generation Partnership Project

ABSTRACT

Criminals are becoming increasingly involved in computing activity and connectivity, but practitioners in the criminal justice field do not seem to be keeping pace with crime in a computing context.

Being comfortable with the technology that underpins the Information Age is a non-negotiable skill for those who have to unravel and bring twenty-first century crimes to book. Chapter two of this study therefore sought to serve two purposes. The first aim was to acquaint the reader with the exceedingly complex technologies involved in computers and networks. The second aim was to clarify the technical context and terminology typical of the collection of electronic evidence.

South Africa signed the Cybercrime Convention in November 2001. At present, the Cybercrime Convention is the only existing internationally accepted benchmark, *inter alia*, for the procedural powers aimed at the collection of electronic evidence. The main objective of this study was to consider whether the South African search and seizure, production and preservation devices need to be augmented and/or aligned so as to be on par with the devices proposed in the Cybercrime Convention. This objective was served in two ways. Firstly, an exposition of the requirements, scope, conditions and safeguards of the domestic and transborder search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention was provided in chapter three of this study. Secondly, an exposition of the domestic and transborder international search and seizure, production and preservation devices available in the current South African legislative framework was given in chapter four of this study. A comparative analysis was done between the South African catalogue of criminal procedural search and seizure, production and preservation devices compared to those set out in the Cybercrime Convention. Where any alignment or augmentation of the South African devices was found to be necessary, this study identified these intervention areas. The findings and recommendations based on this comparative analysis were set out in chapter seven of this study.

In considering any alignments and/or augmentations required in respect of the South African domestic search and seizure, production and preservation mechanisms, the application of the equivalent mechanisms directed at electronic evidence used in the United States of America and England were investigated in chapters five and six respectively. The lessons learned were also referred to in chapter seven of this study.

OPSOMMING

Misdadigers raak deesdae toenemend betrokke by rekenaaraktiwiteit en verbindings ("*connectivity*"), maar dit lyk of praktisyns in die strafregtelike veld nie kan tred hou met misdaad in die rekenaarkonteks nie.

Om gemaklik te kan omgaan met die tegnologie wat die Inligtingsera onderlê, is 'n ononderhandelbare vaardigheid vir diegene wat misdade in die een-en-twintigste eeu moet oplos en sodanige misdadigers aan die pen moet laat ry. Die doel met hoofstuk twee van hierdie ondersoek was daarom tweeledig van aard. Die eerste oogmerk was om die toenemend ingewikkelde tegnologieë betrokke by rekenaars en netwerke aan die leser voor te stel. Die tweede oogmerk was om die tegniese konteks onderliggend tot en die tekenende terminologie insake die insameling van elektroniese getuienis duidelik te maak.

Suid-Afrika het die Kubermisdaadkonvensie in November 2001 onderteken. Op die oomblik is die Kubermisdaadkonvensie die enigste bestaande internasionaal-aanvaarde hoogtemerk ("*benchmark*") vir, onder andere, die proseduriële magte gerig op die insameling van elektroniese getuienis. Die hoofdoel van hierdie navorsing was om te ondersoek of the Suid-Afrikaanse deursoekings- en vistenterings-, produksie- en preserveringsmeganismes aangevul en/of aangepas moet word om gelykstaande te wees aan die meganismes wat in die Kubermisdaadkonvensie voorgestel word. Hierdie doel is op twee wyses nagestreef. Ten eerste is daar in hoofstuk drie van hierdie studie 'n uiteensetting gegee van die voorskrifte, omvang, voorwaardes en veiligheidswaarborge van die nasionale en internasionale deursoekings- en vistenterings-, produksie- en preserverings-meganismes soos vervat in die Kubermisdaadkonvensie. In the tweede plek is daar in hoofstuk vier van hierdie studie 'n uiteensetting gegee van die nasionale en internasionale deursoekings- en vistenterings-, produksie- en preserveringsmagte wat tans in die Suid-Afrikaanse regsraamwerk beskikbaar is. 'n Vergelykende analise is gedoen tussen die Suid-Afrikaanse stel strafregtelike deursoekings- en vistenterings-, produksie en preserveringsmeganismes en die meganismes wat in die Kubermisdaadkonvensie voorgestel word. Hierdie ondersoek het enige aanvullings of aanpassings tot die Suid-Afrikaans meganismes wat nodig blyk te wees, geïdentifiseer. Die bevindings en aanbevelings wat op hierdie vergelykende analise gebaseer is, word weergegee in hoofstuk sewe van hierdie studie.

Ter oorweging van die aanvullings en aanpassings wat in die Suid-Afrikaanse nasionale deursoekings- en vistenterings-, produksie- en preserveringsmeganismes benodig mag word, is die aanwending van soortgelyke meganismes vir die insameling van elektroniese getuienis in die Verenigde State van Amerika en Engeland ook ondersoek, soos onderskeidelik uiteengesit in hoofstukke vyf en ses. Die lesse wat hieruit geleer is, is insgelyks in hoofstuk sewe vervat.

NOPOLO*

Disinyi ka bontsi di amega mo go diriseng le mo kgolaganong ka "computer", mme bao ba dirang ka tsa bosinyi mo lefapheng la bosiamisi ga go bonale ba kgona go lepalepana le bosinyi boo bo dirwang ka tiriso ya "computer".

"Technology" eo e kgotsofatsang eo kitso ya ga jaana e ikaegileng mo go yona e siame, mme fela bothata ke bokgoni mo go bao ba tshwanetseng go rarabolola le go sekisetsa bosinyi ba ngwagakgolo a mabedi le bongwe ono.

Afrika-Borwa e saenetse kopano ya 'Cybercrime" ka Ngwanatsele 2001. Ga jaana, kopano ya "Cybercrime" ke yona fela, lefatshe ka bophara, eo e amogelesegang, mo gare ga tse dingwe, matla a tsamaiso a a kobileng go kokwanya bopaki ba elektroniki. Maikaelelo magolo a thuto eno e ne e le go sekaseka fa didiriswa tsa Afrika-Borwa tsa go phuruphutsa le go thopa, tsweletso le pabalelo di tlhoka go ka oketswa le go/kgotsa go tsepamisiwa gore di nne jaaka didiriswa tseo di sisintsweng mo kopanong ya "Cybercrime". Maikaelelo ano a dirilwe ka mekgwa e le mebedi. Mokgwa wa ntlha ke go supa ditlhokego, sebaka, maemo le tshireletsego ya phuruphutso le thopo, tsweletso le pabalelo mo gae le ka kwa ntle ga melelwane jaaka go sisintswe kwa kopanong ya "Cybercrime" mme e tlhagisitswe mo kgaolong ya boraro ya thuto eno. Mokgwa wa bobedi, ke go bontsha didirisiwa tsa mo gae le tsa kwa ntle tsa phuruphutso le thopo, tsweletso le pabalelo tseo di leng teng ga jaana mo motlhaleng wa molao o filweng mo kgaolong yo bone ya thuto eno.

Mokololo wa papiso o ne wa dirwa magareng a lenaane la tsamaiso ya bosingi ya Afrika-Borwa le didiriswa tsa phuruphutso le thopo, tsweletso le pabalelo le tseo di tlhagisitsweng kwa kopanong ya "Cybercrime". Fa go neng go tlhokega tsepamiso kgotsa koketso ya didiriswa tsa Afrika- Borwa, thuto eno e lemogile mafelo ao a ntseng jaalo a tseraganyo.

Mo go tlhokomeleng epe ya ditsepamiso le kgotsa dikoketso tse di tlhokegang mabapi le phuruphutso tso le thopo, tsweletso le mekgwa ya pabalelo ya selegae tsa Afrika- Borwa, tiriso ya mekgwa e e tsamaelanang e e kobisitsweng go bopaki ba elektroniki bo bo dirisiwang kwa United States le Engelane e ne ya batlisisiwa mo kgaolong ya boplhano le ya borataro ka tatellano ya tsona. Dithuto tseo motho a di ithutileng go bolelwa ka tsona mo kgaolong ya bosupa ya thuto eno.

* Translated by Mr MS Moloi (Supervisor Interpreter at the High Court of Transvaal Provincial Division).

CONTENTS

ACKNOWLEDGEMENTS ..... (v)

ABBREVIATIONS ..... (vii)

ABSTRACT ..... (x)

OPSOMMING ..... (xi)

NOPOLO ..... (xii)

1. CHAPTER 1: INTRODUCTION 1

1.1 Background bits and bytes 2
1.1.1 Search and seizure 16
1.1.2 Production and preservation 17
1.2 Method in the madness 19
1.3 Methodology 19
1.4 Moral of the story: unplugged 23

2. CHAPTER 2: A TECHNICAL CONTEXTUALISATION 25

2.1 Introduction 26
2.2 The object of search and seizure, production and preservation 26
2.2.1 Computer data 26
2.2.1.1 Communications data: a special type of computer data 31
2.3 The objective of search and seizure, production and preservation 36
2.3.1 Electronic evidence 36
2.3.1.1 Mining forensic gold in search of electronic evidence 38
2.3.1.2 Computer forensics: a means to an end 41
2.3.1.3 Anti-Forensics: another one bytes the rust 45
2.4 Caught in the act: interception and monitoring, search and seizure, production and preservation 48
2.4.1 Interception/collection and monitoring 51
2.4.2 Search and seizure 53
2.4.3 Production 56
2.4.4 Preservation 56
2.5 Penetrating the House of Binary: computers of all shapes and sizes 58
2.5.1 Computer system 58
2.5.1.1 Computer hardware 59
2.5.1.2 Computer software 67
2.5.1.3 Categories of computer systems 70
2.6 Categories of computing environments – who moved my bit? 72

2.6.1 Stand-alone computing environments 72
2.6.2 Networked computing environments 73
2.6.2.1 Theoretical network reference models 76
2.6.2.2 Network control strategies 78
2.6.2.3 Network topologies 82
2.6 Categories of computing environments – who moved my bit? (continued) 82
2.6.2.4 Network transmission media 82
2.6.2.5 Categories of computer networks 83
2.6.3 The biggest WAN of all – the Internet and the World Wide Web 86
2.7 Brouter to chapter 7 94

3. CHAPTER 3: SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION @ THE CYBERCRIME CONVENTION 96

3.1 BIOS bits and bytes 99
3.2 The Cybercrime Convention 99
3.2.1 Historical background 101
3.2.2 Aims 101
3.2.3 Status 103
3.2.4 Interrelationship 105
3.2.5 Declarations and reservations 106
3.2.6 Amendments, settlement of disputes and consultations 133
3.3 Domestic search and seizure in computing environments 108
3.3.1 Requirements 108
3.3.1.1 Equivalence 108
3.3.1.2 Comprehensive legal authorisation to search or access 109
3.3.1.3 Extension of the search or access 109
3.3.1.4 Comprehensive legal authorisation to seize or similarly secure 110
3.3.1.5 Coerced cooperation 110
3.3.2 Scope 111
3.3.2.1 Specific criminal investigations or proceedings 112
3.3.2.2 Categories of crimes 112
3.3.2.3 Stored computer data 112
3.3.2.4 Jurisdiction 112
3.3.3 Conditions and safeguards 114
3.3.3.1 Domestic conditions and safeguards 115
3.3.3.2 Minimum international safeguards 115
3.3.3.3 Supervision by competent authorities 116
3.3.3.4 Proportionality 117
3.3.3.5 Third parties 117
3.4 Transborder search and seizure in computing environments 119
3.4.1 Requirements 119
3.4.1.1 Search and seizure specific 119
3.4.1.2 General mutual assistance requirements 121
3.4.1.3 Mutual assistance requirements in the absence of applicable international agreements 123
3.4.2 Scope 126
3.4.2.1 Widest extent possible 126
3.4.2.2 Categories of crime 126
3.4.2.3 Stored computer data 127

3.4.2.4 Jurisdiction 127
3.4.3 Conditions and safeguards 127
3.4.3.1 Domestic fundamental requirements satisfied 127
3.4.3.2 Dual criminality 128
3.4.3.3 Prejudice to the sovereignty of the state and political offences 128
3.4.3.4 Prejudice to investigations or proceedings 128
3.4.3.5 Conditions in the discretion of the requested party 128
3.4.3.6 Confidentiality and use limitations 129
3.4.3.7 Data protection 130

3.5.1 Requirements for production orders 131
3.5.1.1 Domestic production orders 131
3.5.2 Scope 131
3.5.2.1 Specific criminal investigations or proceedings 131
3.5.2.2 Categories of crimes 132
3.5.2.3 Stored computer data 132
3.5.2.4 Jurisdiction 133
3.5.3 Conditions and safeguards 133
3.5.3.1 Domestic conditions and safeguards 133
3.5.3.2 Minimum international safeguards 133
3.5.3.3 Supervision by competent authorities 133
3.5.3.4 Proportionality 133
3.5.3.5 Third parties 133
3.5.3.6 Privileged categories of subscriber information 134
3.5.3.7 Confidentiality 134

3.6.1 Requirements 134
3.6.1.1 General mutual assistance requirements 135
3.6.1.2 Mutual assistance requirements in the absence of applicable international agreements 135
3.6.2 Scope 135
3.6.2.1 Widest possible extent 135
3.6.2.2 Categories of crime 136
3.6.2.3 Any computer data 136
3.6.2.4 Jurisdiction 136
3.6.3 Conditions and safeguards 136
3.6.3.1 Confidentiality and use limitations 136
3.6.3.2 Domestic fundamental requirements satisfied 137
3.6.3.3 Dual criminality 137
3.6.3.4 Conditions in the discretion of the requested party 137
3.6.3.5 Prejudice to the sovereignty of the state and political offences 137
3.6.3.6 Prejudice to investigations or proceedings 137
3.6.3.7 Data protection 137

3.7 Domestic preservation and partial disclosure in computing environments
3.7.1 Requirements 138
3.7.1.1 Domestic expedited preservation of stored computer data 138
3.7.1.2 Domestic expedited preservation and partial disclosure of traffic data 139
3.7.2 Scope 141
3.7.2.1 Specific criminal investigations or proceedings 141
3.7.2.2 Categories of crime 142

3.7.2.3 Stored computer data 142
3.7.2.4 Jurisdiction 143
3.7.3 Conditions and safeguards 143
3.7.3.1 Domestic conditions and safeguards 143
3.7.3.2 Minimum international safeguards 143
3.7.3.3 Supervision by competent authorities 144
3.7.3.4 Proportionality 144
3.7.3.5 Third parties 144
3.7.3.6 Confidentiality 144
3.8 Transborder preservation and partial disclosure orders in computing environments 144
3.8.1 Requirements 145
3.8.1.1 Transborder expedited preservation of stored computer data 145
3.8.1.2 Transborder expedited disclosure of preserved traffic data 146
3.8.1.3 General mutual assistance requirements 146
3.8.1.4 Mutual assistance requirements in the absence of applicable international agreements 147
3.8.2 Scope 147
3.8.2.1 Widest extent possible 147
3.8.2.2 Categories of crime 147
3.8.2.3 Stored computer data 147
3.8.2.4 Jurisdiction 147
3.8.3 Conditions and safeguards 148
3.8.3.1 Domestic fundamental requirements satisfied 148
3.8.3.2 Dual criminality 148
3.8.3.3 Prejudice to the sovereignty of the state and political offences 149
3.8.3.4 Prejudice to investigations or proceedings 149
3.8.3.5 Conditions in the discretion of the requested party 149
3.8.3.6 Confidentiality and use limitations 150
3.8.3.7 Data protection 150
3.9 Brouter to chapter 4 150

4. CHAPTER 4: SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION @ SOUTH AFRICA 153

4.1 BIOS bits and bytes 155
4.2 Domestic search and seizure in computing environments 155
4.2.1 Root domain 156
4.2.2 Requirements 156
4.2.2.1 Articles susceptible to search and seizure 159
4.2.2.2 Domestic search and seizure with a warrant 165
4.2.2.3 Domestic search and seizure without a warrant 172
4.2.3 Scope 172
4.2.3.1 Particularity and specificity 177
4.2.3.2 Categories of crimes 177
4.2.3.3 Use of force in order to conduct a search 178
4.2.3.4 Jurisdiction 180
4.2.4 Conditions and safeguards 180
4.2.4.1 Right to privacy 182
4.2.4.2 Reasonable grounds 185
4.2.4.3 Proportionality 186

4.2.4.4 Supervision by competent authorities ... 188
4.2.4.5 Privileged data ... 193
4.2.4.6 Right against self-incrimination ... 196
4.2.4.7 Third parties ... 197
4.2.4.8 Consequences of unlawful action by the authorities ... 198
4.2.4.9 Propriety ... 198
4.2.4.10 Confidentiality ... 227

4.3.1 Requirements for transborder search and seizure ... 199
4.3.1.1 General mutual assistance framework ... 199
4.3.1.2 Foreign requests to South Africa, as the requested state ... 204
4.3.1.3 Requests from South Africa, as the requesting state ... 206
4.3.1.4 24 Hours a day, 7 days a week network ... 208
4.3.1.5 Search and seizure specific mutual assistance ... 208
4.3.2 Scope ... 211
4.3.2.1 Widest extent possible ... 211
4.3.2.2 Categories of crime ... 212
4.3.2.3 Jurisdiction ... 212
4.3.3 Conditions and safeguards ... 212
4.3.3.1 Dual criminality ... 212
4.3.3.2 Grounds for refusing a mutual legal assistance request ... 213
4.3.3.3 Costs ... 214
4.3.3.4 Admissibility and authentication ... 214

4.4.1 Background ... 215
4.4.2 Requirements ... 216
4.4.2.1 Section 205 of the Criminal Procedure Act ... 216
4.4.2.2 Archived communication-related directions ... 218
4.4.2.3 Sections 39(3) and 40(3) of the RICPCIA ... 222
4.4.3 Scope ... 223
4.4.3.1 Specific criminal investigations or proceedings ... 223
4.4.3.2 Categories of crimes ... 223
4.4.3.3 Stored computer data ... 224
4.4.3.4 Jurisdiction ... 225
4.4.4 Conditions and safeguards ... 225
4.4.4.1 Supervision by competent authorities ... 225
4.4.4.2 Proportionality ... 227
4.4.4.3 Third parties ... 229
4.4.4.4 Privileged categories of information ... 231
4.4.4.5 Confidentiality ... 234
4.4.4.6 Discretionary conditions ... 236
4.4.4.7 Consequences of unlawful action taken ... 236

4.5 Transborder search and seizure in cloud computing environments ...
4.5.1 Domestic search and seizure and production provisional measures in computing environments ...
4.5.2 Transborder search and seizure and disclosure provisional measures in computing environments ...
4.5.3 Practical problems ...

5. CHAPTER 5: A SNAPSHOT OF TROUBLESHOOTING @ THE USA 243

5.1 BIOS bits and bytes 246

5.2 Domestic search and seizure of e-evidence 246

5.2.1 Root domain 247
5.2.2 Right to privacy 251
5.2.3 Search and seizure of e-evidence with a warrant 251
5.2.3.1 Particularity and specificity 256
5.2.3.2 Judicial supervision 257
5.2.3.3 Probable cause requirement 259
5.2.3.4 The quest for an e-evidence search strategy 271
5.2.4 Search and seizure of e-evidence without a warrant 272
5.2.4.1 Warrantless search and seizure doctrines 290

5.3 Domestic production devices 290

5.3.1 Backgound 293
5.3.2 Categories of service providers 293
5.3.2.1 Electronic communication service 294
5.3.2.2 Electronic storage 295
5.3.2.3 Remote computing service 296
5.3.3 Information categories 296
5.3.3.1 Basic subscriber information 297
5.3.3.2 Records or other information pertaining to a customer or subscriber to such a service 297
5.3.3.3 Contents 297
5.3.4 Different production devices 298
5.3.4.1 Compelled disclosure 299
5.3.4.2 Voluntary disclosure 304

5.4 Domestic preservation devices 306

5.4.1 Background 306
5.4.1.1 Section 2703(f) preservation orders 306
5.4.1.2 Section 2705(b) order not to disclose the existence of a warrant, subpoena or court order 307

5.5 Brouter to chapter 6 309

6. CHAPTER 6: A SNAPSHOT OF TROUBLESHOOTING @ ENGLAND 310

6.1 BIOS bits and bytes 310

6.2 Domestic search and seizure of e-evidence 313

6.2.1 Root domain 313
6.2.2 Right to privacy 316
6.2.3 Search and seizure of e-evidence with a warrant 319
6.2.3.1 Search warrant types 320
6.2.3.2 Particularity and specificity 326
6.2.3.3 Judicial supervision 329
6.2.3.4 Reasonable grounds 331
6.2.3.5 In search of an e-evidence strategy 333
6.2.4 Search and seizure of e-evidence without a warrant 340
6.2.4.1 Warrantless search and seizure doctrines 341

6.3 Production devices 355

6.3.1 Background ... 355
6.3.2 Information categories ... 357
6.3.2.1 Legally privileged material ... 357
6.3.2.2 Excluded material ... 359
6.3.2.3 Special procedure material ... 360
6.3.2.4 Communications data ... 360
6.3.2.5 Traffic data ... 361
6.3.2.6 Protected data ... 362
6.3.3 Different production devices ... 362
6.3.3.1 Production order in terms of Schedule 1 to PACE ... 362
6.3.3.2 Authorisations and notices for communications data in terms of RIPA ... 365
6.3.3.3 Notices for protected data in terms of RIPA ... 367
6.4 Preservation and partial disclosure devices ... 374
6.5 Brouter to chapter 7 ... 379

7. CHAPTER 7: SEARCH HITS, CURSORS AND SHUT-DOWN ... 381

7.1 Search engine query ... 382
7.2 Search hits ... 382
7.2.1 A technical contextualisation ... 383
7.2.1.1 Computer data ... 383
7.2.1.2 Electronic evidence ... 384
7.2.1.3 Computer forensics and anti-forensics ... 384
7.2.1.4 Evidence collection mechanisms ... 386
7.2.1.5 Surfing the Third Wave ... 387
7.2.2 Search and seizure, production and preservation @ the Cybercrime Convention ... 387
7.2.2.1 Domestic search and seizure, production and preservation devices ... 387
7.2.2.2 Transborder search and seizure, production and preservation devices ... 391
7.2.2.3 Declarations ... 395
7.2.2.4 Reservations ... 396
7.2.3 South African search and seizure, production and preservation mechanisms compared to the mechanisms proposed by the Cybercrime Convention ... 397
7.2.3.1 Domestic search and seizure, production and preservation devices ... 397
7.2.3.2 Transborder search and seizure, production and preservation devices ... 408
7.2.3.3 Declarations ... 416
7.2.3.4 Reservations ... 416
7.2.4 Search and seizure, production and preservation troubleshooting @ the United States and England ... 417
7.2.4.1 Right to privacy ... 418
7.2.4.2 Unconstitutionally obtained evidence ... 419
7.2.4.3 Domestic search and seizure devices ... 420
7.2.4.4 Domestic production devices ... 424
7.2.4.5 Domestic data preservation devices ... 426
7.3 Cursors ... 427
7.4 Shutdown ... 431

BIBLIOGRAPHY 433

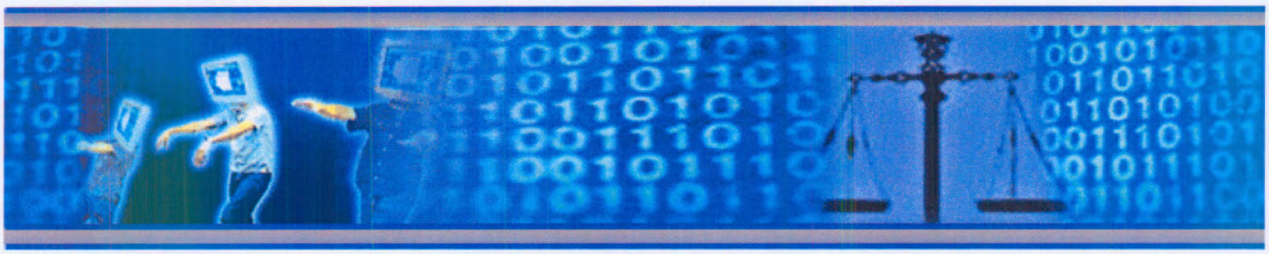
BOOKS AND PERIODICALS 433

CASE LAW 444

STATUTES AND INTERNATIONAL DOCUMENTS 463

INTERNET 471

CHAPTER 1:
INTRODUCTION



1.1 BACKGROUND BITS AND BYTES 2

1.1.1 Search and seizure 16
1.1.2 Production and preservation 17

1.2 METHOD IN THE MADNESS 19

1.3 METHODOLOGY 19

1.4 MORAL OF THE STORY: UNPLUGGED 23

1.1 Background bits and bytes[1]

In 1982, in the most gentlemanly manner possible, *Time Magazine*'s "Man of the Year" gave way to the computer as the "Machine of the Year".[2] It now seems that encircling the globe with high-capacity computer networks, including the Internet, will be one of the great technological feats of the twenty-first century.[3] Computers and computer networks have confirmed the perception that information is a defining feature of our times, arguably the defining feature.[4] There is little doubt that the key modern currency is information, and no longer land, capital or labour.[5]

As crime revolves around currency, criminals are becoming increasingly involved in computing activity and connectivity.[6] The exponential growth of information technology infrastructure such as computer networks and information superhighways not only creates increasing numbers of opportunities for potential offenders, but also an equal number of risks for potential victims.[7] In this context, criminal offences take on a wide variety of guises. These have been labelled, *inter alia*, cybercrime, computer crime, computer-related crime, Internet crime, information

---

1 See paragraph 2.1.1 below for a definition of the small units of binary data called "bits" and "bytes". In this heading, it refers to introductory bits and pieces used to provide a rationale for and to contextualise this research.

2 In that particular year, one of the runners-up also happened to be Margaret Thatcher, which made the term "Man of the Year" award sound noticeably even more politically incorrect. See Rosenblatt 1983 *Time Magazine* 4 and 26.

3 Takach *Computer Law* xvii. Koenig "Meeting Law Enforcement's Responsibilities: Solving the Serious Issues of Today" found on the Internet http://www.neiassocaites.org.seriousissues.pdfspassociates? 8 points out that it took radio 38 years, the computer 16 years, and the Internet a mere 4 years to reach 50 million users. The Internet was, in essence, created as a communications tool. Science fiction writer Bruce Sterling claims that the original idea for the Internet was a "post-apocalypse command grip". The idea was a communications system that could continue to operate even when a major node or hub was destroyed. When a direct route of communication was not available, the system would direct communication traffic around the network via alternative routes. See Sterling "Mondo.184: Bruce Sterling Live at Mondo, Part II" found on the Internet http://www.eff.org.Misc/Publications/William_Gibson/sterling_gibson_nas.speeches 1.

4 Webster *Theories of the Information Society* 215.

5 Information and knowledge are replacing capital and energy as the primary wealth-creating assets just as they, in turn, replaced land and labour 200 years ago. See Van der Merwe *Computers and the Law* 200, Van der Merwe 2003 *THRHR* 33 and Stavrou *Mission Impossible? E-Security in South Africa's Commercial and Financial Sectors* 1.

6 The computer is said to have been around in some form since the abacus (which is known to have existed in 3500 BC in Japan, India and China). It is therefore difficult to determine when the first crime involving a computer actually occurred. It is known, however, that, in 1801, a French textile manufacturer, Joseph Jacquard, designed a forerunner to the computer card that allowed the repetition of a series of steps in the weaving of special fabrics. Jacquard's employees were so concerned about the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage further use of the new technology and induced the commitment of one of the first documented computer-related crimes. See Mobrien "Computer Crime" found on the Internet http://www.mobrien.com/computer_crime1.htm paragraph 22. Contemporary surveys and statistics in respect of criminal involvement in the computing context abound. Examples include the CSO, Carnegie Mellon and CERT® Coordination Center "2004 *e*-Crime Watch™ Survey" found on the Internet http://www.csoonline.com/releases/ecrimewatch04.pdf; Computer Security Institute "2005 CSI/FBI Computer Crime and Security Survey" found on the Internet http://www.p4performance.com/pdfs/whitepapers/FBI2005.pdf; Aus CERT "2006 Australian Computer Crime and Security Survey" found in the Internet http://www.auscert.org.au/images/ACCSS2006.pdf; Rantala 2004 *NCJ*; Home Office "Fraud and Technology Crimes: Findings from the 2003/2004 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources" found on the Internet http://www.homeoffice.gov.uk /rds/pdfs06/rdsolr0906.pdf; KPMG "2002 Global Information Security Survey" found on the Internet http://www.kpmg.com/microsite/informationsecurity/pdf/giss.pdf; and Ernst & Young "Global Information Security Survey 2003" found on the Internet http://www.security management.com/library/EY_Survey1103.pdf. More often than not, this information is conflicting, and it is not expanded upon here, as the body of information in this regard changes continuously. Suffice it to say that criminals are indeed active in computing contexts.

7 Moore *Search and Seizure of Digital Evidence* 1.

technology crime, high-tech crime and *e*-crime.[8] This phenomenon has only recently begun to receive the attention it warrants.

Advances in technology and the ease of global travel have made the world a "global village". This trend has had a dramatic impact on many aspects of life and society; and law enforcement is no exception.[9] The shift in the focus of crime from physical objects to intangibles, targeted by anonymous or pseudonymous individuals, has and will continue to have a staggering sociological, psychological, political and economic impact on society.[10] The spread of computer technology into almost all areas of life, as well as the interconnection of computers via international computer networks, has made computer crime more diverse, more dangerous, more international and more challenging to fight than its physical counterparts, where such counterparts exist. In addition, the growing use of computers renders the successful investigation and prosecution of even traditional crimes all the more dependent on evidence stored or processed by means of modern information technology.[11] The ubiquity of the Internet and the connectivity of virtually every workstation to this global community have ramifications that have yet to be worked out. The globalisation of cybercrime challenges and impedes traditional investigative procedures in several ways.[12]

Cybercrime does not require physical proximity between the victim and the perpetrator for the consummation of the offense. Cybercrime in the virtual "click-and-portal-world" is also unbounded, in that the victim and the perpetrator can be in different cities, states, or even countries. By contrast, the scale of "brick-and-mortar" crime is limited, with a tendency to one-on-one crime that involves one perpetrator and one victim. One-on-one victimisation is not typical of cybercrime, because, unlike real-world crime, it can be automated. With automation, perpetrators can commit thousands of crimes quickly and with little effort, and one-to-many victimisation could be seen as the default assumption of cybercrime.[13]

---

8 There is no consensus on the correct jargon, and the debate continues. See, for example, Van der Merwe *Computers and the Law* 166; Van der Merwe *Computers and the Law* (2nd ed) 187; Van der Merwe 2003 *THRHR* 34; Watney 2003 *TSAR* 56; Wasik *Crime and the Computer* 1991; Mobrien "Computer Crime" found on the Internet http://www.mobrien.com/computer crime1.htm paragraph 22-26; Collier *Criminal Law and the Internet* 320-321; Sommer 1993 *Computer Fraud & Security Bulletin* 10; Brenner 2005 *International Journal of Communications Law & Policy* 5-7; and Gordon *Internet Criminal Law* 423-424. For the purposes of this thesis, the terms "cybercrime", "computer crime", "computer-related crime", "information technology crime", "Internet crime", "high-tech crime" and "*e*-crime" are used interchangeably. On balance, the collection of electronic evidence from computing environments, by means of the legal mechanisms of search and seizure, production and preservation, constitutes the real focal point of this research ("electronic evidence" is defined in paragraph 2.3.1 below; the terms "search and seizure", "production" and "preservation" are discussed in paragraphs 2.4.2, 2.4.3 and 2.4.4 respectively).

9 Proust 2003 *SACJ* 295.

10 Ferrera *et al Cyberlaw Text and Cases* 406.

11 Mobrien "Computer Crime" found on the Internet http://www.mobrien.com/computer_crime1.htm paragraph 146.

12 Four of the most important intervention areas that need attention to enable effective penetration of *e*-crime are inadequate laws to prosecute computer crimes; poor technical investigative ability with regard to locating cybercriminals; insufficient cooperation in the collection and sharing of evidence of the crimes; and lack of resources and trained personnel to investigate and combat high-tech crimes. See Reno "Keynote Address by U.S. Attorney General Janet Reno on High-tech and Compuate (sic) Crime" found on the Internet http://www.usdoj.gov/criminal/cybercrime/agfranc.htm 2.

13 Brenner 2005 *International Journal of Communications Law & Policy* 7-10.

Deterring and punishing cybercriminals requires an international legal framework to investigate and prosecute *e*-crime offences. Law enforcement officers cannot ignore the real-world limits of local, state and national sovereignty and jurisdiction. Obtaining information from foreign countries, especially on an expedited basis, can be a daunting task. This is especially true when the other country is in a different time zone, uses a different language, has different legal rules, or does not have trained experts available.[14] With more than 190 Internet-connected countries in the world, the co-ordination challenges facing any law enforcement effort are tremendous. Even if a foreign legal system does not hamper a local investigation, the "electronic trail" may go cold due to a slow response by foreign law enforcement agencies in providing assistance and co-operation in the investigation of international computer crimes.[15] Any delay in an investigation is critical, as a criminal's trail might, in certain circumstances, end as soon as she[16] disconnects from the Internet.[17] Because everything on the Internet is information, investigators must locate the true source of the communication to connect the cybercrime with a real person in the physical world. The infrastructure of the Internet, however, does not provide a ready mechanism for tracing the "electronic trail" leading from the crime back to the perpetrator. The nature of the technology itself makes tracing the trail difficult.[18] Users can connect to the Internet from anywhere in the world, using old-fashioned telephone lines, wireless phones, cable modems or satellite systems. Each of these telecommunications systems has its own protocols for addressing and routing traffic, which means that tracking information all the way back to the criminal at her computer will require law enforcement officers to be fluent in each of these technical languages.

Academics and practitioners lament the fact that the criminal justice field is simply not keeping pace with crime in the computing context.[19] The "continued mystery surrounding the computer

---

14 Holder "Statement of Eric Holder, Deputy Attorney General of the United States before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary on Internet Denial of Service Attacks and the Federal Response on 29 February 2000" found on the Internet http://www.usdoj.gov/criminal/cybercrime/dag0229.htm 4.

15 Aldesco "Notes and Comments – The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime" found on the Internet http://elr.lls.edu/issues/v23-issue1/aldesco.pdf 88-90.

16 Throughout this study, the pronoun "she" has been used as a conscious choice, in preference to the generic "he" or the clumsy "he/she". This choice resonates with a postmodernist acknowledgement of subjective choices in research, as opposed to a pretence of modernist objectivity. In exposing this ideological petticoat to whoever cares to indulge in reading this footnote, the researcher acknowledges that this choice is a personal statement, open to criticism, and subject to some qualms and a chuckle (also by the maker thereof). The author rests in voicing her desire to make visible women in a field which is often primarily associated with males. It is not meant to imply that all cybercriminals or law enforcement agents are female.

17 Holder "Statement of Eric Holder, Deputy Attorney General of the United States before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary on Internet Denial of Service Attacks and the Federal Response on 29 February 2000" found on the Internet http://www.usdoj.gov/criminal/cybercrime/dag0229.htm 6.

18 Neumann 2000 *Association for Computing Machinery Communications of the ACM New York* 136.

19 Moore *Search and Seizure of Digital Evidence* 1. It is interesting to note, however, that Kent and Ghavalas argue that it is probably fair to say that the approaches to electronic evidence collection and production by law enforcement agencies are much more advanced than those approaches followed in the majority of organisations. This, according to these two authors, stems from the fact that law enforcement agencies have had a head start in the field of computer forensics and have developed and established "very high standards regarding the preservation and presentation of evidence found on digital media". They submit that, in their experience, a large number of organisations do not have any processes or procedures in place for handling events that result in the requirement to produce reliable evidence. Organisations are simply not forensically ready. See Kent and Ghavalas 2005 *Digital Investigation* 239 – 240.

systems environment in general"[20] is precisely what makes computer forensics[21] particularly appealing to some people. However, it has also been said that in the face of the intimidating challenge of unravelling this mystery, it is not surprising that "parents, federal investigators, prosecutors and judges often panic when confronted with something they believe is too complicated to understand".[22] On the basis of the subconscious credo that any sufficiently advanced technology is almost "indistinguishable from magic",[23] the majority of legal and law enforcement practitioners[24] shy away from cultivating an imagination for electronic evil:

> Even if, juristically speaking, we were not accessories to the crime, we are always, thanks to our human nature, potential criminals.... None of us stands outside of humanity's collective shadow. Whether the crime occurred many generations back or happens today, it remains the symptom of a disposition that is always and everywhere present – and one would therefore do well to possess some 'imagination for evil', for only the fool can permanently disregard the conditions of his own nature. In fact, negligence is the best means of making him an instrument of evil.[25]

Society is, moreover, not yet sufficiently aware if how vulnerable it is to cybercrime,[26] and ignorance in cyberspace[27] is not bliss. Its growing dependence on information technology in government and commercial operations has been termed the "Achilles heel of America".[28] This rings equally true for all modern information-based societies. Until the morals of those with digitally-driven deviancies improve, the rest of the net-citizenry will have to abandon their ostrich

---

20 Herold (ed) *The Privacy Papers: Managing Technology, Consumer, Employee, and Legislative Actions* 150.

21 Computer forensics is defined in paragraph 2.3.1.2 below.

22 Hafner *Cyberpunk* 11.

23 Hafner *Cyberpunk* 11.

24 Although many corporate forensic investigators also subscribe to some version of this credo, this research focuses on law enforcement officers. Section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (hereinafter referred to as the RICPCIA) describes a "law enforcement officer" as a member of any of the following: the South African Police Service (hereinafter referred to as the SAPS) established by section 5(1) of the South African Police Service Act 68 of 1995; the Defence Force, referred to in section 199(2) of the Constitution of the Republic of South Africa 108 of 1996 (hereinafter referred to as the Constitution), excluding a member of a visiting force; the Agency and the Service as defined in section 1 of the Intelligence Services Act 38 of 1994; the Directorate of Special Operations referred to in section 1 of the National Prosecuting Authority Act 32 of 1998; or any component of the prosecuting authority designated by the National Director of Public Prosecutions (contemplated in section 179(1) of the Constitution) to specialise in the application of chapter 6 of the Prevention of Organised Crime Act 121 of 1998. For the purposes of this study, the term "law enforcement officer" refers to a member of the SAPS or, in respect of other jurisdictions, a member of the national police force. The terms "law enforcement officers", "law enforcers" and "law enforcement agencies" will have a corresponding meaning.

25 Carl Jung quoted in Moore *Tangled Web* Foreword.

26 Sieber "Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-STUDY" found on the Internet http://www.jura.uni-muenchen.de/sieber/article/article.htm 2.

27 William Gibson coined the term "cyberspace" in his 1984 science fiction novel *Neuromancer* to describe the "original consensual hallucination". Gibson used the word to describe the World Wide Web and/or the Internet, but so far neither of these measures up to what Gibson visualised. The term also refers to the communities that have developed through their common use of such resources. It includes the culture which is developing in such electronically connected communities (such as the social rules of acceptable engagement on the Internet, termed "netiquette"). It may also be used to distinguish the physical world from the digital or computer-based world. See Google "Definitions of Cyberspace on the Web" found on the Internet http://www.google.com/search?hl=en&ie=ISO-8859-1&q=define%3A+cyberspace 1 and 3.

28 Vatis "Statement of Michael A Vatis, Director, National Infrastructure Protection Center & Federal of Investigation on Cybercrime Before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee, Washington, DC, February 29, 2000" found on the Internet http://www.cybercrime.gov/vatis.htm 2.

politics and will have to start spreading the message that a love for computational functionality demands meticulous safe hex:[29]

> The policing of terrestrial space is now very much a pluralistic endeavour. So too is the policing of cyberspace. Responsibilities for the control of computer crime will be similarly shared between agents of the state, information security specialists in the private sector, and individual users. In Cyberspace today, as on terrestrial space two millennia ago, the first line of defence will be self-defence.[30]

The bottom line is that even technophobes must be born again and baptised into the Third Wave,[31] not least law enforcement agents. There is no business like binary business[32] and, nowadays, unless you buy into it, you will be out of business sooner rather than later. You may have to think like a cybercrook to catch one, but there is some solace in the fact that there is no such thing as a born cybercop. Most well-balanced, intelligent people can be trained to investigate *e*-crime. Common sense might prove to be a prerequisite and excessive ego may be a hindrance.[33] Lateral thinking, perspective, tenacity and stamina[34] are all helpful qualities in the make-up of those entrusted with the task of fighting cybercrime.

The first step in this relentless quest is to embrace technology. Sadly, an age-old reliance on tangible evidence, hard fact and an understanding of human motivation has made lawyers members of one of the most technophobic professions on earth:[35]

> One thing lawyers like is certainty. Computers seldom give it. If anything, they show that we live in a universe where uncertainty rules, and if your livelihood depends on your predictability, that's a hard thing to stomach.

Being comfortable with the technology that underpins the computer revolution ushering in the Information Age is absolutely non-negotiable for those who have to investigate twenty-first century crimes and crime scenes. To use an analogy: being stuck in a world where bartering is

---

29 All input to a computer is converted into binary numbers made up of only two digits "0" and "1". Hex is commonly used in the computer world as a shorthand for binary numbers. Binary is a base 2 numbering system, and hex is a base 16 numbering system using 10 digits ("0" to "9") and six letters ("A" to "F"). See paragraph 2.2.1 below for more detail.

30 Wall *Cyberspace Crime* 80. Van der Merwe also advocated the development of some sort of a computer morality ("rekenaarmoraliteit") in Van der Merwe 1991 *THRHR* 105.

31 For lack of a better term to describe the full power and reach of the change brought about by the next transformation that will take humanity a *quantum* leap forward, Toffler termed it the "Third Wave". Other terms that have been used include "a looming Space Age", the "Information Age", the "Electronic Era", a "Global Village", the "Technetronic Age", the "Post-Industrial Society", the "Scientific-Technological Revolution" and a "Super-Industrial Society". Toffler juxtaposes the so-called Third Wave to the First Wave of change (the agricultural revolution) and the Second Wave of change (the rise of industrial civilization). See Toffler *The Third Wave* 23. Vacca argues that this era is characterised by information technology as the dominant technical artefact. In contrast to the more centralised, hierarchical, social, cultural and economic patterns that reflect the Industrial Age's mechanisation of production systems, the current era is characterised by social, cultural and economic patterns that reflect the decentralised, non-hierarchical flow of information. See Vacca *Computer Forensics: Computer Crime Scene Investigation* 803.

32 With apologies to Irving Berlin, who wrote the song "There's no business like show business" for the 1954 film *Annie get your gun*.

33 Wilding *Computer Evidence: A Forensic Investigations Handbook* 33.

34 American Bankers Association 1985 *Computer Crime Participant's Manual National Seminar Program* 31.

35 Grant 1995 *Intelligence Publication* 1.

the dominant mode when she is trying to penetrate the heart of modern financial crimes will leave an investigator clueless; a basic appreciation of payment systems and current legal tender is simply essential. This does not imply that all law enforcement officers must metamorphose into weird and wired geeks, rendering (as a logical conclusion), "the human race as outmoded as dinosaurs".[36] A mere handle on the technical environment may suffice for many of these practitioners.

When an investigator is harvesting electronic evidence from computing environments, the ultimate goal is still to obtain evidence that is admissible as evidence in a court of law, and to preserve its evidential weight optimally. In the Council of Europe's Explanatory Memorandum to the Recommendation on Problems of Criminal Procedural Law connected with Information Technology,[37] the powers of investigating authorities to obtain evidence of computer-related crimes from dynamic objects (such as computer systems and networks) were explored in parallel to those powers that they have with regard to concrete, tangible and material objects. It was found that computer data is a new form of evidence that requires special rules in respect of its collection, preservation and presentation. The rationale for such special powers included the following computational technicalities:[38]

(a) The essential nature of electronic evidence (aggravated by the possibilities of remote access) poses special problems with regard to its reliability, in that it can easily be accurately copied, or erased or destroyed in another way. The volatile character of computer data necessitates exceptionally efficient search and seizure interventions, as well as the power to control the whole system for a certain time, in order to retain unimpeachable continuity and integrity.

(b) Given the gigantic quantity of data which can be processed and stored, as well as the nature of the logical computer operations during processing and storage, it may be

---

36 Kevin Warwick quoted in Jordaan 2006 *Perspektief* 1.

37 Council of Europe "Explanatory Memorandum to Recommendation 1995(13) on Problems of Criminal Procedural Law connected with Information Technology" found on the Internet http://cm.coe.int/stat/E/Public/1995/ExpRep(95)13.htm (hereinafter referred to as the Council of Europe's Explanatory Memorandum to Recommendation 1995(13)). The Council of Europe was founded following a speech given by Winston Churchill at the University of Zurich on 19 September 1946 calling for a "United States of Europe", similar to the United States of America, in the wake of the events of World War II. The Council of Europe was officially founded on 5 May 1949 by the Treaty of London (now known as the Statute of the Council of Europe 1949 ETS No 001) agreed to by the ten original members. The Council is headquartered in Strasbourg, France. In the years after the dissolution of the Soviet Union and the end of dictatorial Communist rule in Eastern Europe, most Eastern European nations joined the Council, bringing the membership total to 45. Only Belarus, Monaco and Vatican City are not members. The Council of Europe concentrates on the protection of democracy and the rule of law, the protection of human rights, the promotion of Europe's cultural identity and diversity and the encouraging of democratic stability via reform. It also addresses problems facing European society (including discrimination, xenophobia, environmental degradation, AIDS, drugs and organised crime). The institutions of the Council of Europe are the Secretariat and the Secretary-General, the Committee of Ministers, the Parliamentary Assembly, the European Commission for Democracy through Law (known as the Venice Commission), the European Court of Human Rights and the Commissioner for Human Rights. The Council of Europe is not to be confused with the Council of the European Union or the European Council, as the Council of Europe is a separate organisation and not part of the European Union (see footnote 10 in paragraph 6.1 below for a reference to the European Union). Answers.com "Council of Europe" found on the Internet http://www.answers.com/topic/council-of-europe 1-6.

38 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 5-6.

practically impossible to identify and to access the data needed as evidence in multi-user systems.

In addition to these technicalities, a number of other technicalities were highlighted in the South African Law Reform Commission's *Discussion Paper 99 on Computer-related Crime*:[39]

(a) Computer data may be subjected to encryption and/or other software protection techniques, rendering it inaccessible for evidentiary purposes in the absence of the required technological converter(s).

(b) Electronic evidence may be inextricably commingled with collateral information that is legally privileged or necessary for the day-to-day functioning of the business or the network itself.

(c) The increasing interconnectedness of computing environments, even spanning multiple legal jurisdictions, requires exceptionally efficient mutual legal assistance mechanisms and causes unique jurisdictional and double jeopardy problems.

Searching electronic evidence tends to be more complicated than searches for tangible evidence in traditional realms. Some of the idiosyncrasies of computing environments include the fact that computer files consist of electrical impulses that can be stored on the head of a pin and moved around the world in an instant. A single file could be located anywhere on the planet, or could be divided up into several locations in different districts or countries. It may be impossible to learn this prior to the actual execution of the search. Files may be stored on a floppy diskette, in a hidden directory on a suspect's laptop, or on a remote server located thousands of miles away. The files may be encrypted, misleadingly titled, stored in unusual file formats, or commingled with millions of unrelated, innocuous and even statutorily protected files.[40] Despite the largely common legal framework, searches for electronic evidence differ from other searches. Computer technologies also frequently force law enforcement officers to perform computer searches in non-traditional ways. Some of the features of the Internet that makes this necessary include its global and borderless nature, its anonymity, its potential to reach vast audiences easily, its potential as a force multiplier of *e*-crime and the wealth of investigative information produced by the routine storage of information.[41]

---

39 South African Law Reform Commission *Discussion Paper 99 on Computer-related Crime* 14-16 (hereinafter referred to as the South African Law Reform Commission's *Discussion Paper 99 on Computer-related Crime*).

40 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 30-40.

41 United States Report of the President's Working Group on Unlawful Conduct on the Internet "The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet" found on the Internet http://www.usdoj.gov/criminal/cybercrime/unlawful.htm 14.

Existing laws may not be adequate for the realm of cyberspace. The impact of information technology on the legal system has not yet been given the attention that it warrants.[42] Cyberspace may not necessarily demand new laws, but it may require that criminal actions be conceptualised in a different light. The challenges posed by cybercrime cannot be solved by merely slapping existing criminal and criminal procedural laws which govern the physical world onto cyberspace.[43] New technologies challenge existing legal concepts, and there has always been a significant lag between the development of technology and the development of the law:[44]

> De wereld van het recht en die van de techniek zijn zeer verschillend. Nieuwe generaties van technische producten wisselen elkaar in onhutsend tempo af. Het recht heeft een tragere hartslag. Het verschil in levensritme met de wereld van die informatie- en communicatietechnologie (ICT) heeft gevolgen voor het effectieve bereik van regulering. Wanneer een wettelijke regeling in werking treedt is het technische product dat de aanleiding vormde weer verdwenen. In beeldspraak: het recht als mosterd na de maaltijd. Als mosterd die wordt opgediend nadat het bijpassende (technische) gerecht werd genuttigd en weer afgeruimd – en plaats heeft gemaakt voor een nieuwe gang. Het is niet zeker dat de mosterd daarbij dan nog past.[45]

Some of these challenges to existing legal concepts can only be addressed by international law.[46]

Hence, it is essential to adopt adequate international legal instruments that will inspire a concerted international effort:[47]

> As Karnow has said 'It is in this digital soup, this hyperrelational environment, that we see the death of the barrier ... what we do have is, the network and the death of dichotomy. This is fatal for the legal system, which depends, for its very life, on the existence of barriers – after all,

---

42 Watney 2004 *TSAR* 513.

43 Burney "The Concept of Cybercrimes – Is it Right to Analogize a Physical Crime to a Cybercrime?" found on the Internet http://www.cybercrimes.net/Virtual/Burney/page3.html Introduction 2.

44 Seipel *From Data Protection to Knowledge Machines* 80 and Van der Merwe 1998 *SALJ* 2000.

45 Bakshi and Suri *Bharat's Handbook of Cyber and E-Commerce Laws* 2. This Dutch quote can be loosely translated into English as follows: "The world of the law and that of technology differ considerably from one another. New generations of technological products replace previous ones at a disconcerting rate. But the law's heart beats to a slower rhythm. Its tempo differs from that of the world of information and communications technology (ICT) and this has consequences for the effective reach of regulation. By the time that a legal regulation becomes effective, the technological product that led to that regulation has disappeared. To put it another way – the law comes as after meat mustard, as mustard that is served after the matching (technological) meat has been eaten and cleared away – and has made room for the next course. It is not certain that the mustard will still complement the next course" (translated by Idette Noomé).

46 Computer networks (the Internet in particular), defy a traditional understanding of national sovereignty and require international regulation. See, for example, Shytov 2005 *International Journal of Law and Information Technology* 260-280; Coleman and Sapte 2003 *Computer Law & Security Report* 131-136; Sussmann "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium" found on the Internet http://www.law.duke.edu/journals/djcil/articles/djcil9p451.htm 9-17; Walden 2004 *European Journal of Crime, Criminal Law and Criminal Justice* 321; Flanagan 2005 *International Journal of Law and Information Technology* 98-117; Nykodym and Taylor 2004 *Computer Law & Security Report* 390-395; Espiner "Give us Tools to Fight Cybercrime" found on the Internet http://news.com.com/Interpol+Give+us+tools+to+fight+cybercrime/2100-7348_3-605 1-4.

47 The Council of Europe "Explanatory Report to the Convention on Cybercrime (ETS No 185)" found on the Internet http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (hereinafter referred to as the Council of Europe's Explanatory Report to the Cybercrime Convention).

> that's what the law does; it utters the line between this and that, and punishes the transgressor.

Sovereignty and the principle of non-interference in the domestic affairs of another state are fundamental principles which ground the relations of states, but also constitute major tools in the armoury of the criminal element in society. Criminals depend heavily upon the barriers of sovereignty and non-interference to shield themselves and evidence of their crimes from detection. Organisations which orchestrate transnational crime, and which then disperse and conceal the proceeds of their illicit activities across the world have no regard for national borders. In fact, by structuring their organisations to span borders, transnational criminal groups are better able to protect their interests and organisations. They are positioned to take advantage of the differences between legal systems, the clash of bureaucracies, the protection of sovereignty, and, all too often, the complete inability of nations to work together to overcome their differences.[48]

The harmonisation and enactment of adequate domestic and transborder coercive procedural measures consequently play a pivotal role in facilitating effective international cooperation. To this end, both as a signatory to the Council of Europe's Cybercrime Convention[49] and in terms of section 39(1)(b) of its own Constitution,[50] South Africa must comply with and/or take cognisance of the procedural provisions required in terms of the Cybercrime Convention. The Cybercrime Convention, like all good inventions, was born of necessity, in the sense that it recognises that the nature of crime is changing, moving from the national to the international arena, and that it is very difficult, indeed sometimes impossible, to use old analogue[51] laws to map a digitised criminal environment.[52] The solutions proposed in the Cybercrime Convention are, however,

---

48 Proust 2003 *SACJ* 296.

49 The Council of Europe "Cybercrime Convention Budapest 23.XI.2001 CETS No: 185" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (hereinafter referred to as the Cybercrime Convention). There is no precise nomenclature for international treaties: "treaty", "convention", "agreement" and "protocol" are all used interchangeably. The uncertainty in the wording is a result of the relativity of treaties. The meaning of most of the terms used in the law of treaties is extremely variable, changing from country to country and from constitution to constitution; in international law it could even be said to vary from treaty to treaty. Each treaty is "a microcosm laying down [in] its final clauses the law of its own existence in its own terms". See Reuter *Introduction to the Law of Treaties* 29. For the purposes of this thesis, the terms "treaty", "convention", "agreement" and "protocol" are also used interchangeably.

50 International law is brought to bear on law enforcement in various sections of the Constitution, examples of which include: section 198(c), which stipulates that national security must be pursued in compliance with international law; section 199(5), which provides that the security services must act, teach and require their members to act in accordance with customary international law and international agreements binding on South Africa; and section 233, which instructs that every court, when interpreting any legislation, must prefer any reasonable interpretation of the legislation that is consistent with international law. Article 39(1)(b) of the Constitution contains the express command that a court, tribunal or forum, when interpreting the Bill of Rights, must consider international law (this is also in line with section 35(1) of the *interim* Constitution). The reference to international law is not limited to customary international law or treaty law which is binding on South Africa. It is furthermore important, in the light of the underlying purpose of the obligation, to consider the persuasive force of the various sources of international law. See Steytler *Constitutional Criminal Procedure* 10 and 11.

51 Used as a metaphor for the traditional laws rooted in the physical realm. See footnote 9 in paragraph 2.2.1 below for an explanation of analogue versus binary.

52 Room 2004 *New Law Journal* 950.

conceived to enjoin the existing legal systems and powers afforded by the criminal procedural law of the member states, rather than to introduce a totally new order of investigative powers.[53]

The Cybercrime Convention not only adapts traditional procedural measures to the new technological environment, but also creates new measures to ensure that traditional measures of collection, such as search and seizure, remain effective in a volatile technological environment.[54] Search and seizure is but one method of obtaining and preserving electronic evidence; hence, the Cybercrime Convention also aims to provide alternative and less intrusive investigative means of securing information relevant to criminal investigations.[55] Examples of such new alternative measures include the expedited preservation of stored computer data, the partial disclosure of traffic data and production orders. These search and seizure, production and preservation measures constitute the focal points of this research.

The old maxim that "a man's house is his castle"[56] and is thus free from governmental snooping, in binary translates to

01100001001000000110110101100001011011100010011101110011001000000110100001101111011101010111001101100101001000000110100101110011001000000110100001011100110111010001101100011001011000001011100110111010001101100011001010110000101110011011101000110110001100101

Juxtaposing the impact of binary technology with a fundamental right to privacy may underscore the public's apprehension that some form of Orwellian society is not far off,[57] and the definition and scope of privacy has already aroused decades of debate.[58] Technology has accelerated our ability to intrude into areas which people normally prefer to hide from prying eyes. Consequently, the reach of constitutional protection must keep pace with the perils created by these new devices.[59] It has been said that in the world as it has been reconstituted by the microchip, the "Constitution's architecture can easily come to seem quaintly irrelevant – or impossible to take seriously"[60] and that "cybercrime's state of alarm is privacy's state of emergency".[61] The nature of the Internet in particular necessitates procedural provisions that

---

53 This was the point of departure followed in the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 6.

54 The Council of Europe's Explanatory Report to the Cybercrime Convention 24.

55 The Council of Europe's Explanatory Report to the Cybercrime Convention 29. Interception and monitoring, on the other hand, is generally regarded as a more intrusive measure with which to obtain and preserve evidence. See also generally the discussion on the distinctions between search and seizure and interception and monitoring in paragraph 2.4 below.

56 Also referred to in Bloom *Searches, Seizures, and Warrants: A Reference Guide to the United States Constitution* xvi. The maxim probably originates from the following quote from *Semanye's Case* [1558-1774] All ER Rep 62: "... the house of everyone is to him as his castle and fortress, as well as for his defense against injury and violence, as for his repose" (at 62).

57 Rosenberg *The Social Impact of Computers* 309. The Orwellian vision refers to the frighteningly totalitarian futuristic world described by George Orwell in his novel *1984*.

58 Michael *Privacy and Human Rights* 1.

59 Messick 1985 *Santa Clara Law Review* 188.

60 Reynolds 1992 *Management Review* 25.

61 Baron 2002 *The Catholic University of America CommLaw Conspectus* 263.

could otherwise be considered dangerously close to encroaching upon constitutionally protected rights and freedoms.[62]

The law cannot afford not to evolve. However, a technical understanding of computer data as the object of collection only underscores the demand that this evolution should take place in a technologically neutral and, more importantly, constitutionally sound way. Intricate constitutional issues are forced into the equation, for example:

(a) the rights of third parties where electronic evidence is commingled with legally privileged information or information in which innocent parties have a reasonable expectation of privacy or a right of freedom of expression;

(b) the rights of third parties where the electronic evidence constitutes an inextricable part of the day-to-day functioning of the business;

(c) the establishment of the duties, if any, of active cooperation by potential witnesses, such as the systems administrator; and

(d) the rights of the defendant such as the right against self-incrimination where she is expected to provide assistance, for example, by providing passwords or access to decryption technology.

Indiscriminate exploratory computer searches and seizures, overly broad production orders and other variants of law enforcement fishing expeditions pose the concomitant danger of causing a gulf between law enforcement procedures and constitutional values.[63] Article 15 of the Cybercrime Convention does stipulate, *inter alia*, that each party must ensure that the procedural powers adopted do provide for adequate protection of human rights and liberties and do incorporate the principle of proportionality. Nevertheless, the treaty has not escaped extensive criticism. Concerns were raised particularly about the treaty's fundamentally imbalanced nature, in that it is extremely law enforcement-oriented, but barely mentions civil liberties, human rights or corporate interests.[64] It is said to include, for example, "very detailed and sweeping powers of computer search and seizure",[65] but no correspondingly detailed standards to protect privacy and to limit government use of such powers.

---

62 Collier *Criminal Law and the Internet* 343.

63 Silvergate and Viles *Constitutional, Legal and Ethical Considerations for Dealing with Electronic Files in the Age of Cyberspace* IIIa3-5.

64 Anon 2001 *UNESCO Courier* 33. See also paragraph 3.1 below for a reference to some of the concerns raised with regard to the Cybercrime Convention.

65 Taylor "The Council of Europe Cybercrime Convention: A Civil Liberties Perspective" found on the Internet http://www.austlii.edu.au/au/other/CyberLRes/2001/30/ 2.

The itchy fingers of governments worldwide on the triggers of their respective crime-control blunderbusses,[66] particularly those aimed at national and transnational cyberterrorism, has prompted the question of whether the price of collective security would be a loss of civil liberties.[67] The key to fighting terrorism is information[68] and global networks are perceived as a "new form of power".[69] These sentiments are well illustrated by the following two quotes:

> The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros – little bits of data. It's all electrons... There's a war out there, a world war. It's not about who has the most bullets.[70]

and

> Modern military operations are not to do with weapons.... If you want to disarm the world...get rid of all the computers. It's not about the muscle, the strong arm of the warrior. It is his nervous system that matters. Signals and Communications.[71]

Because the United States is a dominant globalising force, the terrorist attacks against the United States on 11 September 2001[72] triggered renewed attention worldwide to combatting terrorism.[73] A few days after 9/11, the United Nations Security Council adopted Resolution 1373 on combatting terrorism.[74] As a response to Resolution 1373, many states took various measures aimed at preventing terrorist attacks and at bringing to justice those who participate in the financing, planning, preparation or perpetration of such acts or in supporting them.[75] This legislative impetus was also instrumental in the amplification of evidence collection devices in the electronic realm.

---

66 Burchell first used this term in respect of the anticipated effort of the South African Law Commission and legislature to criminalise what he referred to as "the next area of panic ... that is colloquially called cybercrime." Burchell 2002 *SALJ* 119(3) 579.

67 Ferrera *et al Cyberlaw Text and Cases* 441.

68 Lyon *Surveillance after September 11* 88.

69 Bowrey *Law and Internet Cultures* 178, 174-175. This ties in with the sentiments of anti-globalisation activists that contend that globalisation is a process that is mediated according to elite imperatives. See Answers.com "Globalization" found on the Internet http://www.answers.com/globalisation 6. Internet governance, in particular, is a highly contentious issue. Internet governance is defined as the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. Answers.com "Internet Governance" found on the Internet http://www.answers.com/topic/internet-governance 3. At this stage, ICANN (Internet Cooperation for Assigned Names and Numbers), under contract to the United States government, is responsible for the technical governance of the Internet. ICANN is a non-profit, international association founded in 1998 and incorporated in the United States. It is the successor to the Internet Assigned Numbers Authority (IANA). Its tasks include managing the assignment of domain names and Internet Protocol (IP) addresses. See Answers.com "ICANN" found on the Internet http://www.answers.com/ICANN 1-2. At the first World Summit on the Information Society (WSIS) in Geneva in 2003, the topic of Internet governance was put on the table and the Internet Governance Forum and a Working Group on Internet Governance (WGIG) were set up as a result.

70 Wall *Cyberspace Crime* 448, quoting Cosmos, the villain in the MCA/Universal film *Sneakers*.

71 Webster *Theories of the Information Society* 64, quoting Professor John Erikson as published in *The Guardian* 11 November 1982.

72 Hereinafter referred to as 9/11.

73 Lyon *Surveillance after September 11* 111. The prevention of international terrorism remains a critical priority and was, once again, emphasised by the Madrid bombings in 2004 and the bombings in England in 2005.

74 United Nations Security Council Resolution 1373: Combating Terrorism S/RES/1373 (2001) found on the Internet http://.undoc.org/pdf/crime/terrorism/res_1373_english.pdf. Hereinafter referred to as United Nations Resolution 1373.

75 The most important of the newly introduced legislative measures in the United States, England and South Africa were the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), the Anti-terrorism, Crime and Security Act of 2001 and the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 respectively. These three countries constitute the points of reference for the comparative analysis conducted within the scope of this research. See paragraph 1.3 below with regard to the methodology that was followed.

Bearing in mind the specific comparative scope of this research,[76] it must be pointed out here that the Cybercrime Convention was signed by South Africa,[77] the United States[78] and England[79]. So far, however, none of the three countries has ratified the Cybercrime Convention. Also, none of the three countries has thus far signed or ratified the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature.

As a signatory to the Cybercrime Convention, South Africa[80] has undertaken to introduce the proposed national measures in respect of both substantive criminal law and procedural law into its legal framework.

---

76 This choice of comparison is justified in paragraph 1.3 below.

77 See chapter 4 of this study. The Cybercrime Convention was signed in 2001 by Mr Charles Nqakula, the then Deputy Minister of Foreign Affairs, who was delegated to the task by President Thabo Mbeki. The "Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems Strasbourg, 28.I.2003" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm (hereinafter referred to as the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature) was not signed on this occasion. The current status of the process of ratification is that a Presidential Minute has been drafted (and forwarded to the Presidency on 26 April 2006) to authorise the South African Ambassador in Brussels with the power to sign the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature on behalf of South Africa. It is deemed appropriate to sign both documents first, prior to spearheading the parliamentary ratification process (this information was provided courtesy of Adv Herman van Heerden, attached to the Chief Directorate: International Legal Relations of the Department of Justice and Constitutional Development, who accompanied Mr Nqakula to Budapest for the signing of the Cybercrime Convention). In terms of section 27(1) of the International Cooperation in Criminal Matters Act 75 of 1996 (hereinafter referred to as the International Cooperation in Criminal Matters Act) and sections 83(1), read with 231(1) of the Constitution, the President, as head of the National Executive, may, on such conditions as he deems fit, enter into any agreement with any foreign state for the provision of mutual assistance in criminal matters and may agree to any amendment of such an agreement. After Parliament has agreed to the ratification of, accession to, amendment or revocation of such agreement, the Minister of Justice and Constitutional Development gives notice thereof in the Government Gazette in terms of section 27(2) of the International Cooperation in Criminal Matters Act. The Constitution provides that an international agreement, duly negotiated and signed by the National Executive, only binds South Africa after it has been approved by resolution in both the National Assembly and the National Council of Provinces (articles 231(1) and 231(2) of the Constitution). An exception is provided for in article 231(3), in that an international agreement of a technical, administrative or executive nature, or an agreement which does not require ratification or accession, entered into by the National Executive, does not require approval by the National Assembly and the National Council of Provinces for it to become binding, although it must be tabled within a reasonable time. An international agreement becomes law in South Africa when it is enacted into law by national legislation. A self-executing provision of an agreement that has been approved by Parliament is, however, law in South Africa, unless it is inconsistent with the Constitution or an Act of Parliament.

78 See chapter 5 of this study. The United States has been active behind the scenes in developing and promoting the cybercrime efforts of the leading bodies internationally (including the Council of Europe). See Privacy International "Overview – Not really about Cybercrime" found on the Internet http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65424 1. This active participation by the United States has been termed "policy laundering", and the United States has been accused of "internationalising" controversial domestic policies. The Cybercrime Convention has been said to bear peculiar resemblances to the "Electronic Frontier: The Challenge of Unlawful Conduct Involving the Internet" report released by the United States Department of Justice. See Banisar "Love Letter's Last Victim" found on the Internet http://www.securityfocus.com/news/39 2. The Bush administration's pushing to ratify the Cybercrime Convention so as to "deny 'safe havens' to criminals, including terrorists, who can cause damage to U.S. interests abroad using computer systems" has been met with criticism. Concerns have been raised that the Cybercrime Convention not only threatens core liberties, but will obligate the United States to use extraordinary powers to do the "dirty work" of other nations. Some of the signatories to the Cybercrime Convention include states that have been termed "nations of recent and untested democratic vintage, such as Ukraine and Bulgaria". It has been asked whether it is desirable to have "professional American law enforcement personnel conducting surveillance on people who haven't broken any United States law in order to help enforce the 'law' of some Party apparatchick in China". See Rizvi "Bush Pushes Plan to Permit Internet Surveillance" found on the Internet http://www.commondreams.org/headlines04/0121-01.htm 2. As the United States is generally regarded as the centre of the Internet, it will undoubtedly have to entertain a large volume of requests. Companies in the United States fear that they will be swamped with subpoenas for computer data as law enforcement officers in other countries take advantage of the breadth of the accord. The processing of these requests costs money and strains network systems. Rosen "The US – EU Convention on Cybercrime" found on the Internet http://www.lawtechjournal.comnotes/2002/19_020819_rosen.php 1. The retention of data solely for law enforcement purposes is a significant burden that will ultimately be shifted to consumers in the United States. See Hosein "Privacy and Cyberspace: Questioning the Need for Harmonisation" found on the Internet http://www.itu.int/osg/spu/cybersecurity/docs/Hosein_Privacy_and_Cyberspace.pdf 5.

79 See chapter 6 of this study.

80 For interesting reading, see the findings in McConnell International "Risk *e*-Business: Seizing the Opportunity of Global *e*-Readiness" found on the Internet http://www.mcconnellinternational.com/ereadiness/EreadinessReport.htm 2, 4 and 11. According to this report, South Africa, investigated as one of 42 critical economies in terms of its *e*-readiness, required improvement in respect of *e*-leadership and information security and "substantial improvement" in respect of connectivity, human capital and the *e*-business climate in the conditions necessary to support *e*-business and *e*-government. The *e*-readiness ratings measured status and progress on the five interrelated attributes of connectivity (the ease and affordability of

This study is concerned with the criminal procedural powers of search and seizure, production and preservation. In order to assess the extent to which the South African catalogue of search and seizure, production and preservation mechanisms measures up against those proposed by the Cybercrime Convention, the point of departure was a consideration of the relevant provisions of the Criminal Procedure Act,[81] the Electronic Communications and Transactions Act[82] and the RICPCIA.

The principal hypothesis of this thesis is that a comparative analysis between the current catalogue of South Africa's domestic and international search and seizure, production and preservation mechanisms and the application thereof, with those proposed in the Cybercrime Convention will expose a number of *lacunae*.

In reviewing the South African search and seizure, production and preservation devices, it is imperative that the relevant constitutional rights be heeded, including, in particular, the right to dignity,[83] the right to privacy,[84] the right to freedom of expression,[85] the right not to be deprived of property,[86] and the rights of arrested, detained and accused persons, particularly the right against self-incrimination entrenched in the right to a fair trial.[87] The exclusionary rule[88] and the limitations[89] and interpretation[90] clauses of the Constitution are instrumental for a constitutionally sound assessment.

---

access and the use of networks); *e*-leadership (whether *e*-readiness constitutes a national priority); information security (whether the processing and storage of networked information can be trusted); human capital (whether the right people are available to support *e*-business and build a knowledge-based society); and the *e*-business climate (the ease with which *e*-business can be conducted). Key elements taken into account under the attribute of information security were, *inter alia*, the strength and effectiveness of the legal framework to address and prosecute computer crimes, authorise digital signatures and enable public key infrastructures. In this respect, see McConnell International "Cyber Crime ... and Punishment?" found on the Internet http://www.mcconnellinternational.com/services/cybercrime.htm 1-3. In this report, the state of the law in 52 countries was analysed in order to assess the extent of progress on updating cyber crime laws. Only ten countries had laws in place that covered more than half of the kinds of crime that need to be addressed. South Africa was rated among the 33 countries with no updated laws (this research was, however, conducted prior to the promulgation of two South African legislative interventions in 2002, namely the RICPCIA and the Electronic Communications and Transactions Act 25 of 2002). Outdated laws and regulations, coupled with weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct *e*-business. The Middle East and Africa are reported to present the greatest challenge to *e*-business. The thin infrastructure remains an enormous barrier, despite the cultural propensity to share information and communications technologies (ICT) access among multiple users. With nearly 15% of the world's population, the African continent possesses just 2% of the world's total number of telephones and less than 0.1% of all Internet access. Africa has, however, witnessed complementary growth in Internet host numbers at nearly double the rest of the world's 18% rate by the year 2003. Only five African nations had Internet access in 1998, but all 54 states were connected by 2003. The cost of Internet access relative to the *per capita* income remains a critical unfavourable factor, along with inefficient transportation systems, inadequate treatment of information security and low human capital levels. Although only seven countries were assessed in this report (Egypt, Ghana, Kenya, Nigeria, Saudi Arabia, Tanzania and South Africa), the report concluded that a more inclusive evaluation would have reflected even more negatively on the connectivity of the African continent. See McConnell International "Risk *e*-Business: Seizing the Opportunity of Global e-Readiness" found on the Internet http://www.mcconnellinternational.com/ereadiness/EreadinessReport.htm 15.

81 51 of 1977. Hereinafter referred to as the Criminal Procedure Act.

82 25 of 2002. Hereinafter referred to as the Electronic Communications and Transactions Act.

83 Section 10 of the Constitution.

84 Section 14 of the Constitution.

85 Section 16 of the Constitution.

86 Section 25 of the Constitution.

87 Section 35(3)(j) of the Constitution.

88 Section 35(5) of the Constitution.

89 Section 36 of the Constitution.

90 Section 39 of the Constitution.

The current evolutionary state of, first, search and seizure and, second, production and preservation is discussed briefly below.

1.1.1 Search and seizure

The cybercrime provisions in chapter XIII of the Electronic Communications and Transactions Act are rooted in the proposals of the South African Law Reform Commission's *Discussion Paper 99 on Computer-related Crime*.[91] The second stage of the incremental approach used in this Discussion Paper involved a consideration of the desirability of introducing procedural provisions aimed at enhancing the investigation and prosecution of computer-related crimes. In respect of search and seizure, it was found that chapter 2 of the Criminal Procedure Act would not apply to the search of a computer and the seizure of information located on that computer, although it would allow for the seizure of a particular computer. It was found that the provisions of the Criminal Procedure Act were developed when the idea of a location which does not refer to physical premises or the seizure of something which is not a tangible object were inconceivable.[92] In order to address, *inter alia*, this anomaly in practice, in chapter 3 of its Computer Misuse Bill,[93] the South African Law Reform Commission proposed the inclusion of new search and seizure provisions. The issue of the correct placement of these procedural provisions, particularly referring to the alternative of inserting these provisions into the Criminal Procedure Act, was left open.

However, subsequent to the issuing of the South African Law Reform Commission's *Discussion Paper 99 on Computer-related Crime*, the Department of Communications tabled the Electronic Communications and Transactions Act in Parliament; and it was signed into law on 31 July 2002. Although its chapter XIII provides for extensive coercive powers of inspection, search and seizure, these powers are entrusted to a new breed of so-called "cyber inspectors" employed by the Department of Communications. This initiative is an unexpected and unprecedented extension of the powers of the Department of Communications and has already aroused some cynicism. It has, *inter alia*, been stated that, although the Electronic Communications and Transactions Act clearly foresees an era of fruitful cooperation between cyber inspectors and the South African Police Service,[94] the old impossibility of interdepartmental cooperation may make such cooperation as difficult to achieve in this particular field as in any other.[95]

---

91 South African Law Reform Commission *Discussion Paper 99 on Computer-related Crime* 78.
92 South African Law Reform Commission *Discussion Paper 99 on Computer-related Crime* 14.
93 Hereinafter referred to as the proposed Computer Misuse Bill. See the South African Law Reform Commission *Discussion Paper 99 on Computer-related Crime* 66-68.
94 As well as the other South African law enforcement agencies (see footnote 24 above for a reference to other South African law enforcement capacities).
95 CSIR-Defencetek *CSIR FACTS* 31.

It is an anomaly in the Electronic Communications and Transactions Act that neither the South African Police Services nor any other statutory bodies with powers of inspection, search and seizure in terms of any law can utilise the procedural provisions of the Electronic Communications and Transactions Act without the assistance of a cyber inspector. With specific reference to this anomaly, it has been recommended that the provisions of the Criminal Procedure Act be aligned to solve the problems that arise, in particular with jurisdiction and the restricting interpretations of the words "premises" and "article" as physical entities, as set out in sections 20 and 21 of the Criminal Procedure Act.[96]

It is submitted, as a rationale for this study, that an analysis of the South African search and seizure devices applicable to electronic evidence is warranted.

1.1.2 Production and preservation

The principal recommendations in the South African Law Reform Commission's *Discussion Paper 78 on the Interception and Monitoring Prohibition Act*[97] focus on the augmentation of the then Interception and Monitoring Prohibition Act.[98] The South African Law Reform Commission advised that service providers be obliged to ensure that all communications are capable of interception and monitoring. The insertion of a technically correct definition of "call related information"[99] and certain amendments facilitating the provision of such so-called call-related data were also proposed.

This Discussion Paper preceded the controversial and much-debated RICPCIA, which was only signed into law on 30 September 2005, although the President had already assented to it on 20 December 2002. The RICPCIA sets out to regulate, *inter alia*, the provision of communication-related information[100] under certain circumstances; the execution of directions under the RICPCIA by law enforcement officers; and the assistance to be given by postal service providers, telecommunications service providers and decryption key holders in the execution of these directions.

A cryptography[101] provider may not provide cryptographic services or products in South Africa unless the provider is registered with the Department of Communications.[102] A register of

---

96 Watney 2003 *TSAR* 73.

97 South African Law Reform Commission *Discussion Paper 78 Review of Security Legislation: The Interception and Monitoring Prohibition Act 127 of 1992* (hereinafter referred to as the South African Law Reform Commission *Discussion Paper 78 on the Interception and Monitoring Prohibition Act*).

98 127 of 1992, hereinafter referred to as the Interception and Monitoring Prohibition Act.

99 As *per* section 1 of the Interception and Monitoring Prohibition Bill, 1999 proposed by the South African Law Reform Commission as Annexure "A" to the South African Law Reform Commission *Discussion Paper 78 on the Interception and Monitoring Prohibition Act* 112 – 124.

100 Communication-related information is defined in paragraph 2.2.1.1.2 below.

101 See paragraph 2.3.1.3.2 below for a reference to the meaning of cryptography.

cryptography providers must be established and maintained.[103] Disclosure of the information contained in this cryptography register is restricted to, *inter alia*, a relevant authority investigating a criminal offence for the purposes of any criminal proceedings, government agencies responsible for safety and security in South Africa or a cyber inspector.[104] The deployment of decryption directions under section 21 of the RICPCIA is, however, confined to applications for interception directions in terms of section 16 of the RICPCIA. Decryption directions cannot be utilised to decrypt encrypted electronic evidence obtained, for example, by means of a search and seizure intervention. Also, cyber inspectors cannot apply for an interception direction under the RICPCIA.

The availability of the procedures aimed at the provision of communication-related information, as provided for in the RICPCIA, does not preclude obtaining such information in accordance with a procedure prescribed in any other act, provided that such information is not obtained on an ongoing basis.[105] Section 205 of the Criminal Procedure Act therefore remains available as an important means of inducing an entity to make archived communication-related information available to law enforcement agencies.

It seems that no specific provision has been made in the South African legislative framework for the expedited preservation of stored computer data and the partial disclosure of traffic data, as required by the Cybercrime Convention. Section 30(1) of RICPCIA, however, obliges South African telecommunications service providers to provide a telecommunications service that can store communication-related information. Section 16 of the Electronic Communications and Transactions Act also provides for electronic equivalence in respect of paper-based retention requirements under other acts. It must be considered whether, and if so, to what extent, these data retention requirements make South Africa compliant with the preservation devices required under the Cybercrime Convention.

It is submitted as a rationale for this study, that an analysis of the South African production and preservation mechanisms applicable to electronic evidence is warranted.

---

102 Section 30(1) of the Electronic Communications and Transactions Act.

103 Section 29 of the Electronic Communications and Transactions Act. The following particulars must be recorded in the register: the name and address of the cryptography provider; a description of the type of cryptography service or cryptography product provided and any other particulars that may be prescribed to identify and locate the cryptography provider or its products or services adequately. Confidential information or trade secrets in respect of cryptography services or products are not liable to disclosure.

104 Section 31(2) of the Electronic Communications and Transactions Act.

105 Section 15 of the RICPCIA.

1.2 Method in the madness

The main objective of this thesis is to consider whether the South African criminal procedural law provisions of search and seizure need to be aligned and/or augmented in order to provide the necessary legal infrastructure to effectively and constitutionally search, or similarly access, and seize, copy, or similarly secure, electronic evidence from computing environments. The existing South African procedural mechanisms aimed at inducing the production and preservation of electronic evidence are also examined in this study.[106]

In pursuing this objective, the Cybercrime Convention is used as the yardstick against which the South African catalogue of criminal procedural search and seizure, production and preservation devices is measured.[107] Where any alignment or augmentation of the South African mechanisms is found to be necessary, this study identifies these intervention areas.[108]

In considering any such alignments and/or augmentations, this study furthermore illustrates the application of the equivalent domestic[109] search and seizure, production and preservation mechanisms directed at electronic evidence used in the United States[110] and in England.[111]

1.3 Methodology

In line with the obligation expressed in section 39(1)(b) of the Constitution to take cognisance of international law when interpreting the Bill of Rights, this study attempts an in-depth analysis of the search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention, as opposed to the criminal procedural mechanisms generally available to law enforcement agents under current South African law.[112] In order to consider the desirability of alternative, additional and/or aligned mechanisms aimed at electronic evidence, it is necessary to identify and outline both the relevant legal and technological issues. This thesis remains but an attempt made by a lawyer, bugged and blessed with the heart of a "techie", to focus throughout on the legal aspects of the collection of electronic evidence from computing environments.

---

106 See chapter 4.
107 See chapter 3.
108 See chapter 7.
109 Although both the domestic and transborder procedural mechanisms available in the South African legal framework and those proposed in the Cybercrime Convention are mentioned in this study, only the domestic procedural mechanisms available in the United States and England are considered in this research. An attempt to incorporate the transborder mechanisms, from a comparative perspective as well would have rendered the scope of this thesis far too wide.
110 See chapter 5.
111 See chapter 6.
112 See chapter 4.

In considering foreign law, as provided for in section 39(1)(c) of the Constitution, a comparative legal research methodology will be used. The positions in both the United States and England[113] are studied. From a technical perspective, the decision to undertake such a comparison is, *inter alia*, supported by the fact that the parent companies of the vast majority of Internet Service Providers in South Africa are situated either in the United Kingdom and/or in the United States. Also, the two biggest domain name servers, www.whois.com and www.arin.net, and the Internet Corporation for Assigned Names and Numbers, are located in the United States. This makes them the most critical points of investigative contact with almost all other nation states, particularly with regard to the transborder deployment of search and seizure, production and preservation mechanisms in networked computing environments.

From a legal perspective, South Africa has strong law enforcement ties with both the United States and England,[114] both of which subscribe to the G8 24/7 point of contact,[115] the probable predecessor to the 24/7 network envisaged in article 35 of the Cybercrime Convention. Like South Africa, both these countries are signatories to the Cybercrime Convention. The legal frameworks of the United States and England regarding current compliance with the Cybercrime Convention are probably the most advanced at this stage. Some authors believe that these jurisdictions have laws in place that cover all the Cybercrime Convention's requirements.[116]

Historically, South African criminal procedure takes English law as its common law.[117] The Human Rights Act[118] has now, for the first time, incorporated into English domestic law a right of privacy and the right to a fair trial as *per* articles 8 and 6 of the European Convention for the

---

113 The comparative reach is limited to the position in English law and it is not concerned with the broader legislative framework of the United Kingdom (the positions in Scotland, Wales and Northern Ireland technically do not resort within the scope of this study).

114 Specifically with the Federal Bureau of Investigation (FBI) and Scotland Yard respectively.

115 See paragraph 3.4.1.2.4 below.

116 See, for example, Room 2004 *New Law Journal* 951 with regard to England. The United States Department of Justice has also indicated that it does not anticipate the implementation of any legislation for the United States to become a party to the Cybercrime Convention. Several reasons are cited for this supposition, including that the Cybercrime Convention largely tracks current United States law due to its active participation in the drafting process; the treaty generally permits states to reserve provisions where existing cybercrime laws conflict between states; and the treaty defers to pre-existing international agreements. Interestingly, specific concerns were raised that the Cybercrime Convention and its amendment process may introduce stagnation. It has been argued that, while the Cybercrime Convention essentially exports United States law, current United States law on Cybercrime is far from ideal. Cybercrime legislation in the United States is complicated by its residual ties to property law precedents and telephony-based statutory law. Cybercrime legislation worldwide is in a nascent state and hence highly susceptible to alteration. Alternative paradigms may be found more suitable to cyberspace and a widespread adoption of the Cybercrime Convention could, in actual fact, stunt the development of cybercrime legislation. It has, however, been conceded that, unlike the criminalisation of offences, the provisions establishing procedural laws to provide law enforcement officials with the authority and tools necessary to comply with requests for international cooperation are less clearly traceable to existing United States law. See Weber 2003 *Berkeley Technology Law Journal* 435, 437 and 443. The United States Department of Justice's argument that, upon its ratification of the Cybercrime Convention, the country would not have to pass any new domestic laws to bring it in line with the treaty has been met with some scepticism. Concerns have been raised that, while the treaty is already being used as a pretext in some developing nations to pass some "pretty draconian laws", it would come as no surprise to see it used in a similar way in the United States. See Poulsen "US Defends Cybercrime Treaty" found on the Internet http://www.securityfocus.com/news/8529 1.

117 See paragraph 4.2.1 below for a reference to the historical roots of South African criminal procedural law.

118 Of 1998. Hereinafter referred to as the Human Rights Act or the HRA.

Protection of Human Rights and Fundamental Freedoms[119] respectively. In the United States, there is an entrenched protection against unreasonable searches (and this has been in place for two centuries) and there is consequently a wealth of case law concerning the reconciliation of electronic searches with the Fourth Amendment.[120] Precedents regarding the practical deployment and application not only of search and seizure measures, but also of production and preservation measures, may prove useful to South African law enforcement and legal practitioners.

It is axiomatic that the outcome of any challenge to the legality of a search and seizure, production or preservation intervention depends on the judicial interpretation and application not only of domestic criminal procedural and evidence law, but also of human rights law. It is therefore useful to compare protections afforded by the (South African) Constitution, the (English) Human Rights Act, the European Convention of Human Rights and those granted by the Constitution of the United States. Whilst there may be differences of emphasis and of detail, there are similarities of principle and it is possible to draw insightful analogies.

Bearing in mind the background to this study[121] and the aims of the research,[122] the remainder of the thesis is divided into the following chapters:

(a) **Chapter 2: A technical contextualisation**

Some grasp of the technical environment underpinning the application of the search and seizure, production and preservation devices is a *sine qua non* not only for the physical collection of electronic evidence in computing environments, but also for understanding the legalities involved in such an intervention. Chapter 2 therefore seeks to provide both clarity on terminology and a technical contextualisation of the research parameters.

(b) **Chapter 3: Search and seizure, production and preservation @ the Cybercrime Convention**

The Cybercrime Convention constitutes the internationally agreed benchmark, *inter alia*, for the procedural powers aimed at the collection of electronic evidence. Chapter 3 explores the domestic and the international search and seizure, production and preservation devices proposed by the Cybercrime Convention.

(c) **Chapter 4: Search and seizure, production and preservation @ South Africa**

Chapter 4 provides an exposition of the current South African domestic and international

---

119 Council of Europe "Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol No 11 Rome, 4X.I. 1950" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm. Hereinafter referred to as the European Convention on the Protection of Human Rights or the ECHR.

120 A number of the most pivotal of these cases are referred to in chapter 5 of this thesis.

121 As set out in paragraph 1.1 above.

122 As pointed out in paragraph 1.2 above.

search and seizure mechanisms, as well as the equivalents of the ancillary procedural measures of preservation and production as proposed by the Cybercrime Convention. The rationale for this investigation is the facilitation of a comparative analysis of the requirements of the Cybercrime Convention (as detailed in chapter 3) on the one hand, and the South African *status quo* (as elucidated in chapter 4) on the other. The findings of this comparative analysis are incorporated into chapter 7.

(d) **Chapter 5: A snapshot[123] of troubleshooting @ the United States**

Chapter 5 displays a snapshot of the array of domestic[124] search and seizure, production and preservation mechanisms available within the legal framework of the United States. This exposition provides a contextually comparative troubleshooting utility[125] in respect of the application of these procedural mechanisms to electronic evidence in South Africa.

(e) **Chapter 6: A snapshot of troubleshooting @ England**

Chapter 6 provides a snapshot of the domestic search and seizure, production and preservation mechanisms available in the legal framework of England, similar to the one provided in chapter 5 in respect of the United States.

(f) **Chapter 7: Search hits[126] and cursors[127]**

Chapter 7 lists the findings of the study. It also discusses the resulting recommendations required to align and/or augment the South African search and seizure, production and preservation mechanisms to those put forward in the Cybercrime Convention. The most important lessons learned from the comparative

---

123 A snapshot is similar to a detailed table of contents and contains a set of reference markers, or pointers, to data stored on a disk drive, on a tape or in a storage area network (SAN). Snapshots streamline access to stored data and can speed up the process of data recovery. See SearchStorage.com Definitions "Storage Snapshot" found on the Internet http://searchstorage.tehctarget.com/sDefinition/0,290660,sid5_gci1008820,00.html 1. In this context, snapshot is meant to provide an overview of the most important search and seizure, production and preservation measures (and the application thereof to electronic evidence) in the United States in chapter 5, and in England in chapter 6.

124 See footnote 109 in paragraph 1.2 above.

125 A "utility" is a term used to describe a program designed to help the user in the operation of a computer. A "troubleshooter" is a special type of Help utility available in Windows XP and 2000. Troubleshooter utilities enable the user to pinpoint problems and identify solutions to those problems by asking a series of questions and then providing detailed troubleshooting information based on the user's responses. Brooks *A+ Certification Concepts & Practice* 954. See also paragraph 2.5.1.2.2 below. Here, troubleshooting involves the comparative consideration of the application of search and seizure, production and preservation devices in the United States and England to electronic evidence in order to consider its equivalent application to the South African legislative context.

126 A search "hit" in computing means a successful match. In computer searches the search engine lists the "hits" found to match the specified search conditions. A hit is simply a match of data in a search string against data that is being searched. See Answers.com "Hit" found on the Internet http://www.answers.com/topic.hit 1. A hit can also denote the number of times a program or item of data has been accessed or a connection has been successfully made to a website over the Internet or another network. See also Answers.com "Hits" found on the Internet http://www.answers.com/topic/hits-pulp-album 1. In the context used here, it refers to the findings of this thesis.

127 A cursor (also called a "pointer") in computer science denotes a symbol appearing on a display screen in a graphical user interface (GUI) that lets the user select a command by clicking with a pointing device or pressing the enter key when the pointer symbol is positioned on the appropriate button or icon. A cursor can also mean a symbol used to point some element on screen. See Answers.com "Pointer" found on the Internet http://www.answers.com/pointer 1. A cursor is a bright, usually blinking, movable indicator on a display, marking the position at which a character can be entered, corrected or deleted. On DOS and other character-based screens, it is a blinking rectangle or underline. On Windows and other graphics-based screens, it changes shape as it is moved into different windows. For example, it may turn into an I-beam for editing text, an arrow for selecting menus or a pen for drawing. The literal meaning or the original Latin word "*cursor*" expresses the idea of someone or something that runs. See Answers.com "Cursor" found on the Internet http://www.answers.com/topic/cursor 1. In the context used here, cursors mean the recommendations made as a result of this research.

consideration of the search and seizure, production and preservation devices catered for in the United States and England are also incorporated into this chapter.

1.4 Moral of the story: unplugged

The relationship between the law and information technology can be better understood in the light of a Chinese curse that expresses the wish that the addressee should "live in interesting times".[128] In celebration of the researcher's first, somewhat turbulent 30 years on this planet, an insider trader to this turbulence presented a somewhat off-the-wall, but a contextually spot-on, gift at the time: a fridge magnet reading "to hell with living in interesting times, I want to be bored". Sadly, this reflects the state of mind of all too many lawyers and law enforcers – and there is nothing to hide behind. Quite the opposite: this (law enforcement) business is becoming binary and "the show must go on".[129]

To each her own and beholding therefore the beholder's eye, the *raison d'être* of this research, in the final analysis, is to provide the reader with either an interesting or boring "byte"[130] of the cherry that is the orgasmic world of cyberspace.

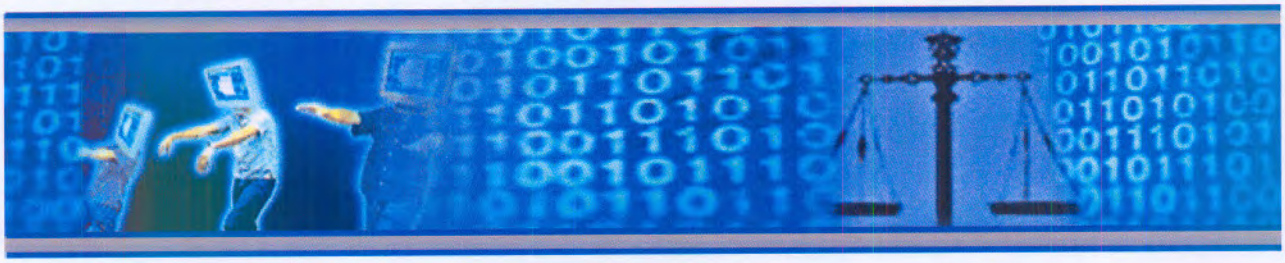
---

128 Lloyd *Information Technology Law* xlv.

129 Borrowing from the theatrical motto dating from the 1800s and which has been applied to other situations since the first half of the 1900s. See Answers.com "The Show Must Go On" found on the Internet http://www.answers.com/The%20Show%20Must%20Go%20On#after_ad1 1.

130 For an understanding of "byte", see paragraph 2.1.1 below.

CHAPTER 2:
A TECHNICAL CONTEXTUALISATION



2.1 BOOTSTRAP 25

2.2 THE OBJECT OF SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION . 26

2.2.1 Computer data 26
2.2.1.1 Communications data: a special type of computer data 31

2.3 THE OBJECTIVE OF SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION 36

2.3.1 Electronic evidence 36
2.3.1.1 Mining forensic gold in search of electronic evidence 38
2.3.1.2 Computer forensics: a means to an end 41
2.3.1.3 Anti-Forensics: another one bytes the rust 45

2.4 CAUGHT IN THE ACT: INTERCEPTION AND MONITORING, SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION 48

2.4.1 Interception/collection and monitoring 51
2.4.2 Search and seizure 53
2.4.3 Production 56
2.4.4 Preservation 56

2.5 PENETRATING THE HOUSE OF BINARY: COMPUTERS OF ALL SHAPES AND SIZES 58

2.5.1 Computer system 58
2.5.1.1 Computer hardware 59
2.5.1.2 Computer software 67
2.5.1.3 Categories of computer systems 70

2.6 CATEGORIES OF COMPUTING ENVIRONMENTS – WHO MOVED MY BIT? 72

2.6.1 Stand-alone computing environments 72
2.6.2 Networked computing environments 73
2.6.2.1 Theoretical network reference models 76
2.6.2.2 Network control strategies 78
2.6.2.3 Network topologies 82
2.6.2.4 Network transmission media 82
2.6.2.5 Categories of computer networks 83
2.6.3 The biggest WAN of all – the Internet and the World Wide Web 86

2.7 BROUTER TO CHAPTER 3 91

2.1 Bootstrap[1]

Before delving into the legalities associated with deploying the procedural devices of search and seizure, production and preservation in computing environments, it is essential to provide an overview of the technicalities underpinning these devices. This chapter is intended to be general, and is particularly germane to those readers who are not very technically proficient. It must be noted, at the onset, that the relentless pace of change in the computer and related industries will quickly outdate even a sophisticated, detailed explanation of the technologies involved.[2] Mindful that familiarity may breed contempt, the aim of this chapter is to familiarise the reader with the exceedingly complex technologies involved in computers and networks. The breathtaking pace of change and the sometimes startling complexity of these technologies have important ramifications for the legal process involved and its protagonists: aspiring to remain relevant and meaningful in the Third Wave is a truly humbling experience that requires enormous perseverance. In as much as a journey of a thousand miles begins with a single step,[3] an understanding of the technicalities intertwined with the harvesting of electronic evidence begins with knowing that you know not.

This chapter seeks to provide both clarity on terminology typical of the collection of electronic evidence, and a technical contextualisation of the research parameters. First, computer data, as the object, and electronic evidence, as the objective, of collection interventions are considered in turn. Next, terms critical to the unfolding of this research are elucidated, namely search and seizure; interception/collection and monitoring (in negatively defining search and seizure); production, preservation and retention (in negatively defining preservation). Finally, a broad overview is given of computers and the computing environments that must be penetrated in search of electronic evidence.

One of the most common pitfalls in computer-related crime investigations is that law enforcement officers become so involved with the technology that they get lost in virtual reality. Whilst this study surfs[4] the technicalities, the legalities root firmly in the Cybercrime Convention

---

1 A "bootstrap" is a small strap or loop at the back of a leather boot that enables one to pull the entire boot on. In computers, to bootstrap (or to "boot") is to load a program into a computer using a much smaller initial program to load in the desired program (which is usually an operating system – see paragraph 2.5.1.2.2 below for a reference to operating systems). In general usage, bootstrapping is the leveraging of a small initial effort into something larger and more significant. There is also a common expression, "pulling yourself up by your own bootstraps" meaning to leverage yourself to success from a small beginning. See SMB Definitions "Bootstrap" found on the Internet http://searchsmb.techtarget.com/sDefinition/0,290660,sid44_gci214479,00.html . In this context, to bootstrap means to introduce the reader to the technicalities associated with collecting evidence from computing environments.

2 Takach *Computer Law* 14.

3 Confucius "Quote DB" found on the Internet http:///.quotedb.com/quotes/1482 1.

4 The term "surfing" in hacker slang initially denoted traversing the Internet in search of interesting material, and the term was used especially if the user was searching with a World Wide Web (WWW) browser. However, many hackers stopped using the term once it went completely mainstream around 1995. The passive couch-potato connotations that go with TV channel surfing and hearing non-hackers wax lyrical about "surfing the net" tended to make hackers feel a bit as though their stamping grounds were being overrun by *ignorami*. See Answers.com "Surf" found on the Internet http://www.answers.com /topic/surf?method=6 1.

and the relevant legislative provisions in South African law. This point of departure is in itself a tall order, without referring to other legal systems at this stage.[5] It is nevertheless imperative to set the scene for a comparative analysis of the requirements of the Cybercrime Convention, as detailed in chapter 3, on the one hand, and the South African *status quo* as elucidated in chapter 4 on the other hand.

2.2 *The object of search and seizure, production and preservation*

When law enforcement officers search for and seize electronic evidence, hardware is not simply transported from a crime scene to an evidence storage facility. Similarly, when such officers request the production or preservation of information in electronic format, the process does not merely involve the handing over or isolation of hardware. On the contrary: when searching and seizing, preserving or producing information collected from computing environments, law enforcement officers enter upon the business of browsing[6] or busting the binary in search of electronic evidence. This transition from the tangible to the largely intangible realm is explored below.

2.2.1 *Computer data*

In contemporary computing, "data"[7] refers to information that has been translated into a form that is convenient to process. In respect of today's computers and transmission media, data is information converted into a digital form.[8] "Digital" refers to the use of a binary code to represent information.[9]

---

5 See, however, chapters 5 and 6 below for a comparative exposition with regard to the legislative frameworks of the United States and England respectively.

6 Browsing refers to moving from website to website by means of a software program used for viewing web pages. This process is also referred to as "surfing". See Byrne *I-Net Certification Study System* 422.

7 In its Latin origin, the word *datum* is technically the singular of *data*. Nowadays, however, the term "data" is commonly used and accepted in English as denoting both the singular and plural form of the word. See Shelly, Cashman and Vermaat *Discovering Computers* 5.03 [hereinafter referred to as Shelly *Discovering Computers 2003*].

8 Whatis.com search Storage.com Definitions "Data" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211894,00.html 1.

9 In telecommunications, data sometimes denotes digitally encoded information to distinguish it from analogue-encoded information such as conventional telephone voice calls. In general, an analogue transmission requires a dedicated continual connection for the duration of a related series of transmissions. Digital data transmission can often be sent with intermittent connections in "packets" that arrive in a piecemeal fashion. See Whatis.com searchStorage.com Definitions "Data" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211894,00.html 1. Digital data can only have certain discrete values (as opposed to analogue data, which can range over a continuity of values), but analogue data can, of course, be represented as digital data. See Google "Definitions of digital on the Web" found on the Internet http://www.google.com/search?hl=en&lr=&ie=ISO-8859-&q=define%3Adigital 1. By converting analogue data to binary data, Internet telephony, for example, allows users to converse over the WWW, just as if they were on a traditional telephone. This is also called Voice over Internet Protocol (IP), commonly referred to as VoIP. See Shelly *Discovering Computers* 1.12. VoIP is a classic example of the coming together and integration of formerly distinct technologies into a single delivery system. At present, one might receive information by telephone, on the television, via the radio, from a newspaper and in print. In future, these different information delivery systems may be replaced by a unified system based wholly on digital technology with all its advantages (such as ease of access and flexibility) and disadvantages (such as increased centralisation, homogeneity and control) that such a convergence model confers. The Electronic Communications Bill [B9B-2005] (hereinafter referred to as the Electronic Communications Bill) aims to promote convergence in the broadcasting, broadcasting signal distribution, and telecommunications sectors. It also aims to provide the South African legal framework for the convergence of these sectors. Its primary object is to provide for the regulation of electronic communications in South Africa in the public interest. It also sets out to promote and facilitate the development of interoperable and interconnected electronic networks, a technologically neutral licensing framework and the universal provision of electronic communications networks and electronic communications services and connectivity for all. See Google

All computer data is ultimately a series of zeros and ones and can therefore be represented as binary numbers.[10]

Binary data that has been broken down into the smallest unit that a computer is capable of representing and/or recognising is called a "bit" (derived from **b**inary dig**it**). A bit represents one of two values, on or off, since most computers are electronic devices powered by electricity, which also has only two states, on or off.[11] The digit zero represents the electronic state of off (the absence of an electronic charge). The digit one represents the electronic state of on (the presence of an electronic charge).[12] By itself, a bit is not very informative. When eight bits are grouped together as a unit, they form a "byte". A byte is informative because it provides enough different combinations of zeros and ones to represent 256 individual characters.[13] These characters include numbers, uppercase and lowercase letters of the alphabet, punctuation marks and other characters such as the letters of the Greek alphabet.[14] The combinations of ones and zeros that represent characters are defined by patterns called a coding system, which makes it possible for humans to interact with a digital computer that recognises only bits.[15] Two popular coding schemes are the American Standard Code for Information Exchange (ASCII) and the Extended Binary Coded Decimal Interchange Code (EBCDIC).[16]

Data that has not been processed for use is called "raw data", "source data" or "atomic data".[17] Data can be defined as a collection of raw unprocessed facts, figures and symbols, processed

---

"Definitions of Convergence on the Web" found on the Internet http://www.google.com/search?hl=en&lr=ie=UTF-8&oi=defmore&q=define:Convergence 2-4. Another innovative example of convergence is the Media Center Personal Computer (PC). Basically, a Media Center PC is an entertainment hub located in the living room, but it can also be used as a personal computer in the study or bedroom. It has all the functionality of a normal Windows XP computer, but features special integrated software which makes it easy to view using a television screen and to navigate with a remote control. See Van der Berg 2005 *SA Computer Magazine* 35. Also refer to paragraph 2.6.3 below for a discussion of the Internet and the WWW, which, of course, constitutes the revolutionary archetype of convergence.

10 Google "Definitions of binary" found on the Internet http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3Abinary 1. "Binary" is commonly used to indicate base 2, which can be described as the numerical representation in which each digit has an "alphabet" of only two symbols: 0 and 1. This binary value can also, for example, be represented (with the exact same value) as octal (base 8), decimal (base 10) or hexadecimal (base 16). Hex is often used as a short way of representing binary numbers. In hexadecimal notation, the decimal numbers zero through to 15 are represented by the decimal zero through to nine and the alphabet digits A through to F. Google "Definitions of hex on the Web" found on the Internet http://www.google.com/search?hl+en&lr+ie+ISO-8859-1&=define%3A=hex 1.

11 Shelly *Discovering Computers* 4.15.

12 Shelly *Discovering Computers* 4.15.

13 A kilobyte (KB/K) equals 1 024 bytes (often rounded off to 1000 bytes), which equals approximately half a page of text. A megabyte (MB) equals 1 048 576 bytes (often rounded off to 1 million bytes), which equals approximately 500 pages of text. A gigabyte (GB) equals 1 073 741 824 bytes (often rounded off to 1 billion bytes), which equals approximately 500 000 pages of text. A terabyte (TB) equals 1 099 511 627 776 bytes (often rounded off to 1 trillion bytes), which equals approximately 500 000 000 pages of text. See Shelly *Discovering Computers* 4.16.

14 Shelly *Discovering Computers* 4.15.

15 When a user presses a key on the keyboard, the electronic signal is converted into a binary form that the computer recognises, and it is stored in memory. Every character is converted to its corresponding byte, consisting of 8 bits. The computer then processes the data as bytes, which is actually a series of on and off electrical states. When processing is finished, software converts the bytes back into numbers, letters of the alphabet or special characters so that they can be displayed on a screen or be printed. See Shelly *Discovering Computers* 4.15.

16 Standards, such as ASCII and EBCDIC, make it possible for components within computers to communicate successfully with each other. ASCII is the coding system most widely used to represent data. Most personal computers and midrange servers use the ASCII coding scheme. The EBCDIC is used primarily on mainframe computers. The ASCII and EBCDIC coding schemes are sufficient for English and Western European languages, but are not large enough for Asian and other languages that use different alphabets. Unicode is a coding scheme capable of representing all the world's current languages. Shelly *Discovering Computers* 4.15.

17 Whatis.com SearchCIO.com Definitions "Raw data" found on the Internet http://searchcio.techtarget.com/sDefinition/0,,sid19_gci878172,00.html 1.

by a computer to create information. Data also includes sounds, images and video.[18] Data is a raw product that is useless in the absence of some sort of technological converter (such as a software program)[19] that places the data in a readable format, or at least provides an understanding of how the data was created and used.

Five broad categories of computer data can be distinguished:[20] active, online data,[21] near-line data,[22] offline storage/archives,[23] backup tapes[24] and erased, fragmented or damaged data.[25] Linked to this categorisation is the format and inertness of the data at the time when it is gathered. The data may be either static, recorded or stored, or fluid and in flux or movement.[26] "Real-time" has been defined as a level of computer responsiveness that a user senses as immediate[27] or that enables the computer to keep up with some external process.[28] A real-time information update essentially happens concurrently with the receiving of information and enables a process to be controlled.[29]

Meta-data, literally "data about data",[30] is a mode of data that has become important in computing contexts, especially on the World Wide Web (WWW), because of the need to sift useful information from the mass of information available.[31] The most common types of meta-

---

18 Shelly *Discovering Computers* 1.04.

19 A software program is the series of instructions that tells the hardware of the computer to process data into information. Shelly *Discovering Computers* 1.04. See paragraph 2.5.1.2 below for a discussion of software.

20 Volonino 2003 *Communications of the Association for Information Systems* 12.

21 Data that is typically stored on hard drives or active network servers, from where it is available for access as it is created and processed.

22 Data that is typically housed on removable media, such as optical disks or magnetic tape, used to store and retrieve records.

23 Data that is generally stored offline on tape or a removable computer storage medium traditionally used for disaster recovery or for data considered archival, in that the likelihood of retrieval is minimal.

24 Backup tapes usually consist of compressed data that is not organised for the retrieval of individual documents or files, because the organisation of the data mirrors the computer's structure and not the human records' management structure.

25 These types of data, although tagged for deletion by the user, may still exist somewhere on the free space of the computer until it is overwritten by new data.

26 See generally paragraph 2.4 below with regard to the importance of the format and inertness of the data at the time when it is gathered.

27 Real time describes a human sense of time rather than the machine's "sense of time".

28 Whatis.com searchSMB.com Definitions "Real time" found on the Internet http://searchsmb.techtarget.com/sDefinition/0,290660,sid44_gci214344,00.html 1.

29 Answers.com "Real-time" found on the Internet http://www.answers.com/topic/real-time-1?method=6 1.

30 Wikipedia "Metadata" http://en.wikipedia.org.wiki/Metadata 1. Although millions of articles, magazines and books spell this term as one word, "meta-data" with the hyphen is the correct spelling for the generic term, because the Metadata company (www.metadata.com) has trademarked the unhyphenated term as its name. Meta-data has existed for centuries. Card catalogues and handwritten indexes are examples from long before the electronic age. See Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&curtab=1512_1&linktext=meta-data 1.

31 If one webpage about a topic contains a word or phrase, then all webpages about that topic should contain the same word. For example, an article about sports utility vehicles (SUVs) would also be given the meta-data keywords "4 wheel drives", "4WD's", and "four wheel drives". These meta-tags are read by search engine spiders or robots, which makes it easier to search. See Byrne *I-Net Certification Study System* 426 and Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=metadata&curtab=1512_1&linktext=meta-data 2. Whereas meta-data is a definition or description of data, meta-language is a definition or description of language. The Extensible Markup Language (XML), which is comparable to the Standard Generalised Markup Language (SGML) and modelled on it, describes how to describe a collection of data. XML could be considered the meta-data for the more restrictive meta-data of, for example, Microsoft's Channel Definition Format (CDF) and other future data definitions based on XML. See Whatis.com SearchSQLServicer.com Definitions "Meta" found on the Internet http://searchsqlserver.techtarget.com/sDefinition/0,290660,sid87_gci212555,00.html 1. Van der Merwe discusses the "layer upon layer of exciting possibilities" that XML continues to reveal in both the areas of legal informatics (described as "the ways in which information technology assists the law") and informatics law (described as "the problems that the use of information technology pose to the law"). See Van der Merwe 2005 *THRHR* 70.

data are file system meta-data,[32] image meta-data,[33] program meta-data,[34] data warehouse meta-data[35] and relational database meta-data.[36] Law enforcement agencies often rely on meta-data for investigative purposes, because it presents a wealth of potential electronic evidence.

When one is harvesting electronic evidence, converting data into a usable product (in other words, information) could pose severe challenges. A distinction can be made between data and information: information is the end product of data processing. Raw data that has undergone processing is sometimes referred to as "cooked data". Although raw data has the potential to become information, it requires selective extraction, organisation and sometimes analysis and formatting for presentation.[37] "Information" is therefore a stimulus that has some meaning in a particular context for its receiver[38] and as such is organised, meaningful and useful.[39] In other words, information has exclusive meaning for human beings, as opposed to data, which is meant as instructions for a computer.[40] When information possesses probative value, it can become admissible as evidence in judicial proceedings.[41]

The procedural measures introduced in section 2 of the Cybercrime Convention in general refer to all types of data. Such data may exist in two forms, namely as stored data or data involved in a process of communication.[42] The applicability of a particular evidence collection procedure to a particular type or form of electronic data depends on the nature and form of the data and on the nature of the procedure, specifically described in each of the articles set out in the Cybercrime Convention that allows for the acquisition of that particular type of data.[43]

---

32 Examples range from simple timestamps, mode bits and other special-purpose information used by the implementation itself, to icons and free-text comments, to arbitrary attribute-value pairs. See Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&cur tab=1512_1&linktext=meta-data 2-4.

33 Such as image files containing meta-data. These include the Exchangeable Image File Format (EXIF) and the Tagged Image File Format (TIFF). See Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&cur lab=1512_1&linktext=meta-data 2-4.

34 Most executable file formats include meta-data describing issues that the runtime or operating system needs to consider when executing the program. Programs such as Microsoft Word and other Microsoft Office products save meta-data into the document files. This meta-data can contain information on the name of the person who created the file (obtained from the operating system), the name of the person who last edited the file, how many times the file has been printed and even how many revisions have been made on the file. See Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&cur tab=1512_1&linktext=meta-data 2-4.

35 Data warehouse meta-data include source system meta-data (source specifications such as repositories and source schemata, source descriptive information such as ownership descriptions, update frequencies, legal limitations and access methods; and process information such as job schedules and extraction code) and data staging meta-data (data acquisition information such as data transmission scheduling and results and file usage; dimension table management, such as definitions of dimensions and surrogate key assignments; transformation and aggregation such as data enhancement and mapping; and audit, job logs and documentation such as data lineage records and data transform logs). See Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&cur tab=1512_1&linktext=meta-data 2-4.

36 Each relational database system has its own mechanisms for storing meta-data, including tables of all the tables in a database, their names, sizes and the number of rows in each table; and the tables of columns in each database, what tables they are used in and the type of data stored in each column. See Answers.com "Metadata" http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&curtab=1512_1&linktext=meta-data 2-4.

37 Whatis.com SearchCIO.com Definitions "Raw data" found on the Internet http://searchcio.techtarget.com/sDefinition/0,,sid19_gci878172,00.html 1.

38 Whatis.com searchDatabase.com Definitions "Information" found on the Internet http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci212343,00.html 1.

39 Shelly *Discovering Computers* 1.04.

40 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 47.

41 See the discussion of electronic evidence in paragraph 2.3.1 below.

42 The Council of Europe's Explanatory Report to the Cybercrime Convention 24.

43 See paragraph 2.4 below for an exposition of the different types of evidence collection procedures involved.

Article 1(b) of the Cybercrime Convention defines "computer data" as[44]

> ... any representation of facts, information or concepts in a form suitable for processing in a computer system[45], including a program suitable to cause a computer system to perform a function.

This definition of computer data is built on the definition of data proposed by the International Standards Organisation (ISO) of the United Nations,[46] with specific reference to the terms "suitable for processing". The term "computer data", as introduced by the Cybercrime Convention, must be understood as data in an electronic form or in another directly processable form.[47] The electromagnetic emissions emitted by a computer during its operation are not considered data in terms of the definition in article 1 of the Cybercrime Convention. However, data can be reconstructed from such emissions.[48] Automatically processed computer data may either be the target of one of the criminal offences[49] defined in the Cybercrime Convention, or it may be the object of the application of one of the investigative measures[50] created by the Cybercrime Convention.

Section 1 of the Electronic Communications and Transaction Act defines data as "electronic representations of information in any form". The real currency of the Electronic

---

44 Although the parties to the Cybercrime Convention are not obliged to copy the four concepts (in other words computer system, computer data, service provider and traffic data) as defined in article 1 of the Cybercrime Convention *verbatim* into their domestic laws, it was understood that the domestic laws should cover such concepts in a manner consistent with the principles of the Convention and that an equivalent framework for its implementation should be offered. See the Council of Europe's Explanatory Report to the Cybercrime Convention 5.

45 See paragraph 2.5.1 below for a discussion of computer systems.

46 The International Standards Organisation (hereinafter referred to as ISO) was founded in 1946 and is a voluntary, non-treaty organisation that produces international standards. The members of the ISO are actually other organisations from 89 member countries. The ISO issues standards on a large number of subjects, ranging from data communications protocols to telephone pole coatings. The ISO has almost 200 technical committees, each dealing with a specific subject. Each committee has subcommittees that are themselves divided into working groups. Most of the real work is done in the working groups. Over 100 000 volunteers are usually assigned to work on ISO matters by companies whose products are affected by the standards being created. ISO standards are sometimes coordinated with recommendations of the International Telecommunications Union, Telecommunications Standards Sector (ITU-T) to avoid two incompatible international standards from arising. The ITU-T is an international organisation within which governments and the private sector coordinate global telecommunications networks and services. ITU-T activities include the coordination, development, regulation and standardization of telecommunications. See Nash *Networking Essentials MCSE Study Guide* 39. It must, however, be borne in mind that ISO definitions and standards are formulated and developed with regard to technology and commerce and cannot therefore be regarded as totally adequate to service the legal field. See, for example, the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 47, where reference is made to the ISO's definition of data. This is a similar, but not entirely identical, definition of data.

47 The Council of Europe's Explanatory Report to the Cybercrime Convention 6.

48 The Council of Europe's Explanatory Report to the Cybercrime Convention 6 and 12. The interception of data from electromagnetic emissions from a computer system is, consequently, included as an offence of illegal interception in terms of article 3 of the Cybercrime Convention.

49 The following offences are defined in the Cybercrime Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

50 The domestic investigative measures created by the Cybercrime Convention are the following: search and seizure of stored computer data; production orders; the expedited preservation of stored computer data; the expedited preservation and partial disclosure of traffic data; the real-time collection of traffic data; and the interception of content data. The transborder investigative measures proposed by the Cybercrime Convention are the following: the expedited preservation of stored computer data; the expedited disclosure of preserved traffic data; mutual assistance regarding the accessing of stored computer data; transborder access to stored computer data with consent or where publicly available; mutual assistance regarding the real-time collection of traffic data; and mutual assistance regarding the interception of content data. These procedural measures aimed at the search and seizure, production and preservation of computer data are elaborated upon in chapter 3 of this thesis.

Communications and Transactions Act is, however, "data messages", which are defined in section 1 as

> ...data generated, sent, received or stored by electronic means and [this] includes voice, where the voice is used in an automated transaction; and a stored record.

Computer data, for the purposes of this thesis, encompasses any electronic representation of information that is suitable for processing by a computer, including communications data (considered in more detail below).

2.2.1.1 Communications data: a special type of computer data

An "electronic communication" is defined in article 1 of the Electronic Communications and Transactions Act as "a communication by means of data messages". Section 1 of the Telecommunications Act[51] defines "telecommunication" as the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio or other electromagnetic waves, or any agency of a like nature, whether with or without the aid of tangible conductors.[52]

In general, the procedural measures introduced in article 2 of the Cybercrime Convention refer to all types of data. This includes three specific types of communications data, namely content data, traffic data and subscriber data. The latter may exist in two forms, namely stored or in the process of communication.[53] The RICPCIA uses the term "communication-related information" instead of "traffic data".

It is important to differentiate between different types of communications data, because the Cybercrime Convention and the RICPCIA introduce different legal regimes for each type of communications data. The applicability of a procedure to a particular type or form of data depends on the nature and form of the data and the nature of the procedure to be used. Accordingly, within a particular set of circumstances, any type of communications data may constitute the object of a search and seizure, production or preservation intervention.[54]

---

51 103 of 1996 (hereinafter referred to as the Telecommunications Act). The draft Electronic Communications Bill will repeal the whole of the Telecommunications Act. The Schedule to the Electronic Communications Bill also proposes certain changes to the RICPCIA. For the purposes of this research, the provisions of the RICPCIA are referred to as the RICPCIA stands. Where necessary, reference is made to differing provisions in the Electronic Communications Bill.

52 Section 1 of the Electronic Communications Bill defines "electronic communications" as "the emission, transmission, or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electromagnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service."

53 The Council of Europe's Explanatory Report to the Cybercrime Convention 24.

54 See paragraph 2.4 below for a discussion of the different types of procedural powers (interception and monitoring, search and seizure, production, preservation and retention) that may be directed against computer data, including the different categories of communications data.

The meanings of the terms content data, traffic data, real-time and archived communication-related information and subscriber information warrant further attention. They are therefore defined below.

2.2.1.1.1 Content data

"Content data" is not defined in the Cybercrime Convention. It is, however, generally understood to refer to the communication content of the communication. The communication content of a communication is the meaning or purport of the communication, or the message or information being conveyed by the communication.[55] It is everything that is transmitted as part of the communication that is not traffic data.[56]

Article 1(1) of the RICPCIA provides that the term "contents", when it is used in respect of any communication, includes any information concerning the substance, purport or meaning of that communication.[57]

2.2.1.1.2 Traffic data[58]

Computers generate traffic data in the chain of communication, in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself.[59] Article 1(d) of the Cybercrime Convention defines "traffic data" as

> ...any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Although not all categories of traffic data are always technically available, capable of being produced by a service provider or necessary for a particular criminal investigation, the definition

---

55 The Council of Europe's Explanatory Report to the Cybercrime Convention 40.

56 The Council of Europe's Explanatory Report to the Cybercrime Convention 45.

57 It is interesting to note that the definition of "content" contained in the draft Convergence Bill 3382 of 2003 was left out in the subsequent Electronic Communications Bill. Section 1 of the Convergence Bill defined content as any sound, text, still picture, moving picture or other audio-visual representation, sensory representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved and communicated electronically, but excludes content contained in private communications between consumers.

58 Traffic data is typically required to trace the source of a communication as a starting point for collecting further evidence proving an offence against a computer system. Traffic data might only be ephemeral, which makes it necessary to order its expeditious preservation. Its rapid disclosure may also be necessary to discern the communication's route in order to collect further evidence before it is deleted, or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. The collection of this data is regarded, in principle, to be less intrusive, since it does not reveal the content of the communication, which is regarded as more sensitive. See the Council of Europe's Explanatory Report to the Cybercrime Convention 7. See paragraphs 3.7 and 3.8 below for a discussion of the procedural mechanisms created in the Cybercrime Convention and specifically aimed at the domestic and transborder expedited preservation and collection of traffic data respectively.

59 The Council of Europe's Explanatory Report to the Cybercrime Convention 7.

of "traffic data" in the Cybercrime Convention exhaustively lists the categories of traffic data that are treated by a specific legal regime in the Cybercrime Convention. These categories are[60]

(a) the "origin", which refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services;

(b) the "destination", which refers to a comparable indication of a communications facility to which communications are transmitted; and

(c) the "type of underlying service", which refers to the type of service used within the network, for example, file transfer, [61] e-mail[62], or instant messaging (IM).[63]

The RICPCIA introduces the more detailed term "communication-related information". This term encompasses the Cybercrime Convention's concept of traffic data. Section 1(1) of the RICPCIA defines "communication-related information" as

> ...any information relating to an indirect communication[64] which is available in the records of a telecommunication service provider,[65] and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system.

The RICPCIA also discerns between archived and real-time communication-related information. "Archived communication-related information" is defined as

---

60 The Council of Europe's Explanatory Report to the Cybercrime Convention 7.

61 File transfer (FTP) is a service offered by the Internet that allows users to upload and download files with other computers on the Internet. Shelly *Discovering Computers* 1.09 and paragraph 2.6.3 below.

62 Electronic mail (email) refers to the transmission of messages and files to and from other computers via a computer network. See Shelly *Discovering Computers* 1.08 and paragraph 2.6.3 below.

63 IM is a real-time communications service that notifies a user when other users are online and then allows the user to exchange messages or files with them or to join a private chat room. See Shelly *Discovering Computers*. A chat room is a service that permits users to chat with each other in real time via a computer while they are connected to the Internet. Shelly *Discovering Computers* 1.11. See paragraph 2.6.3 below for a more detailed discussion of the services that the Internet offers.

64 Section 1(1) of the RICPCIA provides that a "communication" includes both a direct and an indirect communication. "Indirect communication" is defined in the said article as the transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds; data; text; visual images, whether animated or not; signals; or radio frequency spectrum; or in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system. "Direct communication" means an oral communication, other than an indirect communication, between two or more persons, which occurs in the immediate presence of all the persons participating in that communication. It also includes an utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication.

65 The definition of a "telecommunications service provider" in the RICPCIA is substituted by a definition of an "electronic communications service provider" in the Electronic Communications Bill. The definition of an electronic communications service provider includes an Internet service provider. The RICPCIA definition of an Internet service provider is substituted in the Electronic Communications Bill with the definition of "any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with an electronic communication service licence issued to the first-mentioned person under Chapter 3 of the Electronic Communications Act".

> ...any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30(1)(b) for the period determined in a directive referred to in section 30(2)(a), beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates.[66]

"Real-time communication-related information" is defined as

> ...communication-related information which is immediately available to a telecommunication service provider before, during, or for a period of 90 days after, the transmission of an indirect communication; and in a manner that allows the communication-related information to be associated with the indirect communication to which it relates.[67]

2.2.1.1.3 Subscriber information[68]

Subscriber information includes various types of information about the use of a service and the user of that service. Subscriber[69] information is defined in section 18(3) of the Cybercrime Convention as any information contained in the form of computer data or any other form[70] and held by a service provider relating to subscribers of its services, other than traffic data or content data, which can be used to establish

(a) the type of communication service used, the technical provisions[71] taken and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and

---

66 Section 1(1) of the RICPCIA. Interestingly, the concept of archived communication-related information appears in the unobtrusive reference to so-called "historical traffic data that may no longer be available or relevant due to a change in the route of communication" in the Council of Europe's Explanatory Report to the Cybercrime Convention. See the Council of Europe's Explanatory Report to the Cybercrime Convention 42.

67 Section 1(1) of the RICPCIA.

68 In the course of a criminal investigation, subscriber information may be required to identify which services and related technical measures have been used or are being used by a subscriber. This includes the type of telephone service used (for example, mobile services), the type(s) of other associated service used (for example, call forwarding and voicemail services), and the telephone number or other technical address (such as an email address). When a technical address is known, subscriber information may be required to assist law enforcement agencies in establishing the identity of the person concerned. Other subscriber information, such as commercial information about the billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes. The Council of Europe's Explanatory Report to the Cybercrime Convention 34.

69 The term "subscriber" is intended to include a broad range of service provider clients, from people who hold paid subscriptions, to ones paying on a "per use" basis, to ones receiving free services, including information concerning anyone entitled to use the subscriber's account. The Council of Europe's Explanatory Report to the Cybercrime Convention 34.

70 Subscriber information is frequently also contained in paper records. The Council of Europe's Explanatory Report to the Cybercrime Convention 34.

71 Technical provisions include all measures taken to enable a subscriber to enjoy the communications service offered. Such provisions include the provision and registration of communications equipment used by the subscriber (such as telephone devices, call centres or local area networks), as well as the reservation of a technical number or address (such as a telephone number, website address, email address or domain name). See the Council of Europe's Explanatory Report to the Cybercrime Convention 35. Each website has an Information Protocol (IP) address that consists of a series of numbers. Because it is difficult to navigate by using numbers, but easier to remember and type in a name, domain names emerged. Domain names are simply the text version of an IP address. There are two main features of the Internet in relation to which a domain name can be used, namely as an email address and as a web address. See Hiller and Cohen *Internet Law & Policy* 138.

(c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.[72]

Section 1 of the RICPCIA defines a "customer" as any person to whom a telecommunications service provider provides a telecommunications service; or who has entered into a contract with a telecommunications service provider for the provision of a telecommunications service, including a pre-paid telecommunications service.[73]

Chapter 7 of the RICPCIA details the duties of telecommunications service providers and customers. A telecommunications service provider may obtain any information that it deems necessary, for the purposes of the RICPCIA, from a person who enters into a contract with such a provider for the provision of a telecommunications service.[74] The procurement of a minimum threshold of information is obligatory. In the case of a natural person,[75] the following information must be obtained: full names, identity number, residential and business or postal address (whichever is applicable) and a certified photocopy of the person's identification document on which her photo, full names and identity number (whichever is applicable) appear.[76] In the case of a juristic person,[77] the following information must be obtained from the person representing that juristic person: full names, identity number, residential and postal address (whichever is applicable); the business name and address and, if registered as such in terms of any law, the registration number of the juristic person; a certified photocopy of the identification document on which the photo, full names and identity number (whichever is applicable) of the person representing the juristic person appear; and a certified photocopy of the business letterhead of, or other similar document relating to, the juristic person.[78] Telecommunications service providers must ensure that proper records are kept of the information.[79]

---

72 The reference to a service agreement or arrangement should be interpreted in a broad sense, to include any kind of relationship on the basis of which a client uses a provider's services. This information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment, on the basis of the information provided according to the service agreement or arrangement, can be critical to an investigation. See the Council of Europe's Explanatory Report to the Cybercrime Convention 35.

73 Section 1 of the Electronic Communications Bill defines a "subscriber" as a person who lawfully accesses, uses or receives a retail service of a licensee (referred to in chapter 3 of the Bill) for a fee or the retail services of a person providing a service pursuant to a licence exemption. "Subscriber equipment" is defined as any device which a subscriber uses to access, use or receive the services of a licensee (as referred to in chapter 3 of the Bill) or the services of a person providing a service pursuant to a licence exemption, including without limitation, a telephone, regardless of technology such as IP phones, mobile phones, publicly available phones; a handset, a computing device such as a personal digital assistant or a personal computer; a device for receiving a sound radio broadcasting service and a television; or other device or equipment and any associated software.

74 See the general provision in section 39(1)(c) and section 40(1)(c) of the RICPCIA, in respect of the selling or provisioning of cellular phones or Subscriber Identity Module (SIM-) cards. Section 1(1) of the RICPCIA defines a SIM-card as an independent, electronically activated device designed for use in conjunction with a cellular phone. A SIM-card enables the user of the cellular phone to transmit and receive indirect communications by providing access to telecommunications systems and it enables such telecommunication systems to identify the particular SIM and its installed information.

75 See the general provision in section 39(1)(a) and section 40(1)(a) of the RICPCIA, in respect of cellular phones or SIM-cards.

76 The telecommunications service provider must retain the certified photocopy of the identification document of the person. The photograph, full names and identity number, whichever is applicable, of the person must be verified with reference to her identification document.

77 See the general provision in section 39(1)(b) and section 40(1)(b) of the RICPCIA, in respect of cellular phones or SIM-cards.

78 The certified photocopies of both the business letterhead and the identification document of the person representing the juristic person must be retained by the telecommunications service provider. The photograph, full names and identity number,

2.3 The objective of search and seizure, production and preservation

Whereas computer data encompasses any binary representation of information that is suitable for processing by a computer, information is the organised, meaningful and useful end product of data processing. Information is converted into evidence when it becomes admissible as evidence in a court of law. Electronic evidence constitutes the ultimate objective of a search and seizure, production or preservation intervention directed at computing environments. The final objective of computer forensics is to collect and analyse computer evidence in such a way that it enables the successful admission of this evidence in a court of law.[80]

2.3.1 Electronic evidence

Broadly defined, electronic evidence is electronically stored information that can be used as evidence in any legal action.[81] This includes any information of probative value that is either stored or transmitted in a binary form, by means of, for example, cellular phones, digital fax machines, digital audio and digital video.[82] Electronic evidence, for the purposes of this thesis, is defined as probative binary data that is stored or transmitted by means of a computer system. The terms "electronic evidence", "digital evidence" and "*e*-evidence" are used interchangeably, as they all constitute binary evidence accrued from computing environments.

Generally, there are two types of electronic evidence, namely physical and logical electronic evidence. In many cases, both of these leave "bread crumbs" behind on a crime scene. Most computer criminals appear to reuse the same machinery and hard drives, and these constitute the physical evidence. Evidence that resides in log files, embedded in software, in memory or within the file system, is considered logical evidence. Along with the physical and logical evidence, there is a subclass of volatile and non-volatile information. Volatile information may only exist for a short time or may disappear. Volatile evidence is often the most useful for making a case, but it is also the most difficult to preserve and collect, sometimes at the expense of other information or all the evidence contained on the device itself.[83]

---

whichever is applicable, of such a person must be verified with reference to her identification document. The name and registration number of the juristic person must be verified with reference to its business letterhead or other similar document.

79 Including all of the relevant certified photocopies and, where applicable, any change in such information which is brought to its attention; the telephone/cellular number of any other number allocated to the person concerned and any other information in respect of the person concerned which the telecommunications service provider concerned may require in order to enable the provider to identify that person. See the general provision in section 39(2) and section 40(2) of the RICPCIA, in respect of cellular phones or SIM-cards.

80 Casey *Handbook of Computer Crime Investigation* 69.

81 Volonino *Communications of the Association for Information Systems* 7.

82 See Whitcomb 2002 *International Journal of Digital Evidence* 4.

83 In some cases, volatile evidence may demonstrate an active network connection that is not contained in a *config* (configuration) file or in the logging. It may also result in information collected from the contents of volatile memory. See Rittinghouse and Hancock *Cybersecurity Operations Handbook* 389.

Although the emphasis in this research is on the legal procedures designed to collect electronic evidence and not on electronic evidence *per se*, it is useful to briefly consider the admissibility and weight of electronic evidence. Criminal procedural laws in most countries recognise, either explicitly or implicitly, that electronic data can qualify as evidence in criminal proceedings. There are, however, significant differences as to its evidentiary value and presentation. The fundamental issue that all criminal procedural laws and/or laws of evidence have to address is the admissibility and reliability of such evidence.[84] In most jurisdictions, data is considered to be a special written form of evidence.[85]

The Cybercrime Convention explicitly facilitates the collection of evidence of any criminal offence in electronic form. The Convention does not confine the application of its proposed collection procedures only to the offences established in section 1 of the Cybercrime Convention and other criminal offences committed by means of a computer system.[86] In terms of principle 13 of the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), the common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international cooperation, must be recognised. All procedures and technical methods for handling electronic evidence must be developed in an internationally compatible way. Criminal procedural law provisions on evidence relating to traditional documents must also apply to computer data.[87]

Similarly, in terms of principle 4 of the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), the provisions in the criminal procedural law relating to the search and seizure of documents must apply equally to automatically processed data, which is considered the functional equivalent to a traditional document. Computer data, in this context, can be viewed as both an equivalent means of a seizable document, and as an equivalent means of evidence.[88]

In the South African legislative framework, chapter III of the Electronic Communications and Transactions Act deals with the facilitation of electronic transactions. Sections 11 to 20 deal specifically with the legal requirements for the admission of data messages as evidence in court proceedings. The efficacy of these provisions has yet to be tested in court, but they are

---

84 Common law countries generally require the authentication of documents to ensure that they are genuine. Civil law countries, which in principle adopt the system of free presentation and free evaluation of evidence before the Court may also require authentication, in particular when the evidence is generated by information technology. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 32.

85 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 31.

86 Article 14(2) of the Cybercrime Convention.

87 The Council of Europe's Recommendation 1995(13) concerning Problems of Criminal Procedural Law connected with Information Technology 2.

88 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) concerning Problems of Criminal Procedural Law connected with Information Technology 17.

considered a vast improvement on the former muddled state of affairs. It is anticipated that the provisions will allow for a more equitable approach to computer-generated evidence in both civil and criminal proceedings than was possible before.[89]

Section 15 of the Electronic Communications and Transactions Act provides for the admissibility and evidential weight of data messages. It states that the rules of evidence in any legal proceedings must not be applied so as to deny the admissibility of a data message in evidence on the mere grounds that it is either constituted by a data message or not in its original form, if a data message is the best evidence that the person adducing it could reasonably be expected to obtain.[90] It also states that information in the form of a data message must be given due evidential weight.[91] Evidential weight must be assessed by considering

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.[92]

2.3.1.1 Mining forensic gold in search of electronic evidence

Electronic evidence is different from paper-based documentary evidence in a number of ways. Computer evidence is more fragile than paper documentation. A copy of a document stored in a computer file is identical to the original. Other valuable information, such as the time and date of origin and the author's name, may be embedded in the electronic version of a document. Comparisons of computer backups to existing documents can be used to show that a critical document has been altered and when the event occurred. In the case of email, casual and candid correspondence may be "frozen in time, like insects in amber."[93] Electronic documents

---

89 South African courts struggled to classify satisfactorily the products of modern technology as real evidence, documentary evidence or a *sui generis* type of evidence. In *S v Mpumlo* 1986 (3) SA 485 (E) and *S v Baleka* (1) 1986 (4) SA 192 (T), for example, it was decided that video- and audiotapes should be treated as real evidence. However, in *S v Singh* 1975(1) SA 330 (N) and *S v Ramgobin* 1986 (4) SA 117 (N), it was decided that tapes should be treated as documentary evidence. The contentious Computer Evidence Act 57 of 1983 arose directly from the case of *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A) and was confined to civil cases. The Electronic Communications and Transactions Act repealed this piece of legislation and brought about much-needed legal certainty in respect of the admissibility of electronic evidence. See Schwikkard and Van der Merwe *Principles of Evidence* 379-387 and Zeffert, Paizes and Skeen *The South African Law of Evidence* 699-712.

90 Article 15(1) of the Electronic Communications and Transactions Act 25 of 2002.

91 Article 15(2) of the Electronic Communications and Transactions Act 25 of 2002.

92 Article 15(3) of the Electronic Communications and Transactions Act 25 of 2002. Section 15(4) furthermore creates a rebuttable presumption that the facts contained in a business document are correct once a business document is certified to be correct. This provision contains the co-called "shopbook exception" that was inherited from English law. Section 15(4) does not appear in the UNCITRAL Model Law on Electronic Commerce, on which section 15 of the Electronic Communications and Transactions Act was based. See the UNCITRAL "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 *bis* as adopted in 1998" found on the Internet http://www.uncitral.org/pdf/english/text/electom/05-89450_Ebook.pdf.

93 Feldman "The essentials of Computer Discovery" found on the Internet http://www.forensics.com/pdf/Essentials_of_Discovery.pdf 1.

thought to be lost or destroyed can be recovered. Deleted file information has been analogised with a fossil, that may miss a bone here or there, but the fossil remains unchanged until it is completely overwritten. One of the challenges of what has been termed electronic "dumpster diving" is accordingly to recover information that has been partially destroyed and to make sense of the discovered "digital trash".[94]

The most prevalent types of electronic evidence are mined from data files, email and background information. The latter includes, for example, non-printing information;[95] access control lists that limit the rights of users to access, view and edit files; and audit trails and computer logs that leave an electronic trail regarding, *inter alia,* network and computer usage.[96] Data files can be divided into four basic categories, namely active data,[97] replicant data,[98] backup data and residual data.[99] Backup data provides a historical snapshot of the data stored on the system on the particular day the backup was made. Residual data is data that appears to be gone, but is still recoverable from the computer system.[100]

Electronic evidence encapsulated in computer records containing text are often divided into two categories, namely computer-generated records and computer-stored records. The difference hinges upon whether a person or a machine created the record's contents. Computer-stored records refer to documents that contain the writings of some person or persons and that happen to be in electronic form, including email messages, word processing files and Internet chat room messages. By contrast, computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records and ATM receipts are all computer-generated records.[101]

Like any other evidence, electronic evidence must be authentic, accurate, complete, convincing and admissible in conformity with the common law and legislative dictates. This form of evidence, however, poses special problems in that computer data changes moment by moment. These changes could be invisible to the human eye, as it can only be viewed indirectly after appropriate procedures have been followed. Furthermore, the very process of collecting

---

94 Farmer and Venema *Forensic Discovery* 12.

95 Such as the date and time stamp that the operating system puts on every file, revisions of documents and hidden comments.

96 Such as who was on the system, when, where and how long a user was on the system and information pertaining to the programs used, the files accessed, email sent and received and websites visited. Feldman "The essentials of Computer Discovery" found on the Internet http://www.forensics.com/pdf/Essentials_of_Discovery.pdf 5.

97 Readily available and accessible to users.

98 Such as automatically backed-up file clones.

99 Feldman "The essentials of computer discovery" found on the Internet http://www.forensics.com/pdf/Essentials_of_Discovery.pdf 3-4.

100 Such as deleted files that are still extant on a disk surface and data existing in other system hardware, such as buffer memories of printers, copiers and fax machines. Feldman "The essentials of computer discovery" found on the Internet http://www.forensics.com/pdf/Essentials_of_Discovery.pdf 4.

101 CCIPS found on the Internet http://www.cybercrime.gov/searchmanual.htm 101.

computer data may change it in significant ways. The processes of opening a file or printing it out are, for example, not always neutral.[102]

The collection of stored intangible data therefore requires additional measures to maintain its integrity.[103] Data which is copied or removed must be retained in the state in which it was found at the time of its collection and it must remain unchanged during the time that the criminal proceedings take. Law enforcement agents must provide adequate safeguards to guarantee the integrity of the relevant data between its acquisition during the investigation and its presentation at the court proceedings.[104] These safeguarding measures must include keeping track of all the measures that have been taken in handling the data or to prevent its unauthorised use. These measures of ensuring the reliability of electronic evidence, by default, have consequences for powers to collect electronic evidence or the ways in which those powers are executed.

Electronic evidence used to mean a regular print-out from a computer. Many computer exhibits in court are just that. However, for many years now, law enforcement officers have been seizing the ever smaller and ubiquitous actual data media and computers. Then law enforcement officers began to generate their own printouts, sometimes using the original application program, sometimes using specialist analytical and examination tools. Recently, investigators have found ways of collecting evidence from remote computers to which they do not have immediate physical access, provided such computers are accessible via a phone line or network connection. It is even possible to track activities across a computer network, including the Internet. These processes of methodically examining computer media for evidence form part of what is called computer forensics.[105] Although this research focuses on the legal procedures by means of which electronic evidence can be collected, the legalities cannot be elegantly divorced from the technicalities associated with the unearthing of such *e*-evidence. A broad understanding of the technical procedures utilised to collect electronic evidence is accordingly called for and is therefore provided below.

In the early days of forensic computing, before imaging[106] was widely available, most recovered electronic evidence was in the form of copied files or raw sectors. When imaging became the

---

102 See also paragraph 1.1 above in respect of the impact of the unique nature of electronic evidence on the legal collection procedures. Vacca *Computer Forensics: Computer Crime Scene Investigation* 19.

103 The Council of Europe's Explanatory Report to the Cybercrime Convention 38. Data integrity can also mean the degree to which data is correct. The more errors the data contains, the less its integrity. The GIGO (garbage in, garbage out) principle means that correct information cannot be created from data that is incorrect. Shelly *Discovering Computers* 13.03. This type of data integrity must be distinguished from the integrity of data in the context referred to here.

104 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) concerning Problems of Criminal Procedural Law connected with Information Technology 33.

105 Also referred to, *inter alia,* as cyberforensics, digital forensics, computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis and computer examination. Vacca *Computer Forensics: Computer Crime Scene Investigation* 3.

106 See footnote 128 and paragraph 2.3.1.2.1 below for an explanation of imaging process.

norm, the use of copying decreased. Imaging is commonly acknowledged to be the better solution as it enhances the continuity and integrity of the electronic evidence that has been found. However, copying does have some advantages over imaging. Some of these advantages include the following: copies can be viewed immediately; copying can be used when convenient or expedient or to recover evidence from unusual machines or evidence which is not suitable for imaging; there are no special equipment or software requirements; it carries no additional costs; little training is required and it applies to files only.[107]

2.3.1.2 Computer forensics: a means to an end

The word "forensic" is defined in the *Oxford English Dictionary* as an adjective meaning "used in, or connected with a court of law". The term forensic science is defined as a "science that deals with the relation and application of scientific facts to legal problems". Traditionally, forensic science has centred on the physical and applied sciences, such as medicine, engineering, chemistry and ballistics. However, more recently, social sciences, such as psychology and accounting,[108] have been added to the forensic science armoury. The extension of forensic science now called computer forensics is, in essence, concerned with the unearthing of evidence from computer media in order to support legal proceedings.[109]

Although the field is relatively new to the private sector, it has been the mainstay of technology-related investigations in law enforcement and military agencies since the mid-1980s.[110] Computer forensic methods may, however, not be afforded the luxury of time in which to establish themselves, or the longevity that more traditional chemistry- and physics-based forensics enjoys, as newness and obsolescence is the norm in computing contexts.[111] So, for

---

107 Sammes and Jenkinson *Forensic Computing: A Practitioner's Guide* 195.

108 These social science extensions of forensic science have a dominant requirement for interpretative and judgmental skills, rather than the detection of physical evidence. Carr and Williams (eds) *Computers and Law* 146.

109 Carr and Williams (eds) *Computers and Law* 146.

110 Vacca *Computer Forensics: Computer Crime Scene Investigation* 795. See also footnote 19 and paragraph 1.1 above in respect of the cyberforensic capability of law enforcement agencies vis-à-vis the capability of private organisations.

111 Vacca *Computer Forensics: Computer Crime Scene Investigation* 237. This may have contributed to the fact that electronic evidence has not fared all that well under the rigorous standards of admissibility of scientific evidence in the USA. The scientific evidence standards recognised in the USA are the Relevancy Test embodied in the Federal Rules of Evidence 401, 402 and 403 and, in some states, versions thereof that allow anything that materially assists the trier of fact to be deemed relevant by the trier of the law; the Frye standard (*Frye v US* 293 F 1013 (DC Ct App 1923) or the General Acceptance Test that requires that, for the results of a scientific technique to be admissible, the technique must be sufficiently established to have gained general acceptance in its particular field; the Coppolino Standard (*Coppolino v State* 223 So 2d 68 (FLA Dist Ct App 1968), in terms of which the Court allows a novel test or piece of new, sometimes controversial, science to be applied on a particular problem if an adequate foundation can be laid, even if the profession as a whole is not familiar with it; the Marx Standard (*People v Marx* 54 126 Cal Rptr 350 (1975) or the Common Sense/No Scientific Jargon Test, which requires the Court to be satisfied that it did not have to sacrifice its common sense in order to understand and evaluate the scientific expert evidence put before it; the Daubert Standard (*Daubert v Merrell Dow Pharmaceuticals* 509 US 579 (1993)), which is a rigorous test that requires special pre-trial hearings for scientific evidence and special procedures on discovery where the rules are laid out beforehand on validity, reliability, benchmarking, algorithms and error rates. See Vacca *Computer Forensics: Computer Crime Scene Investigation* 24. The four factors applied to determine the reliability of scientific techniques as set out in *Daubert v Merrell Dow Pharmaceuticals* 509 US 579 (1993) are as follows: (a) Has the scientific theory or technique been empirically tested? (b) Has the scientific theory or technique been subjected to peer review and publication? (c) Is there a known or potential error rate and do standards exist that control the technique's operation? (d) Is there a general acceptance of the methodology or technique in the relevant scientific community? During a more recent case, *Kumho Tire Co et al v Carmichael et al* 526 US 137 (1999), the Court found that the tests set out in the *Daubert v Merrell Dow Pharmaceuticals* 509 US 579 (1993) standard were insufficient for testing cases where the methodology was not based on the application of scientific principles. Although these methods were no less valid, the law did not make provision for accounting for this type of

example, as lawyers have educated themselves about the DNA analysis procedure, so challenges to the production of DNA-based evidence have become more widespread and the courts' attention has been directed to the flaws and weaknesses in the process. Similarly, with digital evidence, as lawyers become more aware of the possibilities for improper modification outside the audit systems, more appropriate challenges can be mounted and the courts can assess these dangers.[112]

Computer forensics deals with the preservation, identification, extraction and documentation of computer evidence. Computer forensics is, first and foremost, concerned with forensic procedures, rules of evidence and legal concepts, precedents and processes. Only in the second place is it concerned with computers.[113] The objective in computer forensics is quite simply to recover, analyse and present computer-based material in such a way that it is usable as evidence in a court of law. It is essential that none of the equipment or procedures used during the examination of the computer obviate this objective.[114] Like any other forensic science, computer forensics involves the use of sophisticated technology, tools and procedures which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer-evidence processing.[115] These tools and procedures are briefly considered below.

2.3.1.2.1 Methodology is the key

Computer forensics is one of the most adversarial occupations in information technology. Every aspect of the technical competency and methods of the computer forensic specialist is scrutinised to its very core. Hence, it is imperative for such a specialist to use a deterministic, repeatable process that is clear, concise and simple. Adherence to this process is a forensic examiner's greatest asset and may become her lifeline in court. A defined, proven process incorporates the following elements: the cross-validation of findings with multiple toolsets; proper evidence handling and the safeguarding of the evidential chain of custody;[116] the

---

analysis. The Court came up with additional tests to address these deficiencies: (a) Has the technique been created for a purpose other than litigation? (b) Does the expert sufficiently explain important empirical data? (c) Is the technique based on qualitatively sufficient data? (d) Is there a measure of consistency in the technique's process or methods? (e) Is there a measure of consistency in the technique's process or methods as applied to the current case? (f) Is the technique represented in a body of literature? (g) Does the expert possess adequate credentials in the field? (h) How did the technique used differ from similar approaches? These factors are not hard and fast rules governing the admissibility of scientific or expert testimony, but were developed to assist practitioners in recognising factors that contribute to relevance and reliability. When collecting electronic evidence, it is helpful to keep these questions in mind. See Prosise and Mandia *Incident Response & Computer Forensics* 156.

112 Plowden and Stockdale 1998 *New Law Journal* 432.

113 In contrast to all other areas of computing, where speed is the main concern, in computer forensics the absolute priority is therefore accuracy. Vacca *Computer Forensics: Computer Crime Scene Investigation* 6. See also Davis, Philipp and Cowen, *Hacking Exposed Computer Forensics Secrets & Solutions* 6.

114 Vacca *Computer Forensics: Computer Crime Scene Investigation* 6.

115 Vacca *Computer Forensics: Computer Crime Scene Investigation* 795.

116 The chain of custody involves detailed documentation of the collection, safeguarding and analysis of evidence. Keeping records of who accesses evidence, when they access the evidence and what they do with it helps to refute evidence injection arguments that the opposing counsel may make during litigation. See Kruse and Heiser *Computer Forensics* 315. In Harris *CISSP Certification* 674, the chain of custody is defined as a history that shows how evidence has been collected, analysed, transported and preserved in order to be presented as evidence in court. The chain of custody has a considerable impact on

completeness of the investigation so that no single piece of relevant evidence remains undetected; the management of archives; technical competency; the explicit definition of and a justification of the process; the conducting of the investigation in a manner that allows a forensic specialist to retrace every step in the process; legal compliance and flexibility. These elements make all the difference between an effective, expedient investigation and playing around with a neat piece of software.[117]

Computer forensic procedures involve the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis. The basic methodology consists of what Kruse and Heiser[118] describe as the "AAA of Computer Forensics", namely the acquisition of evidence without altering or damaging the original, the authentication that the recovered evidence is the same as the originally seized data and analysis of the data without modifying it. A more comprehensive methodology is the one designed by Andrew Rosen (the CEO of ASR Data), called the "Six A's of Computer Forensics".[119] This process has been tested in both legal and technical aspects and is flexible enough to handle the diverse requirements posed by the investigation.

The steps in the process entail the assessment,[120] acquisition,[121] authentication,[122] analysis,[123] articulation and archival of electronic evidence.

---

the evidential weight and/or admissibility of electronic evidence. It must be shown that the evidence presented in court is exactly the same as the evidence that existed when the evidence was collected. This is mainly achieved by means of different cryptographic hashing functions. The "hash-value" can best be described as a digital fingerprint. See Earnshaw 2003 *C & L Computer Forensics* 12. These algorithms act like fingerprints, allowing the prosecution to show mathematically that the evidence is the same when it is heard in court as the day when the investigator collected it. A "hash" is a mathematical algorithm that creates a unique number/hash. A hash of the original data in its pristine state must be created before the image is made. Immediately after the imaging, another hash must be created. These two hashes must match. The chosen hashing algorithm must be sufficiently secure. A simple checksum is too easy to spoof (replicate) for evidence verification. The most commonly used hashing algorithms are MD5 and SHA-1. The likelihood of getting the same hash for two different pieces of evidence is statistically almost impossible. The hash is recorded and later compared to a new hash created on the same evidence. Hashing is probably the single strongest tool with which to establish authentication. See Kuchta 2002 *Information Systems Security* 46. See also footnote 122 below.

117 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 10.

118 See Kruse and Heiser *Computer Forensics* 1 and 3.

119 See Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 13.

120 The assessment phase details the steps to be taken in determining a course of action when presented with a computer forensic assignment. First, the scope of the investigation and the approximate quantity of the data must be determined. Second, the repositories of data that could potentially hold evidence and the tools with which to engage that data need to be identified. The third step involves the protection and preservation of the identified data. Fourth, a chain of custody that logs every attempt to access and interpret the data must be established. Finally, the data must be previewed in a manner that guarantees that it is not changed. See Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 13.

121 During the acquisition phase, a forensic copy of the data is created for the purposes of investigation and interpretation. Only forensically approved tools may be used as standard interfaces, because other tools, such as Windows Explorer, can cause inadvertent modifications to, for example, the metadata. Broadly speaking, the acquisition phase of the process involves identifying the source and destination media, selecting the acquisition parameters and creating the image. See Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 13.

122 The purpose of the authentication phase is to determine whether the image is identical to the original data. Authentication entails, first, physical control of access to the evidence by, *inter alia*, limiting the number of people with access to the evidence, evidence lockers and safes with dual control and an evidence log that recounts who had access to the evidence. Second, authentication requires digital documentation that makes it possible to identify the original evidence. The most common way of accomplishing this is to use an application to create a hash of the evidence at the time when the evidence is collected. See footnote 116 above in this respect.

123 Analysis constitutes the "meat" of the investigation. The key criterion to bear in mind when conducting an analysis is completeness. Every virtual nook and cranny needs to be checked out and it is of cardinal importance not to miss any relevant evidence. See Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 13.

An important feature of computer forensics is that it has changed the legal best evidence rule in respect of the processing of *e*-evidence.[124] The best evidence rule has in recent years seen the growth of a standard known as representational accuracy, which means that it is unnecessary to present the originals. If data stored by on a computer or similar device, any printout or other output readable by sight is shown to reflect the data accurately, it is considered an original.[125] The concept of representational accuracy allows investigators to gather forensic duplicates,[126] qualified forensic duplicates,[127] mirror images[128] and, to some extent, logical copies of the computer and data storage systems involved. A logical copy is used to refer to the act of copying discrete files from the logical file system onto media during the collection process.[129] If at all possible, it is prudent to safeguard the original evidence media as they constitute the ultimate control samples of the forensic process.

2.3.1.2.2 Tools of the trade

Typically, computer forensic tools exist in the form of computer software.[130] Computer forensic specialists guarantee accuracy of evidence-processing results by using multiple forensic tools developed by separate and independent developers. It is important to use different tools that have been developed independently to validate results so as to avoid inaccuracies introduced by potential software design flaws and software bugs. Cross-validations using multiple tools and techniques are standard in all forensic sciences. Validation using multiple software tools, different computer specialists and alternative procedures eliminates the potential for errors and the destruction of evidence. When this procedure is not used, it creates advantages for defence lawyers who may challenge the accuracy of the software tool used and thus the integrity of the results.[131]

(a) The EnCase Forensic Edition, developed by Guidance Software,[132] contains a large suite of tools based on the requirements of law enforcement, government and

---

124 Vacca *Computer Forensics: Computer Crime Scene Investigation* 795.

125 Vacca *Computer Forensics: Computer Crime Scene Investigation* 237.

126 A forensic duplicate is a file that contains every bit of information from the source, in a raw bitstream format. A 5 GB hard drive would result in a 5 GB forensic duplicate. Tools used to create a forensic duplicate are the Unix dd command and the open source Open Data Duplicator. Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 153.

127 A qualified forensic duplicate is a file that contains every bit of information from the source, but may be stored in an altered form, such as in in-band hashes and empty sector compression. Tools that create qualified forensic duplicate output files are SafeBack and EnCase. Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 153.

128 A mirror image is created from hardware that does a bit-for-bit copy from one hard drive to another. Hardware solutions are very fast. Mirror imaging introduces an extra step in the forensic process, requiring the examiner to create a working copy in a forensically sound manner. Mirror image backups replicate all the sectors on a given storage device exactly. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as "evidence grade backups" and they differ substantially from standard file backups and network server backups. If it is possible to keep the original drive seized from the computer system that is being investigated, working copies can be easily made. If the original drive must be returned or may never be taken offsite, the analyst is still required to create a working copy of the mirror image for analysis. Examples of hardware duplicators are Logicube's Forensic SF-5000 and Intelligent Computer Solutions' Image MASSter Solo-2 Professional Plus. See Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 154 and Vacca *Computer Forensics: Computer Crime Scene Investigation* 808.

129 Prosise and Mandia *Incident Response & Computer Forensics* 152.

130 See paragraph 2.5.1.2 below for a discussion of computer software.

131 Vacca *Computer Forensics: Computer Crime Scene Investigation* 795.

132 See http://www.guidancesoftware.com.

corporations, spanning seven years. One of the strongest features of EnCase is its repeated industry and court validation and deep analysis capabilities. The EnCase Enterprise Edition greatly extends the capabilities of the EnCase Forensic Edition technology. Its secure network-enabled capability gives corporate and government investigators the ability to respond immediately and centrally to security breaches and to conduct proactive and reactive investigations. One of the key features of the EnCase Enterprise Edition is its ability to investigate a machine thoroughly without having to bring it offline, potentially disrupting business. The EnCase Enterprise Edition also has a feature called Snapshot, which quickly captures volatile data.

(b) Other examples of forensic toolkits are ASR Data,[133] Paraben,[134] Access Data,[135] The Sleuth Kit[136] and New Technology Incorporated (NTI).[137]

2.3.1.3 Anti-Forensics: another one bytes the rust[138]

An anti-forensic technique is any intentional or accidental changing of data that can obscure the data, encrypt it or hide it from forensic tools. As most contemporary forensic examination tools tend not to trust data, the concepts discussed below do not necessarily affect the efficiency of modern forensic tools.[139] However, it is necessary to be familiar with these concepts, as they may become relevant during the course of an investigation or legal proceedings. Two of the most prevalent anti-forensic techniques, namely obscurity methods and privacy measures, are explored below.

2.3.1.3.1 Obscurity methods

An obscurity method is a method by which the true nature or meaning of some data is obscured. Data is typically obscured when the name or contents of a file is changed either intentionally or accidentally, resulting in a file that could be misinterpreted or disregarded in subsequent forensic analysis. File extension renaming can be countered by file signaturing in that some unique aspect of the file is compared to a database of signatures that relate to an extension. Several forensic tools can be used to determine a file's signature. EnCase, for example, has the ability to detect file types and carry out file signature analysis to detect modified file types.[140]

---

133 See http://asrdata.com/SMART.

134 Tools in the Paraben suite include the E-mail Examiner, Network E-mail Examiner, Decryption Collection, PDA seizure, Cell Seizure and NetAnalysis See http://www.paraben-forensics.com.

135 Tools in the Access Data suite include Forensic Toolkit and Password Recovery Toolkit. See http://accessdata.com.

136 The Sleuth Kit and Autopsy Browser are tools in The Sleuth Kit suite. See http://www.sleuthkit.org.

137 NTI offers a get-freespace program, a get-slack program and a file-list program that has the option of creating an MD5 hash for every file on the system and a program that outputs the partition table. See Prosise and Mandia *Incident Response & Computer Forensics* 302.

138 "Rust" is the coating on magnetic computer storage media. See paragraph 2.5.1.1 below for a reference to "rust" in a computing context.

139 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 168.

140 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 169.

Encoding is an obscurity method that changes a file's content in some way that can be easily reversed. A simple encoding mechanism is ROT-13, which rotates the characters 13 times. Such encoding can be detected by using ROT-13 decoders.[141]

Compression obscurity methods allow a file's contents to be reduced in size for storage and transmission. Although it is not difficult to detect compressed files, most forensic tools do not allow direct access to compressed data during a search. FTK and EnCase both allow for searching data without virtually uncompressing the data. SMART and other systems require such files to be exported out of the image, decompressed and then searched using separate tools.[142]

Data stored in slack space, unallocated space and free space may not be detected if an attempt is made to search a disk using non-forensic utilities. Operating systems arrange all data stored on a hard drive into segments called allocation units or clusters.[143] Unallocated space is the area of the hard drive not currently allocated to a file. Fragments of deleted files are often strewn across unallocated space on a hard drive.[144] Free space is the portion of the hard drive media that is not within any currently active partitions.[145] Slack space is a remnant of data that exists within a sector of data that has been overwritten. Specifically, slack space is the area of the sector that was not fully overwritten by a recent write to disk.[146]

2.3.1.3.2 Privacy measures

Some of the recognised anti-forensic techniques, such as encryption, steganography, evidence eliminators and disk wiping, are legitimate attempts to protect the privacy of the individual. It is, however, necessary to be able to identify and access such protected data during the course of a forensic examination.

Wiping is a real problem when it is done correctly, as any data that has been truly wiped from the disk has been overwritten at least once. Current software tools do not provide access to any data that has been overwritten. However, the data can be recovered by using an electron microscope to find the previous state of all the electrons on the disk, thus restoring the wiped information. This is an expensive and labour-intensive process; and very few forensic examiners have access to an electron microscope for analysis purposes. It is possible to determine whether wiping tools have been installed by reviewing the programs that exist and

---

141 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 172.
142 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 173.
143 See also footnote 336 in paragraph 2.5.1.2.2. below for a reference to clusters and units.
144 Kruse and Heiser *Computer Forensics* 75.
145 Prosise and Mandia *Incident Response & Computer Forensics* 275.
146 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 174. Vacca *Computer Forensics: Computer Crime Scene Investigation* 800.

have existed on the disk. If the disk was received during the course of an investigation, legal sanctions may be filed against the person responsible for the wiping or the person may be ordered to produce any other data that may exist. Whether or not a preservation order exists in respect of such data, an opposing party is likely to be ordered to produce further evidence if it can be proved that some of the data that was provided was wiped.[147]

Other than wiping, encryption is the only true anti-forensic method that can defeat the forensic analysis of data. Cryptography is the art of secret writing and comprises a science of codes and ciphers that can be used to conceal the contents of a message. It transforms messages into unintelligible forms in order to hide its content, establish its authenticity and prevent undetected modification. Cryptography largely falls into two camps, namely symmetric or secret key cryptography and asymmetric or public key cryptography. The main difference between the two types of cryptography is that symmetric or secret key cryptography uses the same single key to both encrypt and decrypt, whilst asymmetric or public key cryptography uses one key to encrypt and another one to decrypt.[148] Symmetric key encryption is only as strong as its key length and its ability to keep others from finding the key itself. Asymmetric key encryption is stronger than symmetric encryption, because not only does the length of the key protect it, but the private key that is used to decrypt the data must be found before the data can be accessed. Having the public key used to encrypt the data will not allow access to the original data. If data is encrypted, it is not possible to analyse or search its contents directly. Another method of identifying and accessing the data must then be found. Encrypted data is identified in two ways: either the file has an extension that is used by an encryption program to identify its files or it can be detected by means of a process known as entropy testing.[149]

However, even encryption has its weaknesses, depending on the type used.[150] For data to be encrypted, it must first exist on the disk in its unencrypted form. Although it is possible for someone to download a document in memory and encrypt it in memory before the data even touches the disk, this is very rare, except in the case of email. Instead, most people choose to encrypt a file that already exists on a disk. This means the data could still be stored at three locations: in the original file on the disk if it is still present, in the contents of the deleted file in the unallocated and slack space, or in the original file in the swap or pagefile.[151] If data cannot be accessed in this way, the suspect may be asked to supply the encryption key and the

147 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 181-184.

148 Bharvada 2002 *International Review of Law, Computers & Technology* 268.

149 Entropy testing is a process by which the randomness of the distribution of data within a file can be tested. The specific randomness can then be compared against a table of known algorithm randomness to identify whether a known algorithm has been used. This works well for all publicly known and encryption algorithms, because the law enforcement officer can use them to document their randomness scale. However, if the suspect is using a new or non-public program, an entropy test is not able to identify the type of encryption used. Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 176-179.

150 Russell remarked that: "No one is paranoid enough.... You should use encryption, but you should not trust it.... There is always a possibility that someone can break it." Russell R (ed) *Stealing the Network: How to Own a Continent* 7.

151 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 175.

method by which she encrypted the data. Although this sounds simplistic and too good to be true, it often works. Alternatively, a court of law may order the production of the encryption key and the method used to encrypt the data.[152]

Steganography is the technique of hiding information in other data such as visual images, voice communication and music. The word is derived from the Greek word meaning "covered writing" and it refers to the science of hiding information inside something innocuous so that no-one suspects it is there in the first place. Secret messages written in invisible ink, micro dots and radio signals that resemble noisy static are examples of steganography used in the past. Using the steganography tools available today, suspects can even hide data inside an image and audio files. When a sophisticated suspect is being investigated and remnants of a steganography tool exist, it would be bad practice not to attempt to discover the existence of any hidden data.

Like all cryptographic techniques, steganography is fallible. Sophisticated programs are available to crack the algorithms.[153] Criminals may prefer the use of steganography because of the fact that encrypting data is visible to prying eyes, while the use of steganography is invisible to authorities who may not even know that there is anything that needs decrypting. Steganography has yet to achieve the versatility of public key cryptography. The main areas where it is increasingly being used are where cryptography and strong encryption are outlawed.[154]

2.4 *Caught in the act: interception and monitoring, search and seizure, production and preservation*

The earliest judicial recognition of the right to privacy arose in the context of the protections afforded to domestic occupiers in respect of warrantless searches.[155] Protections were later extended to include not only tangible searches, but also searches effected by surveillance and the interception of communications.[156] In some jurisdictions, bodily intrusion is also regarded as a search that may violate privacy.[157] The most embryonic of protections in respect of the right to

---

152 Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 180.

153 Stegdetect and Steg Suite are well-known steganography detection tools. Davis, Philipp and Cowen *Hacking Exposed Computer Forensics Secrets & Solutions* 181.

154 Bharvada 2002 *International Review of Law, Computers & Technology* 268-269.

155 See, for example, paragraphs 5.2.1 and 6.2.1 below in respect of the evolution of search and seizure powers in the United States and England respectively.

156 In the United States, surveillance effected by bugging persons or premises or intercepting communications is regarded as an integral aspect of search powers. In England, until 1985, with the enactment of the Police and Criminal Evidence Act of 1984, no theoretical or systemic relationship was acknowledged to exist between searches for tangible evidence and the use of covert surveillance. The incorporation of the European Convention on Human Rights into the English legal framework has finally led to some recognition that the acquisition of intangible information may fall within the purview of article 8 and that any prosecution that relies upon such evidence might be challenged under article 6 (the right to a fair trial), if there has been any unreasonable interference with privacy rights. See Sharpe *Search and Surveillance* 111.

157 A further distinction can be made between searches for tangible evidence that incriminate a suspect by virtue of its existence and searches for tangible evidence that incriminate only by virtue of forensic analysis. In England and South Africa, taking a sample from a suspect has not been treated as an aspect of search and seizure, but as a subcategory of identification

privacy currently exists in the area of information acquisition, retention and dissemination.[158] Buttressing the need for the protection of information is the move toward targeted policing and the creation of databases of knowledge as tools of crime control.[159] Sharpe[160] submits that a redefinition of orthodox notions of what constitutes a search in the context of a criminal investigation, from an evolutionary perspective, recognises that the concept now extends to the use of any law enforcement investigatory practice that results in the finding of evidence.[161]

In most jurisdictions, the powers of interception and monitoring of communications have traditionally been seen as more intrusive than the powers of searching and seizing.[162] Content data is generally also more jealously guarded than, for example, traffic and subscriber data.[163] In its turn, the powers to request and/or order the production or preservation of information could, arguably, be considered less infringing to the right of privacy than the powers of search and seizure. Consequently, the law has evolved gradually into different legal powers, emanating from different legal regimes, so as to extend protection to the different facets of the right to privacy.

The question arises whether (and if so, to what extent) the distinction between the facets of the right to privacy that are more and less worthy of protection remains relevant in contemporary computing contexts. So, for example, technology is challenging the legal concepts of search and seizure and interception and monitoring, in that some of the traditional distinctions between these concepts overlap or become blurred in computing environments. Interconnected computer systems provide, for example, the possibility that the search of stored data can be carried out from remote terminals. Where the data is not transferred, but only surveyed or copied, this can be done without the knowledge of the owner or custodian of the data.[164] In theory, this renders a search and seizure intervention as secretive as an interception or monitoring.

Another example of technology forcing the convergence of legal concepts is attributable to the transmutable[165] nature of computer data. Whereas a search is generally executed in respect of

---

evidence. In the United States, however, such evidence is regarded as having been obtained through a process of search: a search of the person of the suspect. See *US v Weir* (1981) 657 F2d (8th Cir) 1005; *Schmerber v State of California* (1966) 348 US 757 and Sharpe *Search and Surveillance* 10-11.

158 Sharpe *Search and Surveillance* 220.

159 Sharpe *Search and Surveillance* 1.

160 See Sharpe *Search and Surveillance* xix.

161 Thus, new technologies, such as electronic surveillance and the power to do DNA analysis, according to her, are likely to be considered part of the package of police methodologies that are used to effect a search and to obtain evidence against a suspect. See Sharpe *Search and Surveillance* xix.

162 This resounds locally, for example, in the fact that interceptions and monitoring are only allowed in respect of certain serious offences, as set out in the Schedule to the RICPCIA and in the definition of a "serious offence" in article 1 of the preceding Interception and Monitoring Prohibition Act.

163 See the Council of Europe's Explanatory Report to the Cybercrime Convention 40.

164 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 12.

165 Examples of such transmutation include cases where data are converted from an electromagnetic form to a paper printout, a visual representation on a monitor-screen or an auditory simulation of human speech. The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 12.

existing recorded data, an interception is aimed at data that is being processed into the form in which it is concurrently transmitted and intercepted. However, data within a computer system can change its form and it can be transmitted from one location to another. Previously recorded data may, accordingly, be transmitted in the same or another electronic format and may be intercepted during this period of transmission.[166]

The approach taken by the international legal community, as reflected in the Cybercrime Convention, is to develop, supplement and continue applying existing legal concepts.[167] This approach is also subscribed to in pursuing the main objective of this research, namely to examine South Africa's compliance with the Cybercrime Convention with regard to the proposed criminal procedural provisions of search and seizure, production and preservation.

The first principle in the Council of Europe's Recommendation of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology[168] accordingly requires that the legal distinction between the search of computer systems and the seizure of data stored therein, as opposed to the interception of data in the course of transmission, be clearly delineated and applied.[169] The reason for this is, specifically, the fact that different legal powers, emanating from different legal regimes, in respect of different categories of computer data, are required in order to execute the actions of search and seizure as opposed to the actions of interception and monitoring. While the end result in both instances is the acquisition of data, the preconditions for using the accompanying safeguards and the scope of these two coercive powers differ.[170]

It is also important to discern between the legal regimes of search and seizure and interception and monitoring in terms of the scope of this research. Interception and monitoring is considered only to the extent required to negatively define search and seizure. In this study, the differentiation between search and seizure and interception and monitoring is based upon the format and inertness of the data at the time of its gathering. Data that is static, recorded and stored, is acquired by means of a search and seizure intervention. However, if the data is fluid and in movement, acquisition is accomplished by means of an interception and monitoring intervention.[171]

---

166 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 12.

167 It would, however, be very interesting to mull over the first in-depth analysis of the technical relevance of these different existing legal concepts. Allow the researcher the indulgence in a (perhaps not so technically flamboyant) "gut feel" that has been painstakingly cultivated by constant contact-inflation with the "techies" of this world: legal practitioners could quite possibly be utterly astounded by the outcomes of such an analysis. The initial differentiation between those facets of privacy that are more and less worthy of protection could become increasingly irrelevant as digitisation overtakes us. This shoemaker is, however, sticking to her last whilst enticing the academics among the techie breed to rise to the occasion.

168 The Council of Europe's "Recommendation No R(95)13 of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology" found on the Internet http://cm.coe.int/ta/rec/1995/95r13.htm (hereinafter referred to as the Council of Europe's Recommendation 1995(13).

169 The Council of Europe's Recommendation 1995(13) 11.

170 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 11.

171 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 12.

The Cybercrime Convention not only adapts traditional search and seizure powers to the demands of the volatile technological environment, but has also created new measures to ensure the continued effectiveness of search and seizure legal devices or to provide less intrusive alternative powers.[172] For this reason, the production, preservation and partial disclosure mechanisms proposed by the Cybercrime Convention are included in the scope of this study, as they signal ways in which search and seizure mechanisms could be facilitated, supplemented or aligned to the dictates of technological progress.

For the purposes of this thesis, computer data is therefore studied as the object of a search and seizure, production and preservation intervention. This implies that for the purposes of this study, the computer data referred to must be static, recorded and stored.

2.4.1 Interception/collection and monitoring

Interception and monitoring in accordance with the Cybercrime Convention is directed at data that is fluid and in movement.[173] It entails the collection of data in currently generated communications collected at the time of the communication.[174] Such data is, generally, in the process of being created at the time when it is gathered. The gathering of real-time data takes place during a certain period in respect of data that will be created or, if it has already been created and recorded, will be transmitted at a particular time or period in the future. Interception and monitoring is generally secretive or surreptitious and the physical presence of law enforcement officers is generally not necessary.[175]

Whilst operationally acknowledging that data is "collected" in both situations, the Cybercrime Convention refers normatively to the collection of traffic data as "real-time collection" and to the collection of content data as "real-time interception". The rationale behind this is to assist in recognising the distinction made by some states, including South Africa, between the real-time interception of content data and the real-time collection of traffic data. The common operational use of the term "collect or record" in the Cybercrime Convention is intended also to recognise that some states do not differentiate between the collection of traffic data and the interception of content data.[176]

"Interception", in terms of section 1(1) of the RICPCIA, means the aural or other acquisition of the contents of any communication through the use of any means, including an interception

---

172 See paragraph 1.1 above.
173 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 12.
174 The Council of Europe's Explanatory Report to the Cybercrime Convention 40. See also the definition of real-time in paragraph 2.2.1 above.
175 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 11 and the Council of Europe's Explanatory Report to the Cybercrime Convention 39.
176 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 40-41.

device, in order to make some or all of the contents of a communication available to a person other than the sender, recipient or intended recipient of that communication. This interception includes monitoring any such communication by means of a monitoring device; viewing, examining and inspecting the contents of any indirect communication; and diverting any indirect communication from its intended destination to any other destination. "Monitoring" includes listening to or recording communications by means of a monitoring device.[177]

In South Africa, a communication is considered to have been intercepted if the interception is effected by conduct within the country and it is intercepted in the course of its occurrence in the case of a direct communication; and in the case of an indirect communication, in the course of its transmission by means of a postal service or telecommunication system, as the case may be.[178] Importantly, the time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system that transmits or has transmitted such an indirect communication is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.[179] The interception of any indirect communication broadcast or transmitted for general reception is not considered the interception of a communication.[180]

The RICPCIA distinguishes between the real-time interception of a communication and the provision of real-time communication-related information.[181] This study is not concerned with interception directions, as they are directed at data in transit and not at stored computer data. Real-time communication-related information is described in section 1 of the RICPCIA as information which is immediately available to a telecommunications service provider before, during or for a period of 90 days, after the transmission of an indirect communication.[182] Technically such "real-time" communication-related information could thus have been stored by the telecommunications service provider for a period of 90 days already. This definition of real-

---

177 "Monitoring device" is defined in section 1(1) of the RICPCIA as any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.

178 Section 1(2)(a) of the RICPCIA.

179 Section 1(2)(b) of the RICPCIA guards against the circumvention of one legal regime, by waiting for a time when the form of the data has changed so as to allow for the utilisation of the legislative power applicable to the new form of the data. An example would be where data has changed from a state of transmission to a state of storage. A practical example can be found in respect of an unopened email message waiting in the mailbox of an Internet service provider until the addressee downloads it to her computer system. A question arises whether such data has to be considered stored computer data or data in transfer. Under the law in some states in the United States, such an email message is part of a communication; and therefore its content can only be obtained by applying the power of interception, whereas other legal systems consider such messages stored data to which the power of search and seizure applies. See the Council of Europe's Explanatory Report to the Convention on Cybercrime 37. In the South African legislative framework, section 1(2)(b) of the RICPCIA directs that such data be made the object of an interception intervention, as it is considered to be data in transfer. An analogy facilitating legal certainty when contracting online can be found in article 23 of the Electronic Communications and Transactions Act.

180 Section 1(3) of the RICPCIA.

181 Section 16 of RICPCIA makes provision for the application for, and issuing of, an interception direction. Section 17 of the RICPCIA makes available an application for, and the issuing of, a real-time communication-related direction. Section 18 contains a combined application for, and the issuing of, an interception direction, real-time communication-related direction and archived communication-related direction or interception direction supplemented by a real-time communication-related direction. Section 15 of the RICPCIA also explicitly brings the production of real-time communication-related information within the scope of section 205 of the Criminal Procedure Act (provided that the information is not provided on an ongoing basis).

182 See paragraph 2.2.1.1.2 above for a definition of real-time communication-related information.

time communication-related information obscures the meaning given to stored computer data in the Cybercrime Convention to some extent. References to real-time communication-related information under the RICPCIA is incorporated into this research only to the extent that it overlaps with stored computer data as *per* the Cybercrime Convention.

Real-time communication-related information could become the object of both a production order under section 205 of the Criminal Procedure Act (but not on an ongoing basis) and a real-time communication-related direction under section 17 of the RICPCIA. The latter provision allows for the ongoing provision of real-time communication-related information. In urgent or exceptional circumstances, an oral real-time communication-related direction can be issued under section 23(7) of the RICPCIA. In circumstances where it is not advisable to order the required real-time communication-related information from the telecommunications service provider, such information could also be collected by means of a search and seizure intervention. This would be the case where the service provider is, for example, collaborating with the suspect.

Provision is also made in the RIPCIA for the production of archived communication-related information, which does resort within the parameters of this research, as it targets stored computer data.[183]

2.4.2 Search and seizure[184]

Search and seizure in accordance with the Cybercrime Convention is directed at any computer data, including all forms of communications data, provided that such data is static, recorded and stored. Search and seizure is concerned with data that has been recorded or registered in the past, either in tangible or in intangible form, and the gathering of this data takes place at a single moment in time, in other words, the period of the search, and in respect of data that exists at that time.[185] Law enforcement officers are generally physically present during the course of a search and seizure and the intervention is generally non-secretive in nature.

To "search" in terms of the Cybercrime Convention means to seek, read, inspect[186] or review data and it therefore allows for both the searching for and the searching or examining of data.[187]

---

183 See paragraph 2.4.3 below.

184 See paragraphs 3.3 and 3.4 and paragraphs 4.2 and 4.3 below for a discussion of the search and seizure mechanisms proposed by the Cybercrime Convention and the search and seizure mechanisms available in the South African legal framework, respectively.

185 As opposed to interception and monitoring. See paragraph 2.4.1 above. The Council of Europe's Explanatory Report to the Cybercrime Convention 36; the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 11.

186 Search can, however, be discerned from inspection by the general maxim in the English legislative framework that inspection is by eye, search by hand, and that, although the power to inspect covers walking around premises, and, for example, examining goods in packing cases, it does not cover searching for things that are hidden, or rummaging through the contents of wastepaper baskets. Stone *The Law of Entry, Search, and Seizure* 328. However, In a very recent and important decision of the South African Constitutional Court it was held that "the threshold question of whether legislation authorises a search in terms of section 14 of the Constitution cannot be answered by a computer scan for the word 'search" (at par [36]). Courts must evaluate the nature and context of the power authorised by the legislation. The Constitutional Court accordingly held that an inspection under section 65(1) and (2) of the North West Gambling Act 2 of 2001 amounts to a search and infringes

The term "similarly access", as introduced by article 19(1) of the Cybercrime Convention, more accurately reflects computer terminology, is said to have a neutral meaning[188] and would include actions such as the mirror imaging of data or the diversion of a copy of the data for scrutiny at another location.

To "seize" means to take away the physical medium in which data or information is recorded and includes the use or seizure of programmes needed to access the data being seized.[189] To "seize" also means to make and retain a copy or image of data or information. The term "similarly secure" is included in article 19(3) of the Cybercrime Convention to reflect other means by which intangible data is removed,[190] rendered inaccessible[191] or otherwise taken control over in computing environments.[192] In order to secure stored intangible data, additional measures of maintaining the integrity or the chain of custody of the data are required. In this context, "secure" means taking control over or taking away data.[193] Data, albeit copied or removed, must be retained in the state in which it was found at the time of the seizure and it must remain unchanged during the time that the criminal proceedings take.

To seize or similarly secure data therefore allows both for gathering evidence (for example, by copying the data) and for confiscating evidence (for example, by copying the data and subsequently rendering the original version of the data inaccessible or by removing it, without necessarily implying a final deletion of the seized data).[194]

The flexible approach of using both the traditional notions of either "search and seizure", or the new and more technology-oriented notions of "access and copying",[195] adopted in the Council of Europe's Explanatory Report to the Convention on Cybercrime is subscribed to in this thesis. The compromise of mixed synonymous expressions such as "search or similarly access" and "seize/copy or similarly secure" is also intermittently used. This inclusive approach to the quest for appropriate terminology seeks to underscore the modernisation and the harmonisation of domestic laws for the purposes of international cooperation. It reflects the evolution of concepts

---

the right to privacy. These sections were found unconstitutional and invalid. See *Magajane v North West Gambling Board* Case CCT 49/05 decided on 8 June 2006.

187 The Council of Europe's Explanatory Report to the Cybercrime Convention 37.

188 As opposed to search. The Council of Europe's Explanatory Report to the Cybercrime Convention 37.

189 The Council of Europe's Explanatory Report to the Cybercrime Convention 38.

190 Such as the imaging of data.

191 For example, by means of encryption or other technological denials of access to data. Encryption is the process of obscuring the content of a message. The process is used to protect data in two ways, namely to maintain privacy and to prove integrity. See Kruse and Heiser *Computer Forensics* 83. See also paragraph 2.3.1.3.2 above.

192 Such as the diversion of data to another destination address. The Council of Europe's Explanatory Report to the Cybercrime Convention 38.

193 The Council of Europe's Explanatory Report to the Cybercrime Convention 38.

194 The Council of Europe's Explanatory Report to the Cybercrime Convention 38.

195 Specific reference is also made in the Council of Europe's Explanatory Report to the Cybercrime Convention to the terms "access and copy" having been adopted in the texts of other international *fora* (such as the G8 High Tech Crime Subgroup). See the Council of Europe's Explanatory Report to the Cybercrime Convention 38.

in the electronic environment, whilst also identifying and maintaining the traditional roots of these concepts.[196]

In the South African legal framework, a "search" is regarded as any act whereby a person, container or premises is visually or physically examined with the object of establishing whether an article is in, on or upon such a person, container or premises.[197] Although the search of premises for, and the seizure of, a computer itself can be authorised under the Criminal Procedure Act, the South African Law Reform Commission has submitted that the same does not apply to the search of a computer and the seizure of information located on that computer.[198] It is argued that words such as "article"[199] and "premises" [200] denote that the criminal procedural provisions are intended to be applied in respect of physical items.

To the extent that communication-related information under the RICPCIA is considered real-time for a period of 90 days after its transmission, such real-time communication-related information can be obtained by means of a real-time communication-related direction or a production order under section 205 of the Criminal Procedure Act. Following the expiration of a period of 90 days after the date of transmission, the communication-related information is considered to be archived communication-related information and, as such, can be obtained by means of a search and seizure intervention, an archived communication-related direction or a production order under section 205 of the Criminal Procedure Act.

The Constitutional Court held that the word "seizure" is not a term of art and should be given its ordinary and natural meaning.[201] The compulsion to produce a document on pain of a criminal sanction must be considered as much a seizure as when a document is physically removed by another person.[202] A seizure takes place when a person is effectively deprived of control over an object which falls within her sphere of privacy.[203] A limited interpretation of the word "seize" to encompass the act of seizure only would render the search and seizure powers under chapter 2 of the Criminal Procedure Act worthless. Seizure accordingly refers not only to the initial seizure, but also to the continued detention of the article after the seizure.[204]

---

196 The Council of Europe's Explanatory Report to the Cybercrime Convention 24.

197 See the National Instruction of the South African Police Services relating to search and seizure in which this definition is used, as referred to in Joubert (ed) *Applied Law for Police Officials* 305.

198 The South African Law Reform Commission's Discussion Paper 99 on Computer-related Crime 14.

199 Section 20 of the Criminal Procedure Act authorises the seizure of "anything" and states that "anything" for purposes of the whole of chapter 2 of the Criminal Procedure Act is referred to as "an article". The term "anything" should, strictly speaking, not be confined to tangibles. See, however, paragraph 1.1.1 above and 4.2.2 1 below. See also chapter 7 in this respect.

200 "Premises" is defined in section 1 of the Criminal Procedure Act and includes land, any building or structure, or any vehicle, conveyance, ship, boat or aircraft.

201 *Rudolph v Commissioner for Inland Revenue* 1996 (7) BCLR 889 (CC) 11.

202 This seemingly brings "seizure" nearer to "production". See *Bernstein v Bester NO* 1996 (4) BCLR 449 (CC) 89.

203 Steytler *Constitutional Criminal Procedure* 84.

204 *Ntoyakhe v The Minister of Safety and Security* 1999 (2) SACR 349 (ECD). Du Toit *et al Commentary on the Criminal Procedure Act* 2-2B.

2.4.3 Production[205]

Production is the submission or handing over of data or information under legal compulsion. Production orders under the Cybercrime Convention are aimed, firstly, at specified stored computer data in a specific person's possession or control and, secondly, at subscriber information relating to such services in a particular service provider's possession or control. Data or information sought by means of a production order is limited to the data maintained by the person or service provider to whom the production order is addressed.[206] Real-time traffic data and real-time content data cannot be acquired by means of production orders under the Cybercrime Convention.

In the South African legislative framework, provision is made in section 205 of the Criminal Procedure Act for general criminal procedural production orders. This mechanism, under section 15 of the RICPICA, can also be directed at communication-related information, but not on an ongoing basis.

Sections 17 and 19, read with sections 13 and 14, of the RICPCIA allow for the production of real-time and archived communication-related information respectively. In addition, section 23(7) of the RICPCIA provides for the oral application for, and issuing of an oral direction or entry warrant for purposes of the provision of, *inter alia*, real-time communication-related information. Section 23(7) is not applicable to archived communication-related information. Sections 39(3) and 40(3) of the RICPCIA allow for the provision of limited information so as to facilitate making applications under the RICPCIA.

2.4.4 Preservation[207]

Data preservation is the activity that keeps existing, stored data secure and safe. In order to "preserve" data, data which already exists in a stored form must be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that data be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be frozen, rendering such data or copies thereof inaccessible to legitimate users.[208]

In relation to computer usage, data preservation must be distinguished from data retention. Data retention is the process of storing data. To "retain" data means to keep data which is

---

205 See paragraphs 3.7 and 3.8 and paragraphs 4.4 and 4.5 below for a discussion of the domestic and transborder production orders proposed by the Cybercrime Convention and the production orders available in the South African legal framework respectively.

206 The Council of Europe's Explanatory Report to the Cybercrime Convention 33.

207 See paragraphs 3.5 and 3.6 and paragraphs 4.6 and 4.7 below for a discussion of the preservation mechanisms proposed by the Cybercrime Convention. In South Africa, preservation is currently accomplished by means of search and seizure and production orders. No specific provision is made in South African law for mechanisms aimed solely at the preservation of computer data. The closest mechanism to such a preservation mechanism would be the Anton Pillar order, referred to in footnote 564 of paragraph 4.6 below. However, Anton Pillar orders are civil law orders.

208 The Council of Europe's Explanatory Report to the Cybercrime Convention 28.

currently being generated (real-time data) in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future period.[209]

The importance of the distinction between preserved and retained computer data in the Cybercrime Convention is evident from the fact that articles 16 and 17 only refer to data preservation and not to data retention. These articles provide for the expedited preservation of stored computer data, and the expedited preservation and partial disclosure of traffic data, respectively.[210]

Section 30(1) of RICPCIA provides for data retention in the South African legislative framework. It obliges South African telecommunications service providers not only to provide a telecommunications service in which communications can be intercepted, but which can also store communication-related information.[211]

Reference is also made to data retention in section 16 of the Electronic Communications and Transactions Act, which provides that where a law requires information to be retained, such a requirement is met in respect of data messages if

(a) the information contained in the data message is accessible so as to be usable for subsequent reference;

(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

---

209 The Council of Europe's Explanatory Report to the Cybercrime Convention 28. Data retention is provided for in Title 5 of the Cybercrime Convention. Articles 20 and 21 of the Cybercrime Convention deal with such flowing data in transfer. They provide for the real-time collection of traffic data and the interception of content data, respectively.

210 See paragraph 3.5 and 3.6 below for a discussion of articles 16 and 17 of the Cybercrime Convention.

211 On the date when a telecommunications service licence is issued under the Telecommunications Act to such a telecommunications service provider or category of telecommunications service providers, and after consultation with the Independent Communications Authority of South Africa (ICASA) and the telecommunications service provider or category of telecommunications service providers concerned, the cabinet members responsible for communications and the administration of justice must issue a directive in respect of that telecommunications service provider or category of telecommunications service providers (section 30(2) of the RICPCIA). This directive must determine the manner in which effect is to be given to the interceptability requirement set out in section 30(1). It also determines the security, technical and functional requirements of the facilities and devices that the telecommunications service provider or category of telecommunications service providers must acquire to enable them to both intercept indirect communications and to store communication-related information. This directive must also determine the type of communication-related information which must be stored and the period for which such information must be stored. This period may not be less than three years and may not exceed five years from the date of the transmission of the indirect communication to which that communication-related information relates. The directive must also determine and mention a period which may not be less than three months and may not exceed six months from the date of its issuance for compliance with the directive. This directive must also, where applicable, prescribe the capacity needed for interception purposes, the technical requirements of the systems to be used, the connectivity with interception centres, and the manner in which duplicate signals of indirect communications, real-time or archived communication-related information will be routed to designated interception centres (section 30(3) of the RICPCIA).

(c) the origin and destination of that data message and the date and time it was sent or received can be determined.[212]

Discerning between data retention and preservation is also important for the purposes of setting the research parameters of this study, as this thesis is essentially concerned with data preservation. Data retention is referred to only in so far as it could make South Africa compliant with the preservation requirements of the Cybercrime Convention.

2.5 *Penetrating the House of Binary: computers of all shapes and sizes*

A broad understanding of computer systems and categories of computer systems targeted for *e*-evidence collection purposes is necessary; and it is therefore provided below. Electronic evidence may exist in many forms and locations within any computer system. Many of these forms and locations are not visible to the average computer user. An awareness of the hardware and software layers of a computer system is therefore instrumental to the discovery of "little electronic nooks and crannies of hidden data"[213] and possibly of *e*-evidence that they might contain.

2.5.1 *Computer system*

A computer can be defined as an electronic machine that can accept data (input), manipulate the data according to specific rules (process), produce results (output), and store the results for future use (storage).[214] A computer system usually consists of different devices, to be distinguished as the processor or central processing unit (CPU), and peripherals. A "peripheral"[215] is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, compact disc (CD) reader/writer or other storage device.[216] A peripheral, although it is not part of the essential computer, is situated relatively close by. It can be mounted in the same case as the processing unit (such as a hard

---

212 This obligation to retain information does not, however, extend to any information the sole purpose of which is to enable the message to be sent or received. Indirect reference is made to data retention in chapter VIII of the Electronic Communications and Transactions Act that provides for the scope of the protection of personal information and the principles for electronically collecting personal information.

213 Hard drives, for example, have been compared to a Russian nesting doll, to be explored electronically. See Kruse and Heiser *Computer Forensics* 65. A hard drive consists of an ever-smaller set of data structures, each contained within the next larger set (namely the hard drive, partition, filesystem, file, record, field). This Russian nesting doll, in the final analysis, is indestructible, in that data cannot be truly erased from magnetic media. Every write leaves behind traces even when the media have been overwritten numerous times. Special electron microscopes can be used to recover overwritten tracks, bit by bit. See Kruse and Heiser *Computer Forensics* 77. There is no guarantee of the complete elimination of, for example, shadow data (that is, fringe data that remains on the physical track of storage media after deletion, sweeping or scrubbing). However, recovering it is not an easy task. See Anonymous "Digital Evidence Collection and Handling" found on the Internet http://faculty.ncwc.edu/toconnor/426/426lect06.htm 10. Also, when a file is deleted, it is not erased or even moved to a different location. When a file is deleted, the computer simply recognises the space used by the file as "available to be overwritten" and this often does not happen immediately. See O'Reilly and Derting 2002 *Computers and Law (C&L) Litigation Support* 39.

214 Shelly *Discovering Computers* 1.04.

215 The Council of Europe's Explanatory Report to the Cybercrime Convention 5.

216 The Council of Europe's Explanatory Report to the Cybercrime Convention 5.

disk drive), or be attached to the computer case with a wired or wireless connection (such as a scanner or printer).[217]

Article 1(a) of the Cybercrime Convention defines a "computer system" as[218]

> ... any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

In terms of the Cybercrime Convention, a computer system is, furthermore, a device that combines hardware with software[219] to automatically process digital data.[220]

2.5.1.1 Computer hardware

Hardware is the physical aspect of computer, telecommunications and other information technology devices and is a collective term.[221] A computer consequently consists of a variety of electric, electronic and mechanical hardware components, including input devices,[222] output devices,[223] a system unit,[224] storage devices[225] and communications devices.[226] Hardware also includes the cables, connectors and power supply units associated with a computer system.[227]

The storage portions of the computer system, where both the data and programs are located, are primarily where electronic evidence is located. The storage portions of a computer system are, therefore, predominantly what electronic evidence collection interventions are directed at.[228]

Computer storage refers to holding data in an electromagnetic form for access by a computer processor.[229] Data on any computer drive is digitised. The data is therefore expressed as

---

217 SearchMobileComputing.comDefinitions "Peripheral" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212774,00.html 1.

218 Cybercrime Convention 3.

219 "Middleware" in the computer industry generally refers to any programming that serves to "glue together" or mediate between two separate and often already existing programs. A common application of middleware allows programs written for access to a particular database to access other databases. See SearchWebServices.com Definitions "Middleware" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212571,00.html 1. Middleware, for the purposes of this thesis, is seen as a form of software.

220 The Council of Europe's Explanatory Report to the Cybercrime Convention 5. "Automatic" means without direct human intervention.

221 SearchSmallBizIT.comDefinitions "Hardware" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci212228,00.html 1.

222 Such as the keyboard, mouse, scanner or a digital camera.

223 Such as a printer, monitor and speakers.

224 The main component of the system unit is the motherboard that houses the CPU and memory. The motherboard is the physical arrangement in a computer that contains the computer's basic circuitry and components (such as the microprocessor, coprocessors, memory, the basic input/output system (BIOS) and expansion slots). The electronic interface between the motherboard and the smaller boards or cards in the expansion slots is called the bus. See searchSmallBizIT.com Definitions "Motherboard" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci212594,00.html 1.

225 Such as floppy disks and hard disks.

226 Such as a modem. Shelly *Discovering Computers* 1.08.

227 SearchSmallBizIT.comDefinitions "Hardware" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci212228,00.html 1.

228 FBI/CART *Conducting Searches in a Computer Environment* 7.

229 SearchStorage.comDefinitions "Storage" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214465,00.html 1.

myriads of ones and zeros. These bits are stored using any of three principles, namely magnetic,[230] optic[231] and magneto optic[232] storage. Most computers use magnetic media for their permanent storage, the common denominator of which is that these media are all coated with a metallic oxide. This ferric (iron) oxide, which is the basic component of the coating of these magnetic media, and which is usually used in conjunction with cobalt or barium, is commonly called "rust".[233] Although optical storage methods quickly began to rival the popularity of magnetic storage, the latter has remained popular due to the fact that magnetic media offer low cost-per-bit storage, they are intrinsically non-volatile and have successfully evolved upward in capacity.[234]

A storage medium is the physical material on which a computer keeps data, instructions and information. A storage device is the computer hardware that records and retrieves items to and from a storage medium.[235] Storage devices transfer data to and from a storage medium into memory. Data can be stored online,[236] offline[237] and near-line[238] and can be shifted from one form of storage to another.

2.5.1.1.1 Primary storage/ memory

While processing data and instructions, the processor places instructions that have to be executed and data needed by those instructions into memory. This memory is a temporary built-in storage place for data, instructions and information. Also called primary storage, this and other types of memory consist of one or more chips on the motherboard or some other circuit board in the computer.[239] Some computers also use virtual memory, which expands memory onto a hard disk.[240]

Primary storage is much faster to access than secondary storage, because of the proximity of the storage to the processor and because of the nature of the storage devices.[241] The more

---

230 Such as floppy disks and hard disks.
231 Such as compact disk read only memory [CD-ROMs] and digital versatile/video discs [DVDs].
232 Such as high end drives. CSIR-Defencetek *CSIR FACTS* 36.
233 FBI/CART *Conducting Searches in a Computer Environment* 2.
234 Brooks *A+ Certification Concepts and Practice* 34.
235 Shelly *Discovering Computers* 7.04.
236 Data that is stored online is readily available to the user. The devices most commonly used for online storage are hard drives. Hard drives are very fast, but their cost is still greater than that of other types of storage media. Central data storage is one of the primary uses of a computer network. See Nash *Networking Essentials MCSE Study Guide* 22.
237 A common way of migrating data offline is to put it on magnetic tape so that it can be loaded back when it is needed. Offline storage devices provide a low-cost solution to storing and archiving data, but do not provide easy access. See Nash *Networking Essentials MCSE Study Guide* 22.
238 Near-line storage is a way to keep data migrated off expensive hard disk space, but close enough to let users access the data. This type of storage can be achieved by means of jukeboxes with large numbers of tapes or optical disks that can automatically put the required data back online fairly quickly, with little intervention from the system administrator. See Nash *Networking Essentials MCSE Study Guide* 22.
239 Shelly *Discovering Computers* 4-15.
240 Webopedia "Memory" found on the Internet http://www/pcwebopedia.com/TERM/m/memory.html 1.
241 SearchMobileComputing.comDefinitions "Storage" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214465,00.html 1.

memory is available, the less frequently the computer has to access instructions and data from the more slowly accessed hard disk form of storage.[242]

Memory is therefore the electronic holding place for instructions and data that the computer's microprocessor can reach quickly. When a computer is in normal operation, its memory usually contains the main parts of the operating system and other system software that control the use of the computer equipment; some or all of the application programs that carry out a specific task, such as word processing; and related data that are being used and processed by the application programs.[243] A computer system unit contains two types of memory: volatile and non-volatile. When the computer's power is turned off, volatile memory loses its contents. Non-volatile memory, by contrast, does not lose its contents when power is removed from the computer.[244] Examples of primary storage include the following:

(a) **Random access[245] memory (RAM)**: RAM consists of memory chips that can be read from and written to by the processor and other devices. When a computer is powered on, certain operating files load from a secondary storage device, such as a hard disk, into RAM, where these files remain for as long as the computer is running.[246] Most RAM is volatile, which means that when the power is turned off, whatever data was in RAM is lost.[247] Two basic types of RAM chips exist: dynamic RAM (DRAM), which must be re-energised constantly to prevent the chips from losing their contents, and static RAM (SRAM), which needs less re-energising than DRAM. DRAM is sometimes called main memory. Many variations of DRAM chips exist, most of which are faster than the basic DRAM.[248] RAM has been compared to the human short-term memory, as opposed to the hard disk, which has been compared the human long-term memory. The short-term memory focuses on the work at hand, but can only keep a limited number of facts in view at one time. It can, however, refresh the brain from facts stored in the long-term memory.[249]

(b) **Read-only memory (ROM)**: ROM is built-in computer memory containing data that can normally only be read, not written to. ROM is non-volatile and is sustained by a small

---

242 SearchMobileComputing.comDefinitions "Memory" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212546,00.html 1.

243 SearchMobileComputing.comDefinitions "Memory" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212546,00.html 1.

244 Shelly *Discovering Computers* 4-16 – 4-17. This may have important ramifications in a search and seizure context and it is, for example, linked to the contentious debate as to whether the plug should be pulled when searching and seizing, or whether the computer should be properly shut down.

245 Note that other forms of storage (such as the hard disk and compact disc read-only memory) are also accessed randomly/directly, but the term "random access" is not applied to those forms of storage. It could rather have been called "nonsequential memory" or "direct access memory". In this respect see SearchMobileComputing.comDefinitions "RAM" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci214255,00.html 2.

246 Shelly *Discovering Computers* 4-17.

247 Webopedia "Memory" found on the Internet http://www/pcwebopedia.com/TERM/m/memory.html 2.

248 Shelly *Discovering Computers* 4-18.

249 SearchMobileComputing.comDefinitions "RAM" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci214255,00.html 1.

long-life battery in the computer system.[250] ROM chips contain data, instructions or information that is recorded permanently. ROM contains, for example, the basic input/output system (BIOS), which is the programming that allows a computer to be booted up or regenerated each time it is turned on.[251] A variation of the ROM chip is programmable read-only memory (PROM), which is a blank ROM chip on which items can be placed permanently.[252] PROM is non-volatile and cannot be erased or changed. Two variations of PROM are erasable programmable read-only memory (EPROM), which is a special type of PROM that can be erased by exposing it to ultraviolet light, and electrically erasable programmable read-only memory (EEPROM), which is a special type of PROM that can be erased by exposing it to an electrical charge.[253]

(c) **Memory cache**: A memory cache is also called a cache store or RAM cache and it primarily uses SRAM chips.[254] Cache memory is sometimes described in levels of closeness and accessibility to the microprocessor.[255] Most modern computers have two or three layers of memory cache: a level 1 (L1) cache, a level 2 (L2) cache and a level 3 (L3) cache. Cache is used to improve the processing times of computers, because it stores frequently-used instructions and data. When the processor needs an instruction or data, it searches its memory in this order: the L1 cache, then the L2 cache, then the L3 cache (if it has one), then RAM, resulting in a greater delay in processing for each level of memory it must search. If the instructions or data are not found in memory, then it must search a slower speed storage medium such as a hard disk.[256]

(d) **Complementary metal-oxide semiconductor memory (CMOS)**: This type of memory chip in the computer system unit stores configuration information about the computer that is used during the start-up process (such as the type of disk drives, keyboard, monitor, the current date and time). CMOS chips use battery power to retain information even when the power to the computer is off, keeping information (such as the calendar, date and time) current even when the computer is turned off.[257] Unlike standard ROM, information in the CMOS is user-adjustable. Such adjustments to CMOS are made during start-up.[258]

(e) **Flash Memory**: Flash memory is also called a flash ROM or flash RAM and it uses a variation of EEPROM. Flash memory is a type of constantly powered non-volatile

---

250 SearchSmallBizIT.comDefinitions "Read-only Memory" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci214271,00.html 1.

251 Shelly *Discovering Computers* 4-20. The acronym BIOS refers to the set of routines in read-only memory that enables a computer to start the operating system and to communicate with the various devices in the system, such as disk drives, the keyboard, monitor, printer and communications ports.

252 Webopedia "Memory" found on the Internet http://www/pcwebopedia.com/TERM/m/memory.html 2.

253 Webopedia "Memory" found on the Internet http://www/pcwebopedia.com/TERM/m/memory.html 2.

254 Shelly *Discovering Computers* 4-18.

255 SearchStorage.comDefinitions "Cache Memory" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211730,00.html 1.

256 Shelly *Discovering Computers* 4-20.

257 Shelly *Discovering Computers* 4-21.

258 CSIR-Defencetek *CSIR FACTS* 27.

memory that can be erased electronically and reprogrammed.[259] Flash memory chips store data and programs on many handheld computers and devices.[260] Flash memory cards store flash memory on a removable device instead of a chip, allowing users to transfer data and information conveniently from these small devices to their desktop computers.[261]

(f) **Expansion slots and expansion cards**: These are also termed cards, expansion cards, expansion boards, boards, adapter cards, adapters, interface cards, add-ins and add-ons. An expansion slot is an opening, or socket, where the user can insert a circuit board into the motherboard. These circuit boards add new devices or capabilities to the computer and the number of expansion slots available determines the expansion potential of the computer system.[262] Four types of expansion cards found in most computers today are video cards, sound cards, network interface cards (NICs) and modem cards.[263] PCMCIA cards (conformed to the standards of the Personal Computer Memory Card International Association) are now called PC cards. They are special types of expansion slots used in mobile computers. Because they are small and versatile, many consumer electronics products[264] use PC Cards.[265]

2.5.1.1.2 Secondary storage

If primary storage is equated to the top of one's desk, secondary storage can be seen as the filing cabinet that holds the file folders, from where a file folder could be removed and placed on the top of one's desk when required.[266] The terms auxiliary storage, auxiliary memory, secondary memory,[267] storage, auxiliary storage, permanent storage and mass storage have also been used for this kind of data repository.[268] Secondary storage holds data which may not be immediately needed for future use. Secondary storage is non-volatile, [269] holds data on external devices and can hold much more data than primary storage.[270]

Numerous types of storage media, varying in cost and speed, exist to meet a variety of user needs. Examples of secondary storage include the following:

---

259 Searchstorage.comDefinitions "Flash Memory" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212130,00.html 1.
260 Such as digital cellular telephones, printers, set-top boxes, digital cameras, automotive devices, digital voice recorders and pagers.
261 Shelly *Discovering Computers* 4-21.
262 Brooks *A+ Certification Concepts & Practice* 943.
263 Shelly *Discovering Computers* 4-23.
264 Such as digital cameras, cable TV and automobiles.
265 Shelly *Discovering Computers* 4-24.
266 Shelly *Discovering Computers* 7.04.
267 SearchMobileComputing.comDefinitions "Memory" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212546,00.html 1.
268 Shelly *Discovering Computers* 7.04.
269 Shelly *Discovering Computers* 7.04.
270 SearchStorage.comDefinitions "Storage" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214465,00.html 1.

(a) **Floppy disks and diskettes**: Floppy disks and diskettes are portable inexpensive magnetic storage media and can be recorded and erased hundreds of times.[271] Although the floppy disk preceded the diskette,[272] these terms are commonly used interchangeably. A floppy disk stores data in sectors which are grouped in clusters and tracks.[273] With reasonable care, floppy disks can last approximately seven years.[274] A floppy disk drive (FDD) is a device that can read from and write on a floppy disk. If a computer has one FDD, this is usually referred to as its Drive A. A high-capacity disk drive is a FDD that uses disks with capacities of 100 megabytes and greater.[275] The magneto-optical (MO) diskette is more popular for mass storage, backup and archiving.[276] Floppy disks have a write-protect function, prohibiting the drive from writing to the diskette.[277]

(b) **Hard disks**: A hard disk, also called a hard disk drive (HDD),[278] contains several inflexible, circular platters that store data electronically. A hard disk can be seen as a set of stacked disks, each of which, like phonograph records, has data recorded on the disk in concentric tracks.[279] A cylinder is the location of a single track through all the platters of the HDD. Like floppy disks, hard disks store data magnetically. An optically-assisted hard drive combines laser and optic technologies with the magnetic media, producing larger storage capacities of up to 250 gigabytes.[280] Most desktop computers contain at least one hard disk inside the computer system unit (called a fixed disk). Removable hard disks (also called disk cartridges) are portable variations. Examples of such are the Jaz® disk and the Peerless™ disk.[281] A formatted hard disk can be divided into separate areas called partitions by issuing a special operating system demand. Each partition functions as if it were a separate hard disk drive. If a hard disk contains only one partition, the first partition is drive C and the second partition is drive D.[282] On a personal computer, a hard disk controller (HDC) is the interface for a hard disk. Examples of a HDC for a personal computer are a Universal Serial Bus (USB), an enhanced integrated drive electronics (EIDE) controller and a small computer system interface (SCSI).[283] Most manufacturers guarantee their hard disks to last somewhere

---

271 Brooks *A+ Certification Concepts & Practice* 944.
272 A diskette has a rigid plastic cover, whilst floppies have flexible plastic covers.
273 In this respect, storage is effected in much the same way as storage on a hard disk.
274 Shelly *Discovering Computers* 7.09.
275 Shelly *Discovering Computers* 7.09.
276 SearchStorage.comDefinitions "Diskette" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211964,00.html 1.
277 Brooks *A+ Certification Concepts & Practice* 36.
278 Although the HDD and the hard disk are not the same thing, they are packaged as a unit and so either term is sometimes used to refer to the whole unit. An HDD is actually the mechanism that controls the positioning, reading and writing of the hard disk. See SearchStorage.comDefinitions "Hard Disk Drive" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci213993,00.html 1.
279 SearchStorage.comDefinitions "Hard Disk" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,sid5_gci212227,00.html 1.
280 Shelly *Discovering Computers* 7.11.
281 Shelly *Discovering Computers* 7.13.
282 Shelly *Discovering Computers* 7.12.
283 Shelly *Discovering Computers* 7.13.

between three and five years.[284] Interestingly, hard disk drives tend to be more delicate than floppy drives and therefore require some special handling considerations to prevent both damage to the unit and loss of data.[285] Interesting hard disk combinations are the following:

(i) The redundant array of independent disks (RAID) is a group of two or more integrated hard disks that are commonly used in networks and Internet servers. To improve data reliability, a RAID system duplicates data, for example, by mirroring (producing one backup disk for each disk) or striping (splitting data across multiple disks in the array).[286] Some RAID variations configure the drives to improve performance, whilst others concentrate on data security.[287]

(ii) An Internet hard drive (also called online storage) is a service on the web that provides storage to users, other than locally in the hard disks of their computer system unit.[288]

(c) **Compact disk (CDs)**: A CD (also called an optical disk) is a storage medium consisting of a flat, round, portable, metal disk with a protective plastic coating. CDs store data by using microscopic pits (indentations) and land (flat areas) that are in the middle layer of the CD. A high-powered laser light creates the pits, whilst a lower-powered laser light reads data from the CD by reflecting light through the bottom of the CD.[289] The reflected light is converted into a series of bits that the computer can process. Land causes light to reflect, which is read as a binary digit 1. Pits absorb the light and this absence of light is read as a binary digit 0. The drive designation of a CD usually follows alphabetically after that of all the hard disks.[290] Manufacturers guarantee that a properly cared for CD will last five years, but a CD could, in fact, last up to 50 to 100 years.[291] CDs are available in a variety of formats, including the following: [292]

(i) Compact disc read-only memory (CD ROM);

(ii) PhotoCD and Picture CDs;

(iii) Compact disc-recordable (CD-R) and compact disk-rewritable (CD-RW); and

(iv) Digital versatile/video disc-ROM (DVD-ROM), which is available in a variety of formats, such as the DVD-recordable (DVD-R) and the DVD rewritable (DVD+RW).

---

284 Shelly *Discovering Computers* 7.15.
285 Brooks *A+ Certification Concepts & Practice* 38.
286 Shelly *Discovering Computers* 7.15.
287 Brooks *A+ Certification Concepts & Practice* 950.
288 Shelly *Discovering Computers* 7.16.
289 Which is usually either solid gold or silver in colour.
290 Shelly *Discovering Computers* 7.18.
291 Shelly *Discovering Computers* 7.30.
292 Shelly *Discovering Computers* 7.25.

CD-R, CD-RW, DVD-R and DVD+RW combine the compatibility, flexibility and storage capacity of a CD or DVD with the drag-and-drop ease of a floppy disk.[293] As the cost of DVD technologies becomes more reasonable, it is expected that DVDs will eventually replace all CD media.[294]

(d) **Memory sticks**: The memory stick is a digital data storage technology with up to ten times the storage capacity of an ordinary diskette. A memory stick is about the size of a flat AA battery and is available in different sizes.[295]

(e) **Tape**: Tape is a magnetically coated ribbon of plastic capable of storing large amounts of data at a low cost. However, access to information stored on tape tends to be very slow, due to the fact that tape operates in a linear fashion.[296] Similarly to a tape recorder, a tape drive reads from and writes data on a tape. Tape is no longer used as a primary method of storage, but is instead used for long-term storage and backup purposes.[297] Its guaranteed life expectancy is two to five years and its potential life expectancy is 20 years.[298]

(f) **Enterprise storage systems**: An enterprise storage system is a strategy that focuses on the availability, protection, organisation and backup of storage on a network by using a combination of storage techniques. An enterprise storage system may, for example, combine servers, a RAID system, a tape library, CD-ROM jukeboxes, Internet backup, network-attached storage (NAS) devices and a storage area network (SAN).[299]

(g) **PC Cards**: PC Cards and flash memory cards can also qualify as secondary storage because they do not necessarily require built-in card readers or slots. An external card reader that attaches to any system unit can also be utilised. A PC card or flash memory can be changed without having to open the system unit or restart the unit (in other words, they are hot swapping, hot plugging or plug-and-play).[300]

(h) **Miniature mobile storage media**: Handheld devices do not have much internal storage. Some use PC cards, of which CompactFlash, Memory Stick®, Microdrive and SmartMedia are examples.[301] There are two basic types of smart cards, namely intelligent and memory. An intelligent smart card contains a processor and has input, output and storage capabilities, whilst a memory card has only storage capabilities.

---

293 Shelly *Discovering Computers* 7.24.
294 Shelly *Discovering Computers* 7.25.
295 SearchStorage.comDefinitions "Memory Stick" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214628,00.html 1.
296 Brooks *A+ Certification Concepts & Practice* 40.
297 Shelly *Discovering Computers* 7.26.
298 Shelly *Discovering Computers* 7.30.
299 Shelly *Discovering Computers* 7.27.
300 Shelly *Discovering Computers* 4.25 and 7.28.
301 Shelly *Discovering Computers* 7.28.

Smart cards are, for example, used to store a prepaid amount of electronic money (*e*-money, digital cash).[302]

(i) **Microfilm and microfiche**: Microfilm and microfiche store microscopic images of documents on roll or sheet film. A computer output microfilm (COM) recorder is the device that records the images on the film. They are inexpensive and have the longest life of any storage media, namely a guaranteed life expectancy of 100 and potential life expectancy of 200 years.[303]

2.5.1.2 Computer software

A computer system is a device that combines its hardware with the appropriate software to process digital data automatically.[304] A "computer program"[305] is a set of instructions to the hardware of the computer that can be executed to achieve an intended result (such as the processing of data into information).[306] "Processing data"[307] therefore means that data in the computer system is operated on by executing a computer program. The computer program essentially tells the hardware of a computer what to do. A computer can run several such software programs, often simultaneously. The terms computer program, program and software are often used interchangeably.[308] The two major categories of software are system software and application software.

2.5.1.2.1 Application software

Application software consists of programs that perform specific specialised tasks for users.[309] Popular application software includes productivity or business software,[310] graphics and multimedia software,[311] software for home, personal and educational use[312] and communications software.[313] Application software is available from application service providers[314] in a variety of forms, such as packaged, custom, freeware,[315] public domain[316] and shareware[317].

---

302 Shelly *Discovering Computers* 7.28.
303 Shelly *Discovering Computers* 7.30.
304 The Council of Europe's Explanatory Report to the Cybercrime Convention 5.
305 The Council of Europe's Explanatory Report to the Cybercrime Convention 5.
306 Shelly *Discovering Computers* 1.04.
307 The Council of Europe's Explanatory Report to the Cybercrime Convention 5.
308 Shelly *Discovering Computers* 1.10.
309 Brooks *A+ Certification Concepts & Practice* 53.
310 Such as word processing software, spreadsheet software, database software and presentation graphics software.
311 Such as computer-aided design software, video and audio editing software, web page authoring software.
312 Such as tax preparation software, clip art gallery software and home design software.
313 Such as email, web-browsers, chat rooms, newsgroups, groupware and videoconferencing software. Shelly *Discovering Computers* 3.04 to 3.34.
314 Shelly *Discovering Computers* 1.12 and 1.13.
315 Freeware is copyrighted software provided at no cost to a user and it cannot be resold by such a user. See Shelly *Discovering Computers* 1.09.
316 Public-domain software is free software that has been donated for public use and has no copyright restrictions. Shelly *Discovering Computers* 1.19.
317 Shareware is copyrighted software distributed free for a trial period. See Shelly *Discovering Computers* 1.21.

2.5.1.2.2 System software

System software consists of the programs that control the operations of the computer and its devices, serving as the interface between the user, the application software and the computer's hardware. Two types of system software are the operating system and utility programs.[318] A utility program is a type of system software that performs a specific task, usually relating to managing a computer, its devices or its programs.[319] Popular utilities offer functions such as viewing, compressing and backing up files; diagnosing problems; uninstalling software; defragmenting, scanning and backing up disks and displaying screen savers.[320]

An operating system (OS) is a set of programs containing instructions that coordinate all the activities among computer hardware devices. Functions common to operating systems include starting a computer, the user interface, managing programs, managing memory, scheduling jobs, configuring devices, accessing the World Wide Web,[321] monitoring performance, providing housekeeping services (such as the file manager and formatting), controlling a network and administering security.[322] Although most operating systems are device-independent, allowing the user to retain existing application software and data files even when changing computer models or vendors, some operating systems are still device-dependent. The latter can only run on a specific type or make of computer. Proprietary operating systems are privately owned and limited to a particular vendor or computer model.[323]

The three basic categories of operating systems are stand-alone, network and embedded operating systems.[324] A stand-alone operating system is a complete operating system that works on a desktop or laptop computer.[325] A client operating system is a stand-alone operating system that can either function on its own, or in conjunction with a network operating system.[326] A network operating system is an operating system that supports a network and typically resides on a server.[327] An embedded operating system resides on a ROM chip and is commonly used in handheld computers and small devices.[328]

---

318 Shelly *Discovering Computers* 8.02.
319 Shelly *Discovering Computers* 3.03.
320 Shelly *Discovering Computers* 8.27.
321 For a reference to the World Wide Web (WWW), see paragraph 2.6.3 below.
322 Shelly *Discovering Computers* 8.04 – 8.16.
323 Shelly *Discovering Computers* 8.17.
324 Shelly *Discovering Computers* 8.17 – See the discussion in paragraph 2.6 below in respect of the different categories of computing environments.
325 Examples of stand-alone operating systems are the disk operating system (DOS), Windows XP, Mac OS X and OS/2 Warp Client. See Shelly *Discovering Computers* 8.22.
326 Shelly *Discovering Computers* 8.17.
327 Examples of network operating systems are Netware, Windows NT Server, Windows 2000 Server, Windows. NET Server and OS/2 Warp Server for E-business. UNIX, Solaris and Linux are multipurpose operating systems because they are both stand-alone and network operating systems. See Shelly *Discovering Computers* 8.24.
328 Examples of embedded operating systems include Windows CE, Pocket PC 2002 and Palm OS. See Shelly *Discovering Computers* 8.25.

The operating system sees all, but it may not tell the user all about what it sees.[329] In fact, it is the job of the operating system to make the complexity of the computer as invisible as possible to the user.[330] This invisibility of complexity poses great challenges to a digital detective mining for electronic evidence.[331] This is also the reason why a forensic-grade image (a physical copy of the disk), as opposed to a logical copy, is required for forensic analysis. A logical copy is only a copy of the files that the operating system has chosen to see, whereas a physical copy is a copy of the data or lack of data in all the electronic nooks and crannies of the disk.[332]

If the printable end product of electronically created information is therefore committed to paper via a standard printing process, critical metadata[333] may be missed.[334] Email printouts, as a further example, do not show blind carbon copies (BCCs), except on the author's message, and they can also be edited by an experienced user to add information such as recipients, attachments and text.[335]

The file system[336] is where probably most time will be spent in mining the binary for different types of forensic gold.[337] There usually is a considerable amount of unallocated space on a disk drive, containing some kind of data which, for the most part, is not deliberately hidden.[338] This data has simply been left orphaned by the operating system and is patiently waiting to be

---

329 Kruse and Heiser *Computer Forensics* 70.

330 Brooks *A+ Certification Concepts & Practice* 449.

331 Kruse and Heiser *Computer Forensics* 74.

332 Kuchta 2002 *Information Systems Security* 45. See also paragraph 2.3.2.1 and 2.3.2.1. above for a reference to computer forensic images.

333 Meta-data can be seen as "data about the data". O'Reilly and Derting 2002 *Computers and Law (C&L) Litigation Support* 37. A data dictionary (DBMS) is a repository for meta-data, that is, data about each file in the database and each field within those files. See Shelly *Discovering Computers* I.05. See also paragraph 2.2.1 above.

334 Such as the original author of the document, the document title, the creation date, hidden notes and changes. O'Reilly and Derting 2002 *Computers and Law (C&L) Litigation Support* 37.

335 O'Reilly and Derting 2002 *Computers and Law (C&L) Litigation Support* 38.

336 The file system (file management system) is the organisational structure that operating systems employ to organise and track files. See Brooks *A+ Certification Concepts & Practice* 943. Formatting organises and prepares a disk to receive data, in other words, to receive a file system. See CSIR-Defencetek *CSIR FACTS* 41. Examples of different file systems are the following: a file allocation table (FAT, or also commonly called FAT16) which is used in approximately 70% of all personal computers; FAT 32; a high performance file system (HPFS) NTFS from Windows NT; Netware from Novell; ISO 9660 used for CD-ROMs and ISO 13346 used for DVDs; universal disk format (UDF) for big capacity disks such as a DVD RAM; and the UNIX filing system. The file system knows where files are saved. It finds and reads the relevant sectors and delivers the data to the operating system. All disks are divided into 512 byte sectors, which is the standard size for the smallest disk unit. Sectors are created when the circular disk is organised into concentric tracks. Each track is divided into sectors. See Kruse and Heiser *Computer Forensics* 74. A cluster (called "blocks" in UNIX systems) is a group of disk sectors. The operating system assigns a unique number to each cluster and then keeps track of files according to which clusters they use. The cluster concept is an administrative invention and is also called an allocation unit. The number of sectors gathered in one cluster depends on the disk size. See CSIR-Defencetek *CSIR FACTS* 46. When a new file is written to a hard disk, the file is stored in one or more clusters that are not necessarily next to each other; they may be rather widely scattered over the disk. When you read a file, the operating system reassembles the file from clusters and places it as an entire file where you want to read it. See SearchExchange.comDefinitions "File Allocation Table" found on the Internet http://searchexchange.techtarget.com/sDefinition/0,,sid43_gci213956,00.html 1. Clusters that are not in use have been described as "kind of hanging out electronic benchwarmers waiting for the coach to call them back into the game". See Kruse and Heiser *Computer Forensics* 73.

337 Kruse and Heiser *Computer Forensics* 72.

338 As opposed to data being intentionally hidden by the suspect. Steganography (where data is secreted within files that appear to be normal) is a data hiding technique that is deployed within the operating system's filesystem. It must, however, be kept in mind that a lot of data hiding techniques do not necessarily involve this type of intimacy with the hard drive and the filesystem. An example of such a technique would be encryption and compression, where the existence of the data is obvious to anyone who looks, but the meaning or content of the obfuscated data is not discernable. See Kruse and Heiser *Computer Forensics* 106 and paragraph 2.3.1.3 above.

overwritten at some indefinite time in the future.[339] File system areas that contain deleted data include, for example, unallocated space and slack space.[340] Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file.[341]

2.5.1.3 Categories of computer systems

Due to rapidly evolving technology, computer categories cannot be demarcated precisely, but are generally categorised on the basis of differences in the size, speed, processing capabilities and price of computers. The six main categories of computers are discussed below.

2.5.1.3.1 Personal computer:

A personal computer contains at least one input device, one output device, one storage device, a memory and a processor, which constitute its basic building blocks. A personal computer can perform all of its input, processing, output and storage activities by itself. A stand-alone desktop computer is a computer that can perform the information processing cycle operations (input, process, output and storage) without being connected to a network. The stand-alone desktop, however, commonly also has networking capabilities. The two best known series of personal computers are the Apple Macintosh (operated using the Macintosh operating system) and the PC and compatibles (operated using the Windows operating system).[342] The notebook or laptop computer and the desktop computer are two important subcategories of personal computers.[343] A workstation desktop is a more powerful desktop computer that requires intense calculations and graphics. Workstations are commonly used in fields such as engineering, desktop publishing and graphic art.[344]

2.5.1.3.2 Handheld computers (palmtop computers)

A handheld computer is a small computing device that can easily fit into one's one hand while the other hand is used to operate it.[345] An example of this is the personal digital assistant (PDA). A handheld computer typically does not have disk drives but instead stores data on chips inside the system unit or on miniature storage media.[346] Like web-enabled cellular telephones and pagers, web-enabled handheld computers allow wireless access to the Internet.[347]

---

339 Kruse and Heiser *Computer Forensics* 74.
340 The unused space in a disk cluster. See also paragraph 2.3.1.3.1 above.
341 Webopedia "Slack Space" found on the Internet http://www.pcweopedia.com/TERM/s/slack_spcae.html 1.
342 Shelly *Discovering Computers* 1.19.
343 Shelly *Discovering Computers* 1.20.
344 Shelly *Discovering Computers* 1.21.
345 Answers.com "Handheld device" found on the Internet http://www.answers.com/topic/handheld-device?method=22 1.
346 Shelly *Discovering Computers* 1.23.
347 Shelly *Discovering Computers* 1.24.

2.5.1.3.3 Internet appliances (information appliances)

An Internet appliance is a computer with a limited functionality, the main purpose of which is to enable novice users to connect to the Internet from home. An example of this is the set-top box.[348] The proliferation of Internet appliances is a crucial component of ubiquitous computing.[349]

2.5.1.3.4 Servers

Servers are powerful network computers that contain the network operating system and manage network resources for other computers.[350] Servers are typically shared by multiple users.[351] If a desktop computer is powerful enough, it can also function as a server on a network. A server manages the resources on the network, by controlling access to software, printers and centralised storage areas.[352] The other computers on the network are called clients. They can, for example, access the contents of the central storage area on the server.[353] A mid-range server is more powerful and larger than a workstation computer, often supporting up to 4000 users at the same time. Users typically access a mid-range server via a personal computer or a terminal. A terminal is a device with a monitor and a keyboard and it does not have processing power. Therefore terminals cannot act as stand-alone computers, but must be connected to a server or mainframe to operate.[354]

2.5.1.3.5 Mainframes

A mainframe is a large, expensive, very powerful computer that can handle hundreds or thousands of connected users simultaneously. A mainframe can also act as a server in a network environment and can store vast amounts of data.[355] Mainframes are ultra-high-performance computers made for high-volume, processor-intensive computing. They are typically used by large businesses and for scientific purposes.[356] Although mainframes are historically associated with centralised rather than distributed computing, nowadays users can access the mainframe with terminals or personal computers.[357]

---

348 Shelly *Discovering Computers* 1.25.
349 SMD Definitions "Internet appliance" found on the Internet http://searchsmb.terchtarget.com/sDefinition/0,190660,sid44_gci914561,00.html 1.
350 Brooks *A+ Certification Concepts & Practice* 953.
351 Answers.com "Server" found on the Internet http://www.answers.com/server 1.
352 Shelly *Discovering Computers* 1.21.
353 Shelly *Discovering Computers* 1.22.
354 Shelly *Discovering Computers* 1.25.
355 Shelly *Discovering Computers* 1.26.
356 Google "Definitions of Mainframe on the Web" found on the Internet http://www.google.com/search?hl=en&lr=&ie-ISO-8859-1&q=define%3A+mainframe 3.
357 Search390.com Definitions "Mainframe" found on the Internet http://search390.techtarget.com/sDefinition/0,,sid10_gci212516,00.html 1.

2.5.1.3.6 Supercomputers

A supercomputer is the fastest, most expensive and most powerful type of computer. Hence, it is capable of processing more than 12 trillion instructions in a single second. An example of a supercomputer is the IBM supercomputer, which covers an area the size of two basketball courts. Weather forecasting, nuclear energy research and petroleum exploration applications use supercomputers.[358] Supercomputers, however, are typically designed for single processes, whereas mainframes can usually execute many programs simultaneously, at a high speed.[359]

2.6 Categories of computing environments – who moved my bit?

The environment associated with computers that are targeted for electronic evidence collection has a vital impact, *inter alia*, on the way the collection is done, the collection potential and the human resources needed to successfully conclude the collection of the sought-after electronic evidence. How computers are connected and what functions they perform determine how the electronic evidence may be gathered.[360] In terms of the definition of a computer system in article 1(a) of the Cybercrime Convention, a computer system may be stand-alone or may be connected to a network with other similar devices. It is also quite possible that a collection site contains a combination of these two computing environments.

Stand-alone and networked computing environments are briefly considered below. In elucidating the networked computing environment, the following issues are referred to: the theoretical network reference model; network control strategies; network topologies; network transmission media and the different categories of computer networks. Lastly, special consideration is given to the Internet and the services it offers.

2.6.1 Stand-alone computing environments

A computer system can stand on its own. A central processing unit, an input device and an output device are by definition required to complete a computer. In addition to these devices, supplementary devices for input, output or storage may be present. What defines a stand-alone computer is that it is self-contained; in other words, it is not directly connected to another computer, and it has its own operating system. Stand-alone computers are inherently finite, meaning that most evidence is found in one place, rendering the search for electronic evidence self-limited. In a stand-alone environment, the storage and operating system are all attached to

---

358 Shelly *Discovering Computers* 1.26.

359 Google "Definitions of Mainframe on the Web" found on the Internet http://www.google.com/search?hl=en&lr=&ie-ISO-8859-1&q=define%3A+mainframe 3.

360 See FBI/CART *Conducting Searches in a Computer Environment* (Rev 2/21/97) 6-8, in respect of search and seizure interventions, specifically.

the computer. In order to search for evidence on a stand-alone computer, one must have possession and control of the target stand-alone machine.[361]

A desktop personal computer is a classic example of a stand-alone computing environment. If a desktop personal computer, however, connects to the Internet, it is no longer a stand-alone system but is, instead, connected to a network of networks.[362]

2.6.2 Networked computing environments

In the Explanatory Report to the Cybercrime Convention, a network is defined as "an interconnection between two or more computer systems".[363] A network may be geographically limited to a small area, or it may span a large area (even the globe), and such networks may themselves be interconnected. Computer systems may be connected to a network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.[364] When a computer connects to a network, it is considered to be online.[365]

The definition of a computer system in the Cybercrime Convention does not restrict the manner by which the devices or group of devices may be interconnected. These interconnections may be earthbound, wireless or both. The distinction between telecommunications and computer communications and the distinctions between their respective infrastructures are blurring with the convergence of telecommunications and information technologies.[366] This coming together of formerly distinct technologies, industries and/or activities enables novel uses of data, new services and products, as well as faster and more flexible communications.[367] The most common usage of the term refers to the convergence of the computing, communications and broadcasting sectors in terms of industry structures and technologies as a result of digitisation.[368] The Internet is, of course, the *locus classicus* of all convergence. With the advent of the Internet and higher bandwidth data transmission, programs and data that are part of the same overall project can be distributed over a network, manifesting the Sun Microsystems slogan: "The network is the computer."[369]

---

361 FBI/CART *Conducting Searches in a Computer Environment* (Rev 2/21/97) 6–7.
362 Tanenbaum *Computer Networks* 2. See paragraph 2.6.2.5 below for a discussion of the different categories of computer networks.
363 The Council of Europe's Explanatory Report to the Cybercrime Convention 6.
364 The Council of Europe's Explanatory Report to the Cybercrime Convention 6.
365 Shelly *Discovering Computers* 1.17 and 9.11.
366 The Council of Europe's Explanatory Report to the Cybercrime Convention 40.
367 Whatis.com "Target Search"™ found on the Internet http://whatia.techtarget.com/definition/0,,sid9_gci211837,00.html 1.
368 Google "Definitions of Convergence on the Web" found on the Internet http://www.google.com/search?hl=en&lr-&ie=UTF –8&oi-defmore&q=define:Convergence 1.
369 SearchWin2000.com Definitions "Computer" found on the Internet http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci211829,00.html 1.

In a classic mainframe environment, there is one large computer that has all the resources. The mainframe is the sole and central brain of the computer system. The terminals attached to this computer merely constitute its input and output devices and the terminals have no processing power. Because all storage in a classic mainframe environment is located within the central processing unit, it follows that the storage location of the electronic evidence is singular. Due to the nature of mainframes, however, seizure is not a practical option, except in extraordinary circumstances. This contrasts with a classic stand-alone environment, where the computer, as such, can be physically seized. Mainframes require specialist electrical and air conditioned physical facilities and are always unique. Although the central processing unit and peripheral devices are standard, their interface to each other is installation-dependent. The operating systems are also device-dependent and they often require the services of a programmer, systems engineer or administrator who is familiar with that particular installation.[370]

Mainframe environments have also been termed centralised computing networks. A well-known contemporary example of this is bank ATMs that run over a centralised network.[371] Some of the advantages of centralised networks include simultaneous access to the most recent data and the ease of backing up data, since all data is stored on a centralised server. Consequently, only the centralised server needs to be secured, as the terminals have no data and do not require floppy drives, reducing the chances that the network will be infected with viruses. Centralised computing is cost-effective in that the terminals are inexpensive, because they require no real processing or storage capability of their own. Some of the disadvantages of centralised networks include its slow network access and connectivity, due to the fact that all users must connect to one central site. Centralised computing also allows for fewer options for meeting a variety of user needs. Due to these limitations, most networks today do not deploy a centralised processing computing model.[372] Contemporary mainframe computing, furthermore, tends to combine the features of a classic mainframe and stand-alone environments.[373]

The essential difference between a networked computing environment, as opposed to both the classic mainframe and stand-alone computing environments, is that the resources of all of the attached computers within a network constitute a whole. Networks may, to some degree, inherit all the characteristics of a stand-alone environment, in that individual computers attached to the network for the purposes of increased functionality may also be able to function as stand-alone machines. The fact that networks are not finite has a profound impact on evidence collection interventions. Information may be found almost anywhere on the network, which makes identifying storage on a network intriguing and problematic. The targeted electronic evidence

---

370 FBI/CART *Conducting Searches in a Computer Environment* (Rev 2/21/97) 8.
371 Nash *Networking Essentials MCSE Study Guide* 9.
372 Nash *Networking Essentials MCSE Study Guide* 10.
373 Search390.com Definitions "Mainframe" found on the Internet http://search390.techtarget.com/sDefinition/0,,sid10_gci212516,00.html 1.

may be associated with a single computer (in a client-server network) or it may be associated with each of the attached computers (in a peer-to-peer or P2P network), or both.[374] It must be noted that the volume of information and potential *e*-evidence contained in a network environment is generally much larger than that in a stand-alone environment.

Distributed computing is the opposite of centralised computing, in that data storage and processing is done on a local workstation in a distributed computing network model. This allows for more rapid access to data, less powerful and expensive servers and the possibility to accommodate users with a variety of needs, whilst allowing them to share data, resources and services.[375] Some of the drawbacks of distributed computing include virus susceptibility, backup difficulty and file synchronisation with several copies of a file stored throughout the network. Collaborative computing is similar to distributed computing, with the added functionality of allowing computers to share processing power across a network. This type of network model can be extremely fast, because users are not limited to the processing power of one system to complete tasks.[376]

Due to the general-purpose nature of computer networks and, in particular, their ability to add new functionality to the network by writing software that runs on affordable, high-performance computers, computer networks have grown enormously. They are now positioned to provide a wide range of services to hundreds of millions of users.[377] Some of these types of network service include the following:[378]

(a) **file services**, which facilitate the easy and seamless sharing of files;[379]

(b) **print services**, which provide the ability to share different types of print devices;[380]

(c) **message services**, which allow for emails with attachment files to be sent over the network, as well as for sharing calendars and scheduling information by using the email backbone;

(d) **directory services**, which maintain information about all the objects in a network[381] and allow users to have only one user account on the entire network and to connect to any resource that support those directory services;

---

374 See paragraph 2.6.2.2 below for a discussion of network control strategies.
375 Nash *Networking Essentials MCSE Study Guide* 11.
376 Nash *Networking Essentials MCSE Study Guide* 11.
377 Peterson and Davie *Computer Networks: A Systems Approach* 51.
378 Nash *Networking Essentials MCSE Study Guide* 21 – 23.
379 The primary reason for networking computers is for the file services that a network can provide. File services include file transfer (the ability to share files and information across a network, albeit it within a building or over great distances); file storage (see paragraph 2.5.1.1 above for a discussion of different types of storage) and file migration (moving data from one form of storage to another); file update synchronisation (the ability to keep track of and coordinate different versions of the same file); archiving the processes of backing up data in case of a hard disk failure). See Nash *Networking Essentials MCSE Study Guide* 21 – 23.
380 Print services can be enhanced to allow for fax services and queue-based printing (allowing the spooling of a print job to a server). See Nash *Networking Essentials MCSE Study Guide* 23.

(e) **application services**, which allow client computers to let the central network servers process data for them;[382] and

(f) **database services**, which coordinate multiple changes and update replicated databases to keep them current.

Networks are complicated structures with many interrelated parts and, as such, pose considerable challenges when they are targeted as an environment from which to gather electronic evidence. A basic understanding of the underlying technicalities of networks is pivotal, not only for executing electronic evidence collection interventions, but also for analysing the legalities that affect these interventions.

2.6.2.1 Theoretical network reference models

A network model provides a conceptual framework that enables a better understanding of the complex interactions taking place among the various devices on a network.[383] In order for computers to communicate, there must be accepted rules of communication, in other words, a protocol. A protocol defines almost every aspect of the language that is used for computers to communicate.[384] For communication to take place on a network composed of a variety of network devices, these rules must be clearly defined. Networking models attempt to define these rules.[385]

---

381 Such as the users, printers, shared resources and servers.

382 An example of this would be the querying of a large database that is stored on a central database server. The server, not the client, would actually search the database. Nash *Networking Essentials MCSE Study Guide* 30.

383 A network model is like a generic car that consists, *inter alia*, of wheels, a drive-train, an engine and suspension. Whereas one car may have an automatic transmission, another may have a manual one and whereas one car may have disk brakes, another may have drums. Likewise, every network has, *inter alia*, a physical layer, a data link layer and a network layer. One network may implement the physical or data link layer differently than another, but they are both networks and they both have the layers in one form or another. The theoretical network explains networking concepts, but just as a theoretical car will not get you to the grocery store, a theoretical network will not get your data to the server. See Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 122.

384 See Nash *Networking Essentials MCSE Study Guide* 37. Some common protocols are Internetwork Packet Exchange (IPX); Transmission Control Protocol/Internet Protocol (TCP/IP) and NetBIOS Extended User Interface (NetBEUI). A *de jure* standard refers to a standard designed by one company or organisation that normally maintains control of the protocol and is responsible for any additions or changes. A *de facto* standard indicates a protocol controlled by the entire industry and it is therefore also known as an industry standard. Anyone can use a *de facto* standard free of charge. When a company does not publish specifications for a protocol, it is considered a closed standard. If the specifications are published, then it is an open standard. Most *de jure* standards can be either open or closed standards and all *de facto* standards are open. TCP/IP and IPX are both open protocols. See Nash *Networking Essentials MCSE Study Guide* 37. A protocol stack is a group of protocols arranged on top of each other as part of a communication process. Each layer of the OSI model (see footnote 386 below) has different protocols associated with it. When more than one protocol is needed to complete a communication process, the protocols are grouped together in a stack. An example of a protocol stack is TCP/IP, which is widely used for UNIX and the Internet. Each layer in the protocol stack receives services from the layer below it and provides services to the layer above it. For two computers to communicate, the same protocol stacks must be running on each computer. Each layer of the protocol stack on one computer communicates with its equivalent, or peer, on the other computer. The computers can have different operating systems and still be able to communicate if they are running the same protocol stacks. For example, a DOS machine running TCP/IP can communicate with a Macintosh machine running TCP/IP. See Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 124.

385 These rules apply, *inter alia*, to the following issues: how network devices contact each other; and, if they have different languages, how they communicate with each other; methods by which a device on a network knows when to transmit data and when not to; methods to ensure that network transmissions are received correctly and by the right recipient; how the physical transmission media are arranged and connected; how to ensure that network devices maintain a proper rate of data flow and how bits are represented by network media. See Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 123.

The term "spaghetti code" is universally understood to be an insult, because good computer scientists passionately underscore modularity. Computer networks are unique in that the "proper" modularity has been handed down in the form of an international standard: the seven-layer reference model of network protocols from the ISO. This model is almost universally used as a starting point for understanding networks, albeit in that the network design in question conforms to the model or deviates from it.[386] The OSI model simply defines which tasks need to be done and which protocols handle those tasks in each of the seven layers of the model, i.e:

(a) **the physical layer**, which transforms data into bits that are sent across the physical media;

(b) **the data link layer**, which packages databits into frames and determines access to the network media;[387]

(c) **the network layer**, which converts databits into dataframes and routes data through a large internetwork in the best possible way, using connectionless transmission to a specified network address;[388]

(d) **the transport layer**, which packages data into segments and which provides end-to-end, reliable connections using connection-orientated transmissions;

(e) **the session layer**, which packages data into packets[389] and which allows users to establish connections using easily remembered names[390] by providing a name space

---

386 The ISO began developing the Open Systems Interconnection (OSI) reference model in 1977 and released it in 1984. See Peterson and Davie *Computer Networks: A Systems Approach* Foreword. See, however, Tanenbaum *Computer Networks* 37, where the two most important network architectures are cited as the OSI (Open Systems Interconnection) Reference Model and the TCP/IP (Transmission Control Protocol/ Internet Protocol) Reference Model. The OSI and TCP/IP reference models have much in common, *inter alia*, the fact that neither of these models and their protocols is perfect.

387 The data link layer contains the media access control and logical link control sublayers. The media access control sublayer is responsible for access to the network media using a contention system (where any device can transmit when it needs to, such as Ethernet) or a deterministic system (where a device first possesses the right to transmit before it can transmit, such as Token Ring). Another way of controlling access to media is by means of addressing; the data link layer is responsible for the physical addresses of devices on the network. Every device on a network has a hard-coded address attached to it that is usually assigned during production, called a MAC address. See Nash *Networking Essentials MCSE Study Guide* 43. The logical link control sublayer establishes and maintains network connections and performs flow control and error checking. See Nash *Networking Essentials MCSE Study Guide* 63. Error control is implemented using cyclic redundancy checks (CRCs) and checksums. A CRC is a method of detecting errors in the transmission of data. Before the data is sent, a CRC number is calculated by running the data through an algorithm and producing a unique number. At the receiving end of the transmission, the data is run through the same algorithm to produce the number. If the numbers match, the data was sent error-free. The unique value generated from the algorithm is called a checksum. See Nash *Networking Essentials MCSE Study Guide* 47.

388 The network layer uses the processes of switching, routing and addressing to find the most efficient route through the network. The type of datagram switching that a service or application may use depends on how quickly the data needs to be delivered. There are three main methods of switching, namely circuit switching (done by means of a dedicated connection between the two communicating devices); message switching (data is stored and sent in whole from device to device across the network); and packet switching (combining circuit and message switching by breaking data into small pieces and routing them from device to device). See Nash *Networking Essentials MCSE Study Guide* 50-51. The network layer is also responsible for correctly routing packets across a network, by setting up a table to show the shortest routes between two networks. These tables can either be dynamic (where the network administrators are not required to enter any information, because all the configuration settings can be detected by the network routers) or static (where the routing tables are set up manually by administrators). See Nash *Networking Essentials MCSE Study Guide* 51. The network layer is also concerned with getting data from one computer to another, even if the computers are on a different network. A device on a network, therefore, not only has a device address (MAC address), but also a network address that tells other computers where to locate that device. By using this network address, the sending device can tell whether the destination device is on the same network segment (local) or on another network segment (remote). Nash *Networking Essentials MCSE Study Guide* 52.

389 Sometimes the term "packet" is used as a generic term for describing data at any layers. See Nash *Networking Essentials MCSE Study Guide* 41.

that is used to tie together the potentially different transport streams that are part of a single application;[391]

(f) **the presentation layer**, which negotiates data packet exchange formats, including data compression, decryption and translation;[392] and

(g) **the application layer**, which transforms packets into messages and which provides the interface between the user's application and the network.[393]

The original designs for TCP/IP were started long before the OSI model was developed. Instead of the OSI's seven-layer model, TCP/IP was based on a United States Department of Defense model with four layers. The four layers can be loosely matched to the OSI model in the following ways:[394]

(a) **The network access layer** corresponds to the physical and data link layers of the OSI model. When TCP/IP was developed, it was made to use existing standards for these two layers, so it could work with such protocols as Ethernet and Token Ring. Over the years, TCP/IP has been shown to run over almost any type of network connection from FDDI (fiber distributed data interface) to radio wave.

(b) **The Internet layer** roughly matches up with the network layer of the OSI model. Both these layers are responsible for moving data to other devices on the network. Internet Protocol (IP) is mainly responsible for this job.

(c) **The host-to-host layer** is similar to the transport layer of the OSI model. The job of both these layers is to communicate between peers on the network. As a result, almost all devices on a TCP/IP network are considered hosts, whether they are workstations, servers or network-attached printers.

(d) **The process/application layer** does the same job as the top three layers of the OSI model, which is to provide network services.

2.6.2.2 Network control strategies

Computers play three roles in a network, namely clients (which use but do not provide network resources), peers (which both use and provide network resources) and servers (which provide

---

390 To establish a session, the user must provide the remote address to which she wants to connect. These addresses are not like MAC addresses or network addresses; they are intended for users and are easier to remember. Examples are DNS names (www.microsoft.com) or computer names (SERVER41). Nash *Networking Essentials MCSE Study Guide* 55.

391 See Peterson and Davie *Computer Networks: A Systems Approach* 26-27.

392 The presentation layer translates information between different types of network devices, because some devices read bits and bytes in different directions. Should the destination device receive the information out of order, the data would be extremely garbled. Three translation services are therefore bit order, byte order and character codes translation. Computers also use binary character codes (such as EBCDIC and ASCII) to represent the numbers, punctuation marks and letters to represent the numbers that they use. The presentation layer is also responsible for this character code translation. Nash *Networking Essentials MCSE Study Guide* 56-57. See paragraph 2.2.1 above for a discussion of character codes.

393 The OSI application layer should not be confused with the actual application that the user is running. See paragraph 2.5.1.2.1 above for a discussion of application software. Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 123.

394 See Nash *Networking Essentials MCSE Study Guide* 171.

network resources). Each of these computer roles is determined by the type of operating system that the computer uses.[395] Computer networks can consist of two different types: server-based and peer-to-peer.[396] In fact, most networks consist of a combination of the two types, and such networks are called hybrid networks. A hybrid network is a client-server network that also has peers that share resources.

Peer-to-peer is a communications model in which each party has the same capabilities; and either party can initiate a communication session. In recent usage, the term peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server. IBM's Advanced Peer-to-Peer Networking (APPN) is an example of a product that supports the peer-to-peer communication model. On the Internet, peer-to-peer is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and access files directly from one another's hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software. Large producers of content, including record companies, have expressed their concern about what they consider illegal sharing of copyrighted content by suing some peer-to-peer users. Meanwhile, corporations are looking at the advantages of using peer-to-peer as a way for employees to share files without the expense involved in maintaining a centralised server, and as a way for businesses to exchange information with each other directly.[397]

Peer-to-peer is the simplest form of networking. In a peer-to-peer network, each workstation acts as both a client and a server; and there is no central server.[398] Small, inexpensive networks can easily be set up using peer-to-peer systems. The peer-to-peer network model works well for small office networks. Once a peer-to-peer network has reached about ten clients, it can become too hard to maintain. This type of network is common in home networks and is typically the type of network most businesses use when they make the decision to share resources and connect their individual systems. All that is needed to connect several individual systems and create a peer-to-peer network are network adapters, cables or other transmission media and the operating system.[399] Peer networks are organised into workgroups.[400]

---

395 Servers run network operating systems such as Windows NT Server or Novell Netware. Clients run client operating systems, such as Windows 95 or the Macintosh operating system. Each of these operating systems is optimised to provide the service for the role it plays. Often the role of a computer is also determined simply by use. For instance, a computer running Windows 95 is not a peer unless it is actually sharing network resources. This means that it may be in use only as a client or that it may not be in a network at all. It is also possible to run Windows NT Server simply as a client operating system, although it does not make much sense to use a powerful operating system in that role. Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 14.

396 See Nash *Networking Essentials MCSE Study Guide* 13.

397 SearchNetworking.com Definitions "Peer-to-Peer" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html 1. Bowrey states that the current popularity of peer-to-peer's points, *inter alia*, to frustration at the way computers have come to be controlled by "plodding IT nerds at work, at universities and via ISPs". These IT experts decide what the terms of the user's engagement with technology will be. She contends that these experts are motivated by "their own interest in an easy life and pleasing the CEO with the stability and security of their unadventurous IT systems." She concludes that peer-to-peer technology can cut such intermediaries out of the technological loop. See Bowrey *Law and Internet Cultures* 144.

398 See Nash *Networking Essentials MCSE Study Guide* 13.

399 See Nash *Networking Essentials MCSE Study Guide* 14.

The term "client-server" describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. Although the client-server idea can be used by programs within a single computer, it is more important in a network. In a network, the client-server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client-server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program, which then sends a request to a database server at another bank computer to retrieve your account balance. The balance is returned to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you.

Security in a peer-to-peer network can be difficult to maintain. Users need to know how to secure their own resources. Because there is no central administration, it is the users' responsibility to ensure that only authorised users can access their data. The users themselves handle sharing of the data, as well as setting any permissions that may be needed. Most peer-to-peer security consists of a single password for each resource; this is known as share-level security. Share-level security requires a user to know the password for a resource before it can be accessed. Users usually need access to a variety of resources and they must often remember a different password for each resource. If an unauthorised person gains possession of the resource password, the password must be changed and all the authorised users must be informed of the new password.[401]

The client-server model has become one of the central ideas of network computing. Most business applications being written today use the client-server model. So does the Internet's main program TCP/IP. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "monolithic" centralised computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client-server model and have become part of network computing.

In the usual client-server model, one server (sometimes called a daemon) is activated and it awaits client requests. Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, a Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which is technically called a Hypertext

---

400 Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 16.
401 See Nash *Networking Essentials MCSE Study Guide* 15.

Transport Protocol or HTTP server) in another computer somewhere on the Internet. Similarly, a computer with TCP/IP installed allows for making client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet. Other program relationship models include master/slave (where one program is in charge of all other programs) and peer-to-peer (with either of two programs able to initiate a transaction).[402]

Server-based networks are the most popular network type today, due to the ease of accessing and backing up data. Security is easily maintained, since a user normally has an account on the central server to which the user's account is tied. This way, an administrator can grant or deny access to one single account per user, instead of having to give each user an account on everyone's workstation, as in a peer-to-peer network.[403] This type of security is known as user-level security.[404] In a server-based network, there is one computer which is dedicated to handing out files and/or information to clients.[405] Since the server is dedicated to handing out files and/or information, it cannot be used as a workstation. Its purpose is strictly to provide services to other computers, not to request services. Servers are optimised to hand out information as rapidly as possible. As the network grows, more than just a single server is required to handle all requests from clients. Different servers may be required to handle different tasks. The two main types of dedicated servers are the file and print server and the application server. Specialised servers, such as mail servers and communications servers, are set up to handle remote users dialling into a network.[406]

Server-based (or client-server) networks divide processing tasks between clients and servers. Clients (often called the "front end") request services, such as file storage and printing, and servers (often called the "back end") deliver them. In Windows NT, server-based networks are organised into domains. Domains are collections of networks and clients that share security trust information. Domain security and logon permission are controlled by special servers called domain controllers. No computer user can access the resources of servers in a domain until she has been authenticated by a domain controller.[407]

All three types of computers operate on hybrid networks. Such networks generally have active domains and workgroups. This means that while most shared resources are located on servers, network users still have access to any resources that are shared by peers in the same

---

402 SearchNetworking.com Definitions "Client/Server" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci211796,00.html 1.
403 See Nash *Networking Essentials MCSE Study Guide* 20.
404 See Nash *Networking Essentials MCSE Study Guide* 19.
405 See Nash *Networking Essentials MCSE Study Guide* 16.
406 See Nash *Networking Essentials MCSE Study Guide* 17.
407 Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 15.

workgroup. It also means network users do not have to log on to the domain controller to access workgroup resources shared by peers.[408]

2.6.2.3 Network topologies

A network topology is the configuration, or physical arrangements, of the devices in a communications network.[409] Topology can include such aspects as the transmission media, adapters and physical design of the network. The four commonly used physical network topologies are the bus, star, ring and mesh.[410] Networks usually use combinations of these topologies. The logical topology, however, usually does not match the appearance of the physical topology, due to the fact that most contemporary network installations employ connection devices. Connection devices alter the appearance of the actual connection scheme; and the particulars of the connection scheme are hidden inside the connecting device.[411] Typical connectivity devices include hubs, repeaters, bridges, routers and gateways.

2.6.2.4 Network transmission media

A communications channel is the path through which information passes between two devices. Bandwidth is the width of the communications channel. The higher the bandwidth, the more data and information the channel can transmit. A communications channel consists of one or more transmission media. Transmission media consist of materials or techniques capable of carrying one or more signals. Data is most likely to travel over a variety of transmission media, especially when the transmission is sent a long distance.[412] Baseband media can transmit only one signal at a time. By contrast, broadband media can transmit multiple signals simultaneously. Media that use broadband transmit signals much faster than those that use baseband. Digital subscriber lines (DSLs), cable television networks and satellites offer broadband transmission.

Transmission media are one of two types: physical or wireless. Physical transmission media use wire, cable and other tangible (touchable) materials to send communications signals. Physical transmission media include the following: twister-pair cable, coaxial cable and fibre-optic cable. Wireless transmission media send communications signals through the air or space using radio, microwave and infrared signals.[413] Wireless transmission media are used when it is inconvenient, impractical or impossible to install cables and include the following: broadcast radio, cellular radio, microwaves, communications satellite and infrared.

---

408 Chellis, Perkins and Strebe *MSCE: Networking Essentials Study Guide* 17-18.
409 Shelly *Discovering Computers* 9.16.
410 See Nash *Networking Essentials MCSE Study Guide* 121.
411 Brooks *A+ Certification Concepts & Practice* 275.
412 Shelly *Discovering Computers* 9.31.
413 Shelly *Discovering Computers* 9.32.

The public-switched telephone network (PSTN) is the worldwide telephone system that handles voice-oriented telephone calls. With the exception of the final link from the local telephone company to the home, today's telephone system is mostly digital. Data, instructions and information are sent of the telephone network using a dial-up line or a dedicated line. The transfer rate is the speed at which a line carries data and information. Rates can range from thousands of bits per second (bps) to billions of bits per second. Four popular types of digital dedicated line are Integrated Services Digital Network (ISDN), digital subscribed line (DSL), T-carrier line and asynchronous transfer mode (ATM).[414]

2.6.2.5 Categories of computer networks

The subject of computer networking covers many different kinds of networks, large and small, well-known and less well-known. Computer networks may have different goals, scales and technologies.[415] An overview of the best-known computer networks is provided below.

2.6.2.5.1 Local area network (LAN)

A local area network (LAN) is a network that connects computers and devices in a limited geographic area (such as a school, office, laboratory or a group of buildings), or closely positioned group of buildings.[416] Each computer or device on the network is a node. Often, the nodes are connected to the LAN via cables. A wireless LAN (WLAN) is a LAN that uses no physical wires. WLANs use wireless media such as radio waves instead.[417]

A peer-to-peer LAN is a simple, inexpensive network that typically connects fewer than ten computers. Each computer on a peer-to-peer network can share hardware or data located on any other computer on the network. Each computer stores files on its own storage devices. Thus, each computer on the network contains both the network operating system and application software. All computers on the network share any peripheral device(s) attached to any computer. Peer-to-peer networks are ideal for very small businesses and home users.[418]

A client-server LAN is a network on which one or more computers act(s) as a server. The other computers on the network can request services from the server. A server, sometimes called the host computer, controls access to the hardware and software on the network and provides a centralised storage area for programs and data. The other computers on the network, called clients, rely on the server for these resources.[419] The main difference between the server computer and the client computers is that the server has more storage space and power than

414 Shelly *Discovering Computers* 9.42.
415 Tanenbaum *Computer Networks* 49.
416 Shelly *Discovering Computers* 1.16 and 9.12.
417 Shelly *Discovering Computers* 9.12.
418 Shelly *Discovering Computers* 9.13.
419 Shelly *Discovering Computers* 9.14.

the clients. Some servers, called dedicated servers, perform a specific task. So, for example, a file server stores and manages files. A print server manages printers and print jobs. A database server stores and provides access to a database. A network server manages the network traffic. Although it can connect a smaller number of computers, a client/server network typically provides an efficient means to connect ten or more computers. Most client/server networks have a network administrator because of the larger size of a client/server network. The network administrator is the operations person in charge of the network.[420]

2.6.2.5.2 Wide area network (WAN)

A wide area network (WAN) is a network that covers a large geographic area (such as one that connects district offices across the country or even the world) using a communications channel that combines many types of media, such as telephone lines, cables and air waves. A WAN can be one large network or can consist of two or more LANs connected together. The Internet is the largest WAN in the world.[421] A WAN may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.[422]

2.6.2.5.3 Metropolitan area network (MAN)

A metropolitan area network (MAN) is a backbone network that connects local area networks in a metropolitan area such as a city or town and handles the bulk of communications activity, or traffic, across that region. A MAN typically includes one or more LANs, but covers a smaller geographic area than a WAN.[423] A MAN is usually managed by a consortium of users or by a single network provider that sells the service to the users. Local and state governments, for example, regulate some MANs. Telephone companies, cable television operators and other organisations provide users with connections to the MAN.[424]

2.6.2.5.4 Storage Area Network (SAN)

A storage area network is a high-speed special-purpose network that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users. Typically, a storage area network is part of the overall network of computing resources for an enterprise.[425]

---

420 Shelly *Discovering Computers* 9.15.
421 Shelly *Discovering Computers* 9.15. See paragraph 2.6.3. below.
422 Whatis.com SearchNetworking.com Definitions "Wide area network" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214117,00.html 1.
423 Whatis.com searchNetworking.com Definitions "Metropolitan area network" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214083,00.html 1.
424 Shelly *Discovering Computers* 9.16.
425 Whatis.com searchStorage.com Definitions "Storage Area Network" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212937,00.html 1.

2.6.2.5.5 Home networks

Multiple computers in a home or home office can be connected with a home network. All the computers in the house can then be connected to the Internet at the same time. Each computer can share peripherals such as a scanner, printer or a DVD drive. Four types of home networks are Ethernet network, HomePLC (powerline) network, a phoneline network and HomeRF (radio frequency) network. Many vendors offer home networking packages that include all the necessary hardware and software to network a home using these techniques. Some also offer intelligent network capabilities. An intelligent home network also extends the basic home network to include features such as lighting control, thermostat adjustment and a security system.[426]

2.6.2.5.6 Virtual private networks

When a mobile user connects to a main office using the Internet, a virtual private network (VPN) provides the mobile user with a secure connection to the company network server, as if the user had a private line. VPNs help to ensure that transmitted data is safe from being intercepted by unauthorised people.[427]

2.6.2.5.7 Intranets and extranets

Recognising the efficiency and power of the Internet, many organisations apply Internet and Web technologies to their own internal networks.[428] An intranet is an internal network that uses Internet technologies. Intranets generally make company information accessible to employees and facilitate working in groups. Simple intranet applications include electronic publishing of organisational materials such as telephone directories, event calendars, procedure manuals, employee benefits information and job postings. In addition, an intranet normally includes a connection to the Internet. More sophisticated uses of intranets include groupware applications such as project management, chat rooms, newsgroups, group scheduling and video-conferencing. An intranet is essentially a small version of the Internet that exists within an organisation. It uses TCP/IP technologies, has a Web server, supports multimedia Web pages coded in HTML and is accessible via a Web browser such as Microsoft Internet Explorer or Netscape Navigator. Users can post and update information on the Intranet by creating and posting a Web page, using a method similar to that used on the Internet.[429]

---

426 Shelly *Discovering Computers* 9.22.
427 Shelly *Discovering Computers* 9.11.
428 Whatis.com SearchWebServices.com Definitions "Intranet" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212377,00html 1.
429 Shelly *Discovering Computers* 9.20.

Sometimes a company uses an extranet, which allows customers or suppliers to access part of its intranet. An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers or other businesses. An extranet can be regarded as part of a company's intranet that is extended to users outside the company.[430] Federal Express, for example, allows customers to access its intranet to print air bills, schedule pickups and even track shipped packages as they travel to their destinations.[431] As a public network, anyone with the proper connection can access the Internet. A private corporate intranet or extranet, by contrast, restricts access to specific authorised users.

2.6.3 The biggest WAN of all – the Internet and the World Wide Web

The world's most famous and largest network is the Internet.[432] The Internet is a worldwide collection of networks[433] that links together millions of businesses, government agencies, educational institutions and individuals. Because an abundance of resources and data are accessible via the Internet, more than 459 million users use the Internet for a variety of reasons.[434] The Internet is indeed many things to many people.[435]

The Internet is a public, cooperative and self-sustaining facility accessible to millions of people worldwide. Physically, the Internet uses a portion of the total resources of the existing public telecommunications networks. Technically, what distinguishes the Internet from other networks is its use of a set of protocols called TCP/IP (Transmission Control Protocol/ Internet Protocol). Two recent adaptations of Internet telephony, the intranet and the extranet, also use the TCP/IP protocol.[436]

Today, the Internet no longer has a simple hierarchical structure. It is made up of many wide and local area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continuously changing.[437]

---

430 Whatis.com searchSecurity.com Definitions "Extranet" found on the Internet http://searchsecurity.techtarget.com/sDefinition/0,,sid_gci212089,00.html 1.

431 Shelly *Discovering Computers* 9.20.

432 Tanenbaum argues that, despite considerable confusion in the literature, neither the Internet nor the WWW can technically be defined as a network. The Internet is not a single network but a network of networks; and the Web is only a distributed system that runs on top of the Internet. The key distinction between a distributed system and a network is that, in a distributed system, a collection of independent computers appears to its users as a single coherent system, like Web pages in the case of the WWW. See Tanenbaum Computer Networks 2.

433 Strömer named the Internet "Die Mutter aller Netze" (this can be translated as "The mother of all networks"). See Strömer TH *Online-Recht Rechtsfragen im Internet* 3.

434 Shelly *Discovering Computers* 1.17.

435 Gahtan, Kratz and Mann *Internet Law A Practical Guide for Legal and Business Professionals* 1.

436 Whatis.com searchWebservices.com Definitions "Internet" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212370,00.html 1.

437 Forouzan and Fegan *TCP/IP Protocol Suite* 4.

The main communication path for the Internet is a series of networks, established by the United States government, to link supercomputers together at key research sites. This pathway is referred to as the backbone and is affiliated with the National Science Foundation (NSF). Since the original backbone was established, the Internet has expanded around the globe and offers access to computer users in every part of the world.[438] The Internet is a fully connected communications tool. Internet access is provided in tiers. The top is composed of major Internet Service Providers directly connected to the Network Access Points, which connect with one another in a peer arrangement. These Internet Service Providers then offer access to smaller, local Internet Service Providers that are often better equipped to service businesses and individuals than the major Internet Service Providers. Internet Service Providers are divided into the following three service scopes:

(a) Local Internet Service Providers provide dial-up or digital Internet access directly to the consumer.

(b) Internet Service Providers provide the high-speed intermediary access between local Internet Service Providers and the primary Internet backbone.

(c) Value-added Internet Service Providers offer specialty servers like Web-site hosting, email and security firewalls.[439]

Article 1(c) of the Cybercrime Convention defines a "service provider" as[440]

> ...any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.

This definition of service provider encompasses a broad category of persons that play a particular role with regard to communicating or processing data on computer systems. Both public and private entities that provide users with the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether services are free of charge or provided for a fee. A closed group can, for example, be the employees of a private enterprise to whom the service is offered by a corporate network. The term also extends to those entities that store or otherwise process data on behalf of other persons. For example, under this definition, a service provider includes services that provide hosting and caching services, as well as services that

438 Brooks *A+ Certification Concepts & Practice* 303.
439 Byrne JJ *I-Net Certification Study System* 29.
440 The Council of Europe's Explanatory Report to the Cybercrime Convention 3.

provide a connection to a network. However, a mere provider of content[441] is not intended to be covered by this definition if such a content provider does not also offer communication or related data processing services.[442]

Section 1(1) of the RICPCIA defines an Internet service provider as any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or such a service is provided under and in accordance with a telecommunications service licence issued to the first-mentioned person under chapter V of the Telecommunications Act.[443]

Technologies available for establishing Internet connectivity include LAN, Digital Subscriber Line (DSL), Cable: Integrated Service Digital Network (ISDN), Dial-up, Satellite, and Wireless.[444]

Netiquette, which is short for Internet etiquette, is the code of acceptable behaviour users should follow when on the Internet; that is the conduct expected of individuals while they are online. Netiquette includes rules for all aspects of the Internet, including the WWW, email, FTP, newsgroups and message boards, chat rooms and instant messaging.[445]

The Internet is constructed of resources, or services, offered to users. A uniform resource locater (URL) is used to access services on the Internet.[446] The different services available on the Internet include the following:

(a) **The World Wide Web (WWW)**: The WWW is a menu system that ties together Internet resources from around the world. These resources are scattered across computer systems everywhere. Web servers inventory the Web's resources and store address pointers (referred to as links) to them. To access a Web site, the user must place the desired uniform resource locator (URL) on the network. Each URL begins with http:// of https://.[447] Web pages are accessed and viewed using a software program called a Web

---

441 Such as a person who contracts with a web hosting company to host her Website.

442 The Council of Europe's Explanatory Report to the Cybercrime Convention 6.

443 See footnote 65 in paragraph 2.2.1.1.2 above for the definition of an Internet Service Provider in the Schedule to the Electronic Communications Bill.

444 Brooks *A+ Certification Concepts & Practice* 305.

445 Shelly *Discovering Computers* 2.37.

446 Brooks *A+ Certification Concepts & Practice* 335.

447 A URL is composed of two parts. The first part specifies an Internet resource that is to be accessed. HTTP or FTP are examples of an Internet resource. Frequently, the resource is the name of a particular protocol. For example, both FTP and HTTP are well-established protocols used on the Internet. The second part of a URL lists the name of the server (also referred to as the domain name). The server name is followed by the directory path and file name of a particular document. Other common ways of referring to an Internet name are to call it a Web address, Internet address or Website. This is a reference to the static IP addresses assigned to the server name. See Brooks *A+ Certification Concepts & Practice* 335 and Networking Definitions "URL" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,290660,sid7_gci213251,00.html 1. A static IP address is a number that is assigned to a computer by an Internet service provider to be its permanent address on the Internet. Computers use IP addresses to locate and talk to each other on the Internet, much the same way people use phone numbers to locate and talk to one another on the telephone. When the Internet was first conceived, its architects did not foresee the need for an unlimited number of IP addresses. Consequently, there are not enough IP numbers to go around. Many Internet service providers limit the number of static IP addresses they

browser. The two most popular Web browsers are Microsoft Internet Explorer and Netscape Navigator.[448]

(b) **Electronic mail (Email)**: Email is the transmission of messages and files via a computer network. Email is quickly becoming a primary communications method for both personal and business use. Messages can be created, sent, received, forwarded, stored, printed and deleted using an email program.[449] An email address is a combination of a user name and a domain name that identifies a user in order to receive Internet email. A username, or user-id, is a unique combination of characters such as letters of the alphabet or numbers that identifies the user. Each username must be different from the other usernames in the same domain. In an Internet email address, an "@" symbol separates the username from the domain name. The domain name is supplied by the Internet service provider. Although no complete listing of Internet email addresses exists, several Internet sites list addresses collected from public sources. These sites also allow the voluntary listing of email addresses. As the user receives email messages, they are placed in a mailbox. A mailbox is a storage location usually residing on the computer that connects the user to the Internet, such as the server operated by the Internet Service Provider. The server that contains the mailboxes is often called a mail server. Most Internet service providers provide an Internet email program and a mailbox as a standard part of their Internet access services.[450] Some Web sites provide free email services. When an email message is sent, a program on the mail server determines how to route the message through the Internet and then sends the message. When the message arrives at the recipient's mail server, the message transfers to a POP or POP3 server. POP (Post Office Protocol) is a communications technology for retrieving email from a mail server. The POP server holds the message until the recipient retrieves it with her email software.[451]

(c) **File Transfer Protocol (FTP):** File transfer protocol is an Internet standard that allows the user to upload or download files with other computers on the Internet. For example, if the user clicks a link on a Web page that begins to download a file to her hard disk, she is probably using FTP.[452] It is the simplest way to exchange files between computers on

---

allocate, and economise on the remaining number of IP addresses they possess by temporarily assigning an IP address to a requesting Dynamic Host Configuration Protocol (DHCP) computer from a pool of IP addresses. The temporary IP address is called a dynamic IP address. See .Net Definitions "Static IP address/ dynamic IP address" found on the Internet http://searchvb.techtarget.com/sDefinition/0,290660,sid8_gci520967,00.html 1.

448 Shelly *Discovering Computers* 1.18.

449 Shelly *Discovering Computers* 2.30.

450 Hopkins *The Non-Profit's Guide to Internet Communications Law* 9 and Shelly *Discovering Computers* 2.31.

451 Shelly *Discovering Computers* 2.32. An anonymous remailer is a computer service which privatises email by stripping out the sender's name and email address before forwarding the email. It could be compared to dropping a letter in the post office without a return address. High-quality remailers are in sharp contrast to the privacy protection afforded to the normal email account at the average Internet Service Provider. There are four main types of remailers, i.e. cypherpunk anonymous remailers, mixmaster anonymous remailers, mixminion remailers and pseudonymous remailers. See Bacard "Anonymous Remailer FAQ" found on the Internet http://www.andrebacard.com/remail.html 1-7.

452 Shelly *Discovering Computers* 2.32.

the Internet.[453] A FTP server is a computer that allows users to upload and download files using FTP. A FTP site is a collection of files including text, graphics, audio, video and program files that reside on an FTP server. Some FTP sites limit file transfers to individuals who have authorised accounts (usernames and passwords) on the FTP server. Many FTP sites allow anonymous FTP, whereby anyone can transfer some, if not all, available files. Many program files on anonymous FTP sites are freeware or public domain software. Others are shareware. Large files on FTP sites often are compressed to reduce storage space and download time. Before a compressed file is used, it must be expanded with a decompression program, such as Winzip. Such programs are usually available for downloads from a FTP site. In some cases, the user may want to upload a file to a FTP site. For example, if the user creates a personal Web site, she will want to publish it on a Web server. Many Web servers require users to upload the files using FTP. To upload files from the user's computer to a FTP site, an operating system with FTP capabilities or a FTP program is used. Some Internet Service Providers include a FTP program as part of their Internet access service. Some FTP programs can also be downloaded from the Web.[454]

(d) **Newsgroups and message/bulletin boards**: A newsgroup is an online area in which users conduct a written discussion about a particular subject. To participate in a discussion, a user sends a message to the newsgroup, and other users in the newsgroup read and reply to the message. The entire collection of Internet newsgroups is called Usenet, which contains thousands of newsgroups on a multitude of topics. Some major topics areas include news, recreation, business, science and computers. A computer that stores and distributes newsgroup messages is called a news server. Many universities, corporations, Internet service providers and other large organisations have a news server. Some newsgroups require the user to enter a username and password to participate in the discussion. Only authorised members can use this type of newsgroup. To participate in a newsgroup, the user usually uses a program called a newsreader, which is included with most browsers. A popular Web-based type of discussion that does not require a newsreader is a message board. Many Web sites provide a message board, also called a discussion board. Message boards typically are easier to use than newsgroups.[455]

(e) **Mailing lists**: A mailing list is a group of e-mail names and addresses given a single name. When a message is sent to a mailing list, every person on the list receives a copy of the message in her mailbox. Some mailing lists are called LIST-SERVs, named after a popular mailing list software product. Thousands of mailing lists exist on a variety

---

453 Networking Definitions "File transfer protocol" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,290660,sid7_gci213976,00.html 1.

454 Shelly *Discovering Computers* 2.33.

455 Hopkins *The Non-Profit's Guide to Internet Communications Law* 10 and Shelly *Discovering Computers* 2.34.

of topics in areas of entertainment, business, computers, society, culture, health, recreation and education.[456]

(f) **Chat rooms**: A chat is a real-time typed conversation that takes place on a computer. In this instance, real-time means that the user and the people with whom she is conversing are online at the same time. As the user types on her keyboard, a line of characters and symbols is displayed on the computer screen. Others connected to the same chat room server can also see what the user has typed. In some chat rooms, the user clicks a button to see a profile on someone in the chat room. A chat room is a location on an Internet server that permits users to chat with each other. Anyone in the chat room can participate in the conversation, which is usually specific to a particular topic. Some chat rooms support voice chats and video chats, where the user hears or sees others and they can hear or see the user as she chats.[457] To start a chat session, the user connects to a chat server through a chat client. A chat client is a program on the user's computer. Today's browsers usually include a chat client. Chat clients can also be downloaded from the Web.[458]

(g) **Instant messaging (IM)**: Instant messaging is a real-time Internet communications service that notifies the user when one or more people are online and then allows her to exchange messages or files or join a private chat room with them. Many IM service also can alert the user to information such as calendar appointments, stock quotes, weather or sports scores. People use IM on all types of computer, including desktop computers and wireless computers such as notebook computers and Web-enabled devices. To use IM, software may have to be installed from an instant messaging service, sometimes called an instant messenger, onto the computer or device with which to use IM. Some operating systems, such as Windows XP, include an instant messenger. Thus, the user and all those individuals on her notification list need to use the same or a compatible instant messenger to guarantee successful communications.[459]

2.7 *Brouter*[460] *to chapter 3*

An understanding of the technicalities involved in the collection of electronic evidence begins with knowing that you do not know. This notion, coupled with the aspiration to remain relevant

---

456 See Whatis.com "Mailing list" found on the Internet http://whatis.techtarget.com/definition/0,289893,sid9_gci212515,00.html 1 and Shelly *Discovering Computers* 2.35.

457 Shelly *Discovering Computers* 2.35.

458 Shelly *Discovering Computers* 2.36.

459 Shelly *Discovering Computers* 2.36.

460 "Brouter" is the portmanteau word for a bridge router, a device that functions both as a router and a bridge. A brouter understands how to route specific types of packets, such as TCP/IP packets. Any other packets it receives are simply forwarded to other network(s) connected to the device (this is the bridge function). See Webopedia "Brouter" found on the Internet http://www.webopedia.com/TERM/B/brouter.html 1. A brouter is a network device that works as a bridge and a router. The brouter routes packets for known protocols and simply forwards all other packets as a bridge would. See Answers.com "Brouter" found on the Internet http://www.answers.com/brouter 1. In this context "brouter" denotes both a bridge of relevance to the next chapter and a router to the most important (within the context of the broader thesis) concluding remarks. See chapter 7 for a list of the findings extracted from the contents of chapter 2.

and meaningful in the Third Wave, could challenge protagonists of legal processes to their very (stereotypically egocentric) core. In its attempt to assist law enforcement practitioners, in particular, to rise to the occasion and meet some of these challenges, this chapter sought to serve three main purposes. The first aim was to familiarise the reader with the exceedingly complex technologies involved in computers and networks. The second aim was to provide a technical contextualisation of the research parameters. The third aim was to establish clarity on terminology typical of the collection of electronic evidence.

In firmly rooting the legalities which underpin the technicalities in the Cybercrime Convention and the relevant legislative provisions in South African law, the scene was set for a comparative analysis between the requirements of the Cybercrime Convention, detailed in the next chapter, and the South African *status quo*, elucidated in chapter 4 of this thesis.

CHAPTER 3:
SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION @ THE CYBERCRIME CONVENTION

3.1 BIOS BITS AND BYTES 96

3.2 THE CYBERCRIME CONVENTION 99

3.2.1 Historical background 99
3.2.2 Aims 101
3.2.3 Status 101
3.2.4 Interrelationship 103
3.2.5 Declarations and reservations 105
3.2.6 Amendments, settlement of disputes and consultations 106

3.3 DOMESTIC SEARCH AND SEIZURE IN COMPUTING ENVIRONMENTS 108

3.3.1 Requirements 108
3.3.1.1 Equivalence 108
3.3.1.2 Comprehensive legal authorisation to search or access 109
3.3.1.3 Extension of the search or access 109
3.3.1.4 Comprehensive legal authorisation to seize or similarly secure 110
3.3.1.5 Coerced cooperation 110
3.3.2 Scope 111
3.3.2.1 Specific criminal investigations or proceedings 112
3.3.2.2 Categories of crimes 112
3.3.2.3 Stored computer data 112
3.3.2.4 Jurisdiction 112
3.3.3 Conditions and safeguards 114
3.3.3.1 Domestic conditions and safeguards 115
3.3.3.2 Minimum international safeguards 115
3.3.3.3 Supervision by competent authorities 116
3.3.3.4 Proportionality 117
3.3.3.5 Third parties 117

3.4 TRANSBORDER SEARCH AND SEIZURE IN COMPUTING ENVIRONMENTS 119

3.4.1 Requirements 119
3.4.1.1 Search and seizure specific 119
3.4.1.2 General mutual assistance requirements 121
3.4.1.3 Mutual assistance requirements in the absence of applicable international agreements 123
3.4.2 Scope 126
3.4.2.1 Widest extent possible 126
3.4.2.2 Categories of crime 126

3.4.2.3 Stored computer data 127
3.4.2.4 Jurisdiction 127
3.4.3 Conditions and safeguards 127
3.4.3.1 Domestic fundamental requirements satisfied 127
3.4.3.2 Dual criminality 128
3.4.3.3 Prejudice to the sovereignty of the state and political offences 128
3.4.3.4 Prejudice to investigations or proceedings 128
3.4.3.5 Conditions in the discretion of the requested party 128
3.4.3.6 Confidentiality and use limitations 129
3.4.3.7 Data protection 130

3.5 DOMESTIC PRODUCTION ORDERS IN COMPUTING ENVIRONMENTS 131

3.5.1 Requirements for production orders 131
3.5.1.1 Domestic production orders 131
3.5.2 Scope 131
3.5.2.1 Specific criminal investigations or proceedings 131
3.5.2.2 Categories of crimes 132
3.5.2.3 Stored computer data 132
3.5.2.4 Jurisdiction 133
3.5.3 Conditions and safeguards 133
3.5.3.1 Domestic conditions and safeguards 133
3.5.3.2 Minimum international safeguards 133
3.5.3.3 Supervision by competent authorities 133
3.5.3.4 Proportionality 133
3.5.3.5 Third parties 133
3.5.3.6 Privileged categories of subscriber information 134
3.5.3.7 Confidentiality 134

3.6 INTERNATIONAL VARIANT: SPONTANEOUS PRODUCTION 134

3.6.1 Requirements 134
3.6.1.1 General mutual assistance requirements 135
3.6.1.2 Mutual assistance requirements in the absence of applicable international agreements 135
3.6.2 Scope 135
3.6.2.1 Widest possible extent 135
3.6.2.2 Categories of crime 136
3.6.2.3 Any computer data 136
3.6.2.4 Jurisdiction 136
3.6.3 Conditions and safeguards 136
3.6.3.1 Confidentiality and use limitations 136
3.6.3.2 Domestic fundamental requirements satisfied 137
3.6.3.3 Dual criminality 137
3.6.3.4 Conditions in the discretion of the requested party 137
3.6.3.5 Prejudice to the sovereignty of the state and political offences 137
3.6.3.6 Prejudice to investigations or proceedings 137
3.6.3.7 Data protection 137

3.7 DOMESTIC PRESERVATION AND PARTIAL DISCLOSURE ORDERS IN COMPUTING ENVIRONMENTS 137

3.7.1 Requirements 138
3.7.1.1 Domestic expedited preservation of stored computer data 138
3.7.1.2 Domestic expedited preservation and partial disclosure of traffic data 139
3.7.2 Scope 141
3.7.2.1 Specific criminal investigations or proceedings 141
3.7.2.2 Categories of crime 142
3.7.2.3 Stored computer data 142
3.7.2.4 Jurisdiction 143
3.7.3 Conditions and safeguards 143
3.7.3.1 Domestic conditions and safeguards 143
3.7.3.2 Minimum international safeguards 143

3.7.3.3 Supervision by competent authorities 144
3.7.3.4 Proportionality 144
3.7.3.5 Third parties 144
3.7.3.6 Confidentiality 144

3.8 TRANSBORDER PRESERVATION AND PARTIAL DISCLOSURE ORDERS IN COMPUTING ENVIRONMENTS 144

3.8.1 Requirements 145
3.8.1.1 Transborder expedited preservation of stored computer data 145
3.8.1.2 Transborder expedited disclosure of preserved traffic data 146
3.8.1.3 General mutual assistance requirements 146
3.8.1.4 Mutual assistance requirements in the absence of applicable international agreements 147
3.8.2 Scope 147
3.8.2.1 Widest extent possible 147
3.8.2.2 Categories of crime 147
3.8.2.3 Stored computer data 147
3.8.2.4 Jurisdiction 147
3.8.3 Conditions and safeguards 148
3.8.3.1 Domestic fundamental requirements satisfied 148
3.8.3.2 Dual criminality 148
3.8.3.3 Prejudice to the sovereignty of the state and political offences 149
3.8.3.4 Prejudice to investigations or proceedings 149
3.8.3.5 Conditions in the discretion of the requested party 149
3.8.3.6 Confidentiality and use limitations 150
3.8.3.7 Data protection 150

3.9 BROUTER TO CHAPTER 4 150

3.1 BIOS bits and bytes[1]

In the previous chapter, a contextualisation of the technicalities and terminology underpinning the deployment of search and seizure, production and preservation procedural devices in computing environments was provided. In doing so, care was taken to root the legalities associated with these technicalities in the Cybercrime Convention and the relevant legislative provisions in South African law. This technical contextualisation laid the foundation for a comparative analysis between the requirements of the Cybercrime Convention and the South African status quo. This chapter provides an exposition of the search and seizure, production and preservation mechanisms proposed in the Cybercrime Convention against which to measure the South African devices available.[2]

As contentious as it may be,[3] the Cybercrime Convention constitutes the current internationally agreed upon benchmark, *inter alia*, for the procedural powers aimed at the collection of

---

1 BIOS is an acronym for Basic Input and Output System. It refers to the set of routines in read-only memory that enables a computer to start the operating system and to communicate with the various devices in the system, such as disk drives, the keyboard, monitor, printer and communications ports. Also see the discussion in paragraph 2.2.1 above regarding bits and bytes. In this heading, it means some introductory bits and pieces with which to contextualise the search and seizure, production and preservation devices proposed in the Cybercrime Convention. It also broadly contextualises the relevance of this chapter within the overarching framework of this thesis.

2 An exposition of the South African search and seizure, production and preservation mechanisms are provided in chapter 4 of this thesis. The findings and recommendations based on a comparative analysis of these devices *vis-à-vis* those proposed in the Cybercrime Convention are listed in chapter 7.

3 Criticism against what has been described as the "closed, secretive and undemocratic" manner in which the Cybercrime Convention was drafted has been wide-spread. The treaty has been called a law enforcement wish-list. It is accused of lacking the balance which might have been contributed by the points of view of various groups, such as industry, users and public interest groups. See TreatyWatch.org "Eight Reasons the International Cybercrime Treaty Should Be Rejected" found on the Internet http://www.treatywatch.org.about/html 4; Taylor G "The Council of Europe Cybercrime Convention: A Civil Liberties Perspective" found on the Internet http://www.austlii.edu.au/au/other/CyberLRes/2001/30/ 2 and American Civil Liberties Union "Seven Reasons the Senate Should Reject the International Cybercrime Treaty" http://www.aclu.org//privacy/internet/14861res20031218.html 4. The Cybercrime Convention has been described as contrary to well-established norms for the protection of the individual in that it improperly extends the police authority of national governments. It is also feared that the Cybercrime Convention will undermine the development of network security techniques and that it will reduce government accountability in future law enforcement conduct. See Gruenwald 2000 *Interactive Week* 18. No fewer than 23 organisations, banding together under the banner of the Global Internet Liberty Campaign, have signed a letter condemning the 25th draft of the Cybercrime Convention in protest against what they have termed mere "cosmetic changes" to appease their concerns. They called the Cybercrime Convention "appalling" and warned that it handed law enforcement agencies "sweeping powers to snoop and could seriously erode online privacy". The Council of Europe has been chastised for refusing to open up the redrafting debates to non-governmental organisations and for ignoring the human rights concerns of organisations such as the American Civil Liberties Union, the Electronic Privacy Information Center and Privay International. See Ward "Treaty Could Stifle Online Privacy" found on the Internet http://news.bbc.co.uk/1/hi/sci/tech/1378482.stmm 2. The Council of Europe has also been accused of dispelling the "quaint myth" that legislative bodies were meant to be independent of national bureaucracies and responsive to the will of the people. The Cybercrime Convention is said overall to read like "some perverse decree drafted by that mighty triumvirate of paranoid fantasy, the Council on Foreign Relations, the Bilderberg Group and the Trilateral Commission in some world-domination free-for-all", rendering the "world-government rumours" not mere irrational fears. See Greene "Cybercrime Justifies World Government" found on the Internet http://www.theregister.co.uk/2001/0531cybercrime_justifies_world_government/pri... 1 and 4. In considering a proportionate and effective response against countering criminal use of the Internet, it has been recommended that the following tests be applied to any proposals made: the proposals must provide a clear net benefit for society; the proposed measures must discriminate effectively between criminals and honest, law abiding citizens; the proposals should be based on clearly defined policy objectives and should be enforceable, transparent and accountable; and the measures adopted must be the best in the sense that they are the most effective in countering criminal activity, while having the least impact on honest citizens and the lowest cost for taxpayers and businesses. See Cyber-Rights & Cyber Liberties (UK) "Cyber-rights vs Cyber-Crimes" found on the Internet http://www.cyber-rights.org/reports/palermo.html 1-2. The Cybercrime Convention has even been accused of hampering efforts to stop cybercrime and track down people who launch computer-related attacks. In moving too quickly in banning the tools used by hackers, the tools used by law enforcement will, by default, also be banned. See Perera R "Internet Business Group Calls for Delay in Cybercrime Treaty" found on the Internet http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,53469,00... 1.

electronic evidence. Once a large number of states have ratified a treaty such as the Cybercrime Convention, it becomes acceptable to treat it as general law. Treaties are, in fact, the only mechanisms that exist for adapting international law to new conditions and for strengthening the force of a rule of law between states.[4]

The adoption of the Cybercrime Convention was all but a peaceful one. This should perhaps be ascribed to the fact that its true motivations were, unfortunately, not always properly understood. Although few question the need for some kind of convention,[5] the Cybercrime Convention has been opposed by a wide variety of industry stakeholders, particularly by ones that seek a minimal global enforcement regime.[6] Countries also jealously guard their sovereignty, lest they have to sacrifice it on the altar of globalisation.

The Cybercrime Convention has, *inter alia,* been described as aimed at accommodating "flexible harmonisation", so as to achieve law enforcement goals designed to support the timely eradication of cybercrime. This has been explained against the background of an appreciation of the decentralised nature of international law, particularly in the sphere of criminal law enforcement. A sense for "what will fly" in the international body politic, which depends heavily on cultural understandings and differences, must always be a practical and necessary concern.[7]

The Cybercrime Convention has also been labelled "a potential tool for establishing hegemony in Internet regulation". It has been claimed that the intention is to export this hegemonic regulatory scheme to the rest of the world, rather than to harmonise the cybercrime laws of the current parties to the Cybercrime Convention.[8] The ethics of such exportation are said to have

---

4 Keyser 2003 J Transnational Law & Policy 296.

5 Conventions as a harmonisation model for international criminal enforcement have, however, also been subjected to criticism for several reasons. Several of these criticisms underscore what Miquelon-Weismann termed "the flawed approach to procedural harmonisation" in the Cybercrime Convention. Conventions are criticised on, *inter alia*, the following grounds: conventions may not come into force within a reasonable time because they are not ratified in time; conventions do not include any follow-up measures to ensure that ratification is followed by compliance; member states may express reservations that allow for exemption from certain operative provisions of the convention in question; the failure of the uniform interpretation of conventions is problematic; and linguistic and cultural differences translate into a serious concern about the prosecution of foreign nationals. The recognition of cultural differences among nations appears to be the greatest stumbling block to achieving harmonisation in the area of procedural due process. Miquelon-Weismann concludes that the decentralised nature of international law, particularly in the sphere of criminal law enforcement, may explain the Cybercrime Convention's accommodation of flexible harmonisation to achieve law enforcement goals aimed at the timely eradication of cybercrime. See Miquelon-Weismann 2005 *The John Marshall Journal of Computer & Information Law* 354 and 361.

6 In this respect, it has been argued that a strong regime for private enforcement must supplement public law enforcement. Private enforcement is particularly necessary for litigating against powerful corporate actors in cyberspace. A strong tort regime must teach Internet wrongdoers that "tort does not pay". Also, the remarkable capacity of the law of torts to adapt and evolve to meet new threats and dangers renders the law of tort an important instrument of social control. Private enforcement in the form of so-called "*E*-Cops" is already becoming well-established on the Internet, as many American Internet companies, for example, are sceptical about the role of government in detecting and punishing cybercriminals. Examples of such cybercops include the Internet Fraud Watch Group and the *e*-police force funded by the Software Publisher's Association (SPA). Another example can be found in the private investigators employed by the online auction house "E-Bay" to patrol its website. See Rustad 2001 *Southern California Interdisciplinary Law Journal* 96, 100 and 115.

7 See Miquelon-Weismann 2005 The John Marshall Journal of Computer & Information Law 354 and 361.

8 See Weber 2003 Berkeley Technology Law Journal 446.

been weighed up against the limited number of realistic alternatives.[9] If the Cybercrime Convention did not exist, as criminal activity becomes increasingly un-remediable by technological fixes and traditional mechanisms of international cooperation, countries might resort to unilateral assertions of power to conduct remote searches or otherwise assert jurisdiction to solve the problem of cybercrime. If digitally advanced countries fail to come to terms within the context of a treaty or similar instrument, then the jurisdictional problems of cybercrime legislation will continue to threaten state sovereignty.[10]

The overarching motivation, however, remains that the virtual impunity from which criminal conduct in cyberspace has seemed to benefit could no longer be tolerated without jeopardising both the future and the potential of computerised networks. The individual rights of all Internet users could simply not continue to be left unprotected against attacks committed against or through the networks. The Cybercrime Convention has to be regarded and understood as a first step in a resolute commitment to combat cybercrime.[11] Despite its flaws, the Cybercrime Convention is a welcome and long-overdue start towards addressing the exigent circumstances of the evolving Information Age. The Council of Europe deserves much credit for accepting the significant, but daunting, task of drafting the Convention.

The Cybercrime Convention is the only existing international tool that brings together nations so that "the world can fight cybercrime as one".[12] Information flows in international computer networks do not seem to respect national borders and the principle of territoriality, while law enforcement agencies are strictly bound to their national environment.[13] This renders international cooperation indispensable. The ultimate value of the Cybercrime Convention may be that it will attract more members over time. Its success will hinge upon the cooperation of all countries, both those that are parties to the Cybercrime Convention and those that are not.[14]

---

9 Fisher argues that the Cybercrime Convention is not an appropriate response to Internet crime. He recommends the following steps as a permissible course of action against cybercrime: strengthening the federal investigative and prosecutorial bodies; creating and strengthening a world-wide cybercrime investigations body within existing structures, such as Interpol; promoting the extradition of cybercriminals within existing extradition treaties; where no such extradition treaty exists within a nation, promoting the enactment of one by tying the signing of such an agreement to greater incentives, such as trade or foreign aid; encouraging foreign nations to update their criminal codes; and encouraging the training of foreign law enforcement officials and prosecutors to investigate and punish cybercriminals. See Fisher 2001 *The University of West Los Angeles (UWLA) Law Review* 360. Another alternative to the Cybercrime Convention is the establishment of a model cybercrime code. A model cybercrime code could be advantageous because it could be changed more easily. States could also maintain consistency between their own legislative schemes and the model code better. The process of developing such a model code might also yield superior solutions to the jurisdictional problems permeating cybercrime legislation. However, it has been argued that the establishment of a model cybercrime code is unlikely to be the hoped for panacea, as the worldwide harmonisation of cybercrime legislation would take even longer to achieve under such a model. Also, a successful model code is at any rate likely to replicate much of the content of the Cybercrime Convention. See Weber 2003 *Berkeley Technology Law Journal* 445.

10 See Weber 2003 Berkeley Technology Law Journal 446.

11 See Cyber-Rights & Cyber-Liberties "February 2002 – CoE Published the First Draft Version of the First Additional Protocol" found on the Internet http://www.cyber-rights.org/cybercrime/coe_archieve.htm 5.

12 Marler 2002 New England Law Review 219.

13 The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 6.

14 Hopkins 2003 Journal of High Technology Law 121.

The Cybercrime Convention is accordingly used as the yardstick against which the South African catalogue of criminal procedural search and seizure, production and preservation devices, as set out in the next chapter, can be measured. This chapter is focused on an exposition of both the domestic and the international search and seizure,[15] production[16] and preservation[17] devices proposed by the Cybercrime Convention. The requirements, scope and conditions, and safeguards applicable to these mechanisms are emphasised.

An introductory look-and-feel[18] of the Cybercrime Convention is provided below. The historical background to the Cybercrime Convention; its aims, status and interrelationships; declarations, reservations and amendments provided for; as well as the settlement of disputes and consultations are briefly examined.

3.2 The Cybercrime Convention

3.2.1 Historical background

In November 1996, the European Committee on Crime Problems (CDPC) decided to set up a committee of experts to deal with Cybercrime.[19] The Committee of Experts on Crime in Cyberspace (PC-CY) was established and commenced its work in April 1997.[20] Its terms of reference included, *inter alia*, the examination of the use, including the possibility of the transborder use, and the applicability of coercive powers in a technological environment within the framework of a binding international instrument. Between April 1997 and December 2000, the PC-CY held ten meetings in plenary and 15 meetings of its open-ended drafting group.[21]

---

15 See paragraphs 3.3 and 3.4 below.

16 See paragraphs 3.5 and 3.6 below.

17 See paragraphs 3.7 and 3.8 below.

18 "Look-and-feel" refers to the general appearance and operation of a user interface. See Webopedia "Look-and-feel" found on the Internet http://webopedia.com/TERM/l?look_and_feel.html 1. A user interface is the point of contact between a user and a computer program. See Webopedia "User interface" found on the Internet http://www.webopedia.com/TERM/U/user_interface.html 1. In this context, it means a general overview of the Cybercrime Convention.

19 As *per* decision CDPC/103/211196 of the CDPC. This was based on the rationale that only a binding international instrument can ensure the necessary efficiency in the fight against both those new crime phenomena, directed against the integrity, availability and confidentiality of computer systems and telecommunication networks, as well as traditional offences committed by using such networks or their services. The point of departure was that a legal instrument with more engagement than a recommendation was required. The CDPC took into account the report prepared at its request by Professor H W K Kaspersen (Kasperson *Implementation of Recommendation N R (89) 9 on Computer-Related Crime CDPC (97)5 and PC-CY (97)5* 106). Similar sentiments already emerged from the Council of Europe's Report Attached to Recommendation N R (89) 9 Concerning Substantive Law (Computer-related crime, Report by the European Committee on Crime Problems) 86 and from the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 2, 3 and 38. See also the Council of Europe's Explanatory Report to the Cybercrime Convention 1 and 2.

20 As *per* decision CM/Del/Dec(97)583, taken at the 583rd meeting of the Ministers' Deputies to the Committee of the Council of Europe (hereinafter referred to as the Ministers' Deputies) held on 4 February 1997. See also the Council of Europe's Explanatory Report to the Cybercrime Convention 2.

21 The European Ministers of Justice twice expressed their support for the negotiations on the Cybercrime Convention. Resolution No 1, adopted at their 21st Conference (Prague, June 1997), recommended that the Committee of Ministers of the Council of Europe (hereinafter referred to as the Committee of Ministers) support the work carried out by the CDPC on cybercrime in order to bring domestic criminal law provisions closer to each other and to enable the use of effective means of investigation concerning such offences. Resolution No 3, adopted at the 23rd Conference of the Committee of Ministers (London, June 2000), encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of states to become parties to the Cybercrime Convention. It also acknowledged the need for a swift and efficient system of international cooperation, which duly takes into account the specific requirements of

Based on a decision taken by the PC-CY, the 19th draft version of the Cybercrime Convention was declassified and released in April 2000. It was followed by subsequent drafts released after each plenary meeting, in order to enable the negotiating states to consult with all interested parties.[22]

After the expiry of its extended terms of reference,[23] the PC-CY experts held three more meetings under the auspices of the CDPC. The purpose was to finalise the draft Council of Europe's Explanatory Report to the Cybercrime Convention and to review the draft Cybercrime Convention in the light of the opinion of the Parliamentary Assembly, adopted at the 2nd part of its plenary session in April 2001.[24]

The revised and finalised 27th draft Cybercrime Convention and the Council of Europe's Explanatory Report to the Cybercrime Convention were submitted for approval to the CDPC at its 50th plenary session in June 2001.[25] The Committee of Ministers subsequently adopted both documents at its 109th session on 8 November 2001. The Cybercrime Convention was opened for signature in Budapest on 23 November 2001 at the International Conference on Cybercrime.[26]

On 7 November 2002, the Committee of Ministers adopted an Additional Protocol to the Convention on Cybercrime. It concerned the Criminalisation of Acts of a Racist and Xenophobic Nature. They also adopted the Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature.[27] On 28 January 2003, these documents were opened in Strasbourg for signature by

---

the fight against Cybercrime. The member states of the European Union expressed their support of the work of the PC-CY through a Joint Position, adopted in May 1999. The Council of Europe's Explanatory Report to the Cybercrime Convention 4.

22 Taylor "The Council of Europe Cybercrime Convention: A Civil Liberties Perspective" found on the Internet http://www.austlii.edu.au/au/other/CyberLRes/2001/30/ 2.

23 As *per* decision No CM/Del/Dec(99)679 of the Ministers' Deputies. The PC-CY was due to finish its work by 31 December 1999, but was unable to do so, whereupon its terms of reference were extended until 31 December 2000. See the Council of Europe's Explanatory Report to the Cybercrime Convention 4.

24 In October 2000, the Parliamentary Assembly was requested by the Committee of Ministers to give an opinion on the draft Cybercrime Convention. See the Council of Europe's Explanatory Report to the Cybercrime Convention 4.

25 Out-Law News "Final form of the Cybercrime Convention Wins Approval" found on the Internet http://www.out-law.com/page-1751 1.

26 The Council of Europe's Explanatory Report to the Cybercrime Convention 4.

27 The Council of Europe "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems Strasbourg, 28.I.2003" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/189 (hereinafter referred to as the Council of Europe's Explanatory Report to the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature). During the negotiations around the Cybercrime Convention, parties were strongly divided about whether the Cybercrime Convention should criminalise the dissemination of racist and xenophobic material in computer networks. This diversity is also very well reflected in the number and nature of reservations to the International Convention on the Elimination of All Forms of Racial Discrimination, New York, December 21, 1965, in force as of January 4, 1969 (commonly referred to as the CERD-Convention). The CERD-Convention has so far been signed by 137 states, including South Africa, the United Kingdom and the United States. Many reservations were, however, expressed by countries such as Belgium, France, Ireland, Italy, Japan, Switzerland, the United Kingdom, the United States and Australia. See Kaspersen "Cyber Racism and the Council of Europe's reply" found on the Internet http://www.hreoc.gov.au/racial_discrimination/cyberracism/kaspersen.html 11. A copy of the CERD-Convention can be found at http://www.unhchr.ch/html/menu3/b/d_icerd.htm. The drafters of the Cybercrime Convention could not reach consensus on the issue of the criminalisation of other content-related offences, such as the distribution of racist propaganda through computer systems. Although there was strong support for the inclusion of

the member states that had signed the Cybercrime Convention.[28]

3.2.2 Aims

The Cybercrime Convention is aimed principally at[29]

(a) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;[30]

(b) providing for the domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, as well as of other offences committed by means of computer systems or evidence in relation to such offences in electronic form;[31] and

(c) setting up a fast and effective regime for international cooperation.[32]

The Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature extends the scope of the Cybercrime Convention to cover offences related to racist or xenophobic propaganda. It not only addresses the harmonisation of the substantive law elements of offences of racist or xenophobic propaganda, but also allows for the utilisation of the Cybercrime Convention's domestic and international procedural powers against these types of offences.[33]

3.2.3 Status

The Cybercrime Convention is intended to be a binding international instrument. Article 36(3) set the initial number of ratifications, acceptances or approvals required for the Cybercrime Convention to come into force at five, of which at least three must be Council of Europe members. The Cybercrime Convention accordingly entered into force on 1 July 2004 after its

---

such acts as criminal offences, some delegations, particularly from the United States, expressed concern about including such provisions on the grounds that they inhibited freedom of expression. The Committee of Ministers subsequently entrusted the CDPC, specifically its Committee of Experts on the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (hereinafter referred to as the PC-RX) with the task of preparing the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature and its Explanatory Report. See the Council of Europe's Explanatory Report to the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature 2. It has been pointed out that the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature may represent the first step in the "zoning of cyberspace – in which access to content may be restricted based on the user's citizenship and domicile". See CNN.com/Law Center "Can Europe Block Racist Web Sites From its Borders" found on the Internet http://www.cnn.com/2003/LAW/02/06/findlaw.analysis.ramasastry.cyberlaw/index.ht... 2.

28 The Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature 1.

29 The Council of Europe's Explanatory Report to the Cybercrime Convention 4.

30 See sections 1 and 3 of chapter II of the Cybercrime Convention.

31 See sections 2 and 3 of chapter II of the Cybercrime Convention.

32 See chapter III of the Cybercrime Convention.

33 See the Council of Europe's Explanatory Report to the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature 2.

ratification by Albania, Croatia, Estonia, Hungary and Lithuania.[34] In respect of any party which subsequently expresses its consent to be bound by it, the Cybercrime Convention enters into force on the first day of the month following the expiration of a period of three months after the date of the expression of the state's consent to be bound[35] or after the date when its accession instrument has been deposited.[36]

The Cybercrime Convention is also a treaty of global ambition and article 37(1) allows for other states to be invited to accede to the Cybercrime Convention. Canada, Japan, South Africa and the United States of America have actively participated in the elaboration of the Cybercrime Convention and were thus also allowed to sign up in terms of article 36(1).[37] However, so far, none of these states have ratified the Cybercrime Convention. To date, 42 states have signed the Cybercrime Convention and 11 have ratified it.[38]

Although the text of the Council of Europe's Explanatory Report to the Cybercrime Convention does not constitute an instrument providing an authoritative interpretation of the Cybercrime Convention, it might facilitate the application of the provisions contained therein.[39]

The Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature has been signed by 25 states.[40] Following its ratification by five states, as required in terms of article 10(1), it entered into force on 1 March 2006.

---

34 Jones "Council of Europe Convention on Cybercrime: Themes and Critiques" found on the Internet http://www.sims.berkeley.edu/~cjones/Full%20Text%20Papers/Council%20of%20Europe%20Convention%20on%20Cybercrime%20–%20Themes%20and%20Critiques.pdf 3

35 Article 36(4) of the Cybercrime Convention.

36 Article 37(2) of the Cybercrime Convention.

37 The Council of Europe's Explanatory Report to the Cybercrime Convention 63.

38 The member states of the Council of Europe that signed the Cybercrime Convention are listed below. The first date in brackets following the name of the signatory party indicates the date of signature; the second date, if any, indicates the date of ratification; followed by a third date, if any, that denotes the date when the Cybercrime Convention came into force in the country concerned. The signatory parties to the Cybercrime Convention are the following: Albania (23 November 2001; 20 June 2002; 1 July 2004), Armenia (23 November 2001), Austria (23 November 2001), Belgium (23 November 2001; 17 October 2002; 1 November 2004), Bosnia and Herzegovina (9 February 2005), Bulgaria (23 November 2001; 7 April 2005; 1 August 2005), Croatia (23 November 2001), Cyprus (23 November 2001; 19 January 2005; 1 May 2005), Czech Republic (9 February 2005), Denmark (22 April 2003; 21 June 2005; 1 October 2005), Estonia (23 November 2001; 12 May 2003; 1 July 2004), Finland (23 November 2001), France (23 November 2001), Germany (23 November 2001), Greece (23 November 2001), Hungary (23 November 2001; 4 December 2003; 1 July 2004), Iceland (30 November 2001), Ireland (28 February 2002), Italy (23 November 2001), Latvia (5 May 2004), Lithuania (23 June 2003; 18 March 2004; 1 July 2004), Luxembourg (28 January 2003), Malta (17 January 2002), Moldova (23 November 2001), the Netherlands (23 November 2001), Norway (23 November 2001), Poland (23 November 2001), Portugal (23 November 2001), Romania (23 November 2001; 12 May 2004; 1 September 2004), Serbia and Montenegro (7 April 2005), Slovakia (4 February 2005), Slovenia (24 July 2002; 8 September 2004; 1 January 2005), Spain (23 November 2001), Sweden (23 November 2001), Switzerland (23 November 2001), the former Yugoslav Republic of Macedonia (23 November 2001; 15 September 2004; 1 January 2005), the Ukraine (23 November 2001) and the United Kingdom (23 November 2001). Non-member states of the Council of Europe which are parties to the Cybercrime Convention include Canada (23 November 2001), Japan (23 November 2001), South Africa (23 November 2001) and the United States (23 November 2001). The website of the Council of Europe Treaty Office is a very useful source of information and can be found at http://conventions.coe.int. See the Council of Europe "Convention on Cybercrime CETS No.: 185" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG 1 and 2.

39 The Council of Europe's Explanatory Report to the Cybercrime Convention 1.

40 The member states of the Council of Europe that signed the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature are listed below. The first date in brackets following the name of the signatory party indicates the date of signature; the second date, if any, indicates the date of ratification; followed by a third date, if any, that denotes the date of entry into force of the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature in

3.2.4 *Interrelationship*[41]

The Cybercrime Convention is generally intended to supplement and not supplant existing multilateral and bilateral treaties and arrangements between parties.[42] Therefore, regarding general matters, the parties to the Cybercrime Convention should in principle apply such other existing treaties or arrangements. However, in respect of specific matters dealt with only by the Cybercrime Convention, the rule of interpretation *lex specialis derogat legi generali* provides that the parties should give precedence to the rules contained in the Cybercrime Convention.[43]

Consistent with the Cybercrime Convention's supplementary nature and its approach to international cooperation, article 39(2) provides that parties are free to apply agreements that are already in force, or that may come into force in the future. Article 39(2) also allows parties to assume more specific obligations, in addition to those set out in the Cybercrime Convention, when establishing their relations concerning matters dealt with in the Convention. Parties are, however, obliged to respect the objectives and principles of the Cybercrime Convention when applying other agreements. Therefore they cannot accept obligations that would defeat its purpose.[44] Parties may also agree to apply the international cooperation provisions set out in article 27 of the Cybercrime Convention in *lieu* of other agreements. Article 39(3) is a savings clause that ensures that the Cybercrime Convention leaves unaffected other rights, restrictions,

---

the country concerned. The signatory parties to the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature are the following: Albania (26 May 2003; 26 November 2004), Armenia (28 January 2003), Austria (30 January 2003), Belgium (28 January 2003), Bosnia and Herzegovina (9 February 2005), Croatia (26 March 2003), Cyprus (19 January 2005; 23 June 2005), Denmark (11 February 2004; 21 June 2005), Estonia (28 January 2003), Finland (28 January 2003), France (28 January 2003), Germany (28 January 2003), Greece (28 January 2003), Iceland (9 October 2003), Latvia (5 May 2004), Lithuania (7 April 2005), Luxembourg (28 January 2003), Malta (28 January 2003), Moldova (25 April 2003), the Netherlands (28 January 2003), Poland (21 July 2003), Portugal (17 March 2003), Romania (9 October 2003), Serbia and Montenegro (7 April 2005), Slovenia (26 February 2004; 8 September 2004), Sweden (28 January 2003), Switzerland (9 October 2003) and the Ukraine (8 April 2005). As for the non-member states of the Council of Europe, only Canada (8 July 2005) is currently a party to the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature. See the Council of Europe "Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (ETS No. 189)" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=10/11/2005&CL=ENG1 and 2.

41 The final provisions contained in chapter IV of the Cybercrime Convention (i.e. article 36: signature and entry into force; article 37: accession to the convention; article 39: effects of the convention; article 40: declarations; article 41: federal clause; article 42: reservations; article 44: amendments; article 45: settlement of disputes; article 46: consultations of the parties) are for the most part based on the Model Final Clauses for Conventions and Agreements concluded within the Council of Europe. The final clauses were approved by the Committee of Ministers at the 315th meeting of the Deputies in February 1980. These final provisions either use the standard language of the model clauses or are based on long-standing treaty-making practice at the Council of Europe. See the Council of Europe's Explanatory Report to the Cybercrime Convention 62. The interrelationship between conventions of the Council of Europe in relation to one another and/or other treaties, concluded outside of the Council of Europe, is not, however, dealt with by these proposed model clauses. See the Council of Europe's Explanatory Report to the Cybercrime Convention 64.

42 Article 39(1) mentions three Council of Europe treaties in particular as non-exhaustive examples: the 1957 European Convention on Extradition (ETS No 24), the 1959 European Convention on Criminal Matters (ETS No 30) and its 1978 Additional Protocol (ETS No 99). Furthermore, in determining the Cybercrime Convention's relationship to other international agreements, the drafters also concurred that parties may look for additional guidance to relevant provisions in the Vienna Convention on the Law of Treaties. See the Council of Europe's Explanatory Report to the Cybercrime Convention 65.

43 An example is article 30, which provides for the expedited disclosure of preserved traffic data when necessary to identify the path of a specified communication. In this specific area, the Cybercrime Convention, as a *lex specialis*, should provide a rule of first resort over provisions in more general mutual assistance agreements. See the Council of Europe's Explanatory Report to the Cybercrime Convention 64.

44 The Council of Europe's Explanatory Report to the Cybercrime Convention 65.

obligations and responsibilities that may exist, but that the Cybercrime Convention does not deal with.[45]

Article 8 of the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature addresses the relationship of this Additional Protocol with the Cybercrime Convention.[46] The extension of both the domestic procedural law provisions and the international cooperation provisions to include the racist and xenophobic propaganda offences created in terms of articles 2 to 7 of the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature is particularly important for this research.

Several articles of the Cybercrime Convention provide for the co-existence of domestic law and the treaty. So, for example, article 15 incorporates the conditions and safeguards under the domestic law of the parties to the procedural powers and procedures provided for in section 2 of the Cybercrime Convention. Article 23 requires the parties to cooperate with each other to the widest extent possible, *inter alia*, by applying the domestic laws of the parties. Article 26(1) provides for the spontaneous production of information obtained within the framework of a party's own investigations, within the limits of its domestic law. Article 29(3) requires parties, in adherence to a mutual legal assistance request, to take all appropriate measures to facilitate the expedited preservation of stored computer data in accordance with its domestic law. Article 31(2) facilitates mutual assistance regarding the accessing of stored computer data through the application of, *inter alia*, a party's domestic laws, as referred to in article 23. Articles 33 and 34 direct that mutual assistance regarding the real-time collection of traffic data and the interception of content data must be governed by the conditions and procedures provided for under the domestic laws of the relevant parties. Article 35 makes provision for facilitating assistance by the 24 hour, 7 day a week network. If this is permitted by a party's domestic law and practice, it provides for directly providing technical advice, preserving data pursuant to articles 29 and 30 and collecting evidence, giving legal information and locating suspects.

---

45 The Council of Europe's Explanatory Report to the Cybercrime Convention 65.

46 Article 8(1) postulates that articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Cybercrime Convention apply *mutatis mutandis* to the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature. In terms of article 8(2), the parties must also extend the scope of application of the measures defined in articles 14 to 21 and articles 23 to 35 of the Cybercrime Convention to articles 2 to 7 of the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature.

3.2.5 *Declarations and reservations*[47]

The Cybercrime Convention allows for article 40 declarations. These are considered acceptable interpretations of the Cybercrime Convention provisions and permit parties to include certain specified additional elements that modify the scope of certain provisions, in order to accommodate conceptual or legal differences among the parties.[48] These additional elements should be declared at the time of signature or when depositing an instrument of ratification, acceptance, approval or accession.[49] The declaration provided for in article 27(9)(e) of the Cybercrime Convention is relevant to this research. It provides that a party may require that, for reasons of efficiency, urgent requests made under article 27(9) must also be addressed to its central authority and may not be made directly to its judicial authorities.

Reservations in terms of article 42 of the Cybercrime Convention permit a party to exclude or to modify the legal effect of certain obligations set out in the Cybercrime Convention.[50] These reservations recognise that, for some parties, certain reservations are essential to avoid conflict with their constitutional or fundamental legal principles. To secure to the largest possible extent the uniform application of the Cybercrime Convention by as many parties as possible, article 42 constitutes a *numerus clausus* of possible reservations. A party may furthermore only make reservations at the time when it signs or deposits its instrument of ratification, acceptance, approval or accession. Although article 43 imposes no specific time limit for the withdrawal of reservations, it states that they should be withdrawn as soon as circumstances permit. The Secretary General of the Council of Europe may periodically enquire about the prospects for withdrawal.[51] The reservations provided for in articles 22(2), 29(4) and 41(1) are relevant to this research.

---

47 The following countries entered reservations and declarations in respect of the articles, listed next to the name of the country: Bulgaria (articles 14; 24, 27 and 35); Denmark (articles 9, 14 and 38); Estonia (articles 24, 27 and 35); Hungary (articles 9, 24, 27 and 35); Lithuania (articles 2, 4, 24, 27, 29 and 35); Romania (articles 24, 27 and 35); the former Yugoslav Republic of Macedonia (articles 24 and 27). See Council of Europe "Convention on Cybercrime CETS No.: 185" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG 1-6. Article 12(3) of the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature allows for declarations, requiring additional elements to the crimes of racist and xenophobically-motivated insults and the denial, gross minimisation, approval or justification of genocide or crimes against humanity as provided for in articles 5(2)(a) and 6(2)(a) of the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature. Article 8 incorporates articles 1, 12, 13, 14-21, 22, 23-35, 41, 44, 45 and 46 of the Cybercrime Convention into the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature. Denmark is the only country that has thus far entered reservations and declarations in respect of the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature: Denmark (articles 3, 5, 6 and 14). See Council of Europe "2993 Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (ETS No. 189)" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=10/11/2005&CL=ENG 1 and 2.

48 In terms of article 40, the possibility of requiring additional elements is provided for under article 2, article 3, article 6(1)(b), article 7, article 9(3) and article 27(9)(e).

49 Such notification is particularly important concerning the definition of offences, as the condition of dual criminality will have to be met by the parties applying certain procedural powers. See the Council of Europe's Explanatory Report to the Cybercrime Convention 65.

50 Article 42 refers to the reservations exclusively provided for in articles 4(2), 6(3), 9(4), 10(3), 11(3), 14(3), 22(2), 29(4) and 41(1).

51 The Council of Europe's Explanatory Report to the Cybercrime Convention 67.

Article 22(2) of the Cybercrime Convention provides that a party may reserve the right not to apply the jurisdiction rules laid down in article 22(1)(b), (c) and (d) or to apply them only in specific cases or conditions. Article 29(4) provides that a party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data, may reserve the right to refuse the request for the expedited preservation of stored computer data in cases where it has reason to believe that, at the time of disclosure, the condition of dual criminality cannot be fulfilled. This reservation applies only in respect of offences other than those established in accordance with articles 2 to 11 of the Cybercrime Convention.

Article 41 of the Cybercrime Convention allows for a reservation that accommodates minor variations in its applicability, as a result of the well-established domestic law and practice of a party that is a federal state. These variations must, however, be based on the Constitution or other fundamental principles concerning the division of powers in criminal justice matters between the central government and the constituent states or territorial entities of a federal state. The scope of application of the federal clause has been restricted to the provisions of chapter II. Federal states entering this reservation are still obliged to cooperate with the other parties under chapter III of the Cybercrime Convention. A federal state may also not apply the terms of such a reservation to exclude or substantially diminish its obligations to provide for the measures set out in chapter II. The federal government must refer provisions the implementation of which come within the legislative jurisdiction of the constituent states or other similar territorial entities to the authorities of these entities with a favourable endorsement in order to encourage them to take appropriate action to effect these provisions.[52]

Reservations and declarations made by a party to a provision of the Cybercrime Convention are *ipso facto* applicable to the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature.[53]

3.2.6 Amendments, settlement of disputes and consultations[54]

Despite its noble aspiration to technological neutrality, it is unlikely that the Cybercrime Convention will not be adapted. This is due to what has been called "technological

---

52 Article 41(3) of the Cybercrime Convention. The Council of Europe's Explanatory Report to the Cybercrime Convention 66.

53 Article 12(1) of the Council of Europe's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature. However, the parties may declare otherwise at the time of signature or when depositing an instrument of ratification, acceptance, approval or accession.

54 Articles 44, 45, and 46 of the Cybercrime Convention are made applicable on the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature by means of its article 8.

turbulence."[55] The drafters considered that major changes to the Cybercrime Convention could be made in the form of additional protocols. They therefore only provided for an amendment procedure that is mostly thought to be for relatively minor changes of a procedural and technical nature.[56] The parties themselves may examine the need for amendments or protocols under the consultation procedure provided for in article 46.[57] In seeking the uniform evolution of the Cybercrime Convention, any amendment adopted would, however, only come into force when all the parties have informed the Secretary General of their acceptance of such an amendment.[58]

The parties must keep the CDPC informed about their interpretation and application of the provisions of the Cybercrime Convention.[59] In this respect, the parties are obliged to seek a peaceful settlement of any dispute, and any procedure for solving disputes should be agreed upon by the parties concerned. Three possible mechanisms for dispute-resolution are suggested by article 45(2) of the Cybercrime Convention, namely the CDPC itself, an arbitral tribunal or the International Court of Justice.

Article 46 creates a framework for the parties to consult in respect of the implementation of the Cybercrime Convention, the exchange of information on significant legal, policy or technological developments pertaining to the subject of cybercrime and the collection of evidence in electronic form, and the possibility of supplementing or amending the Cybercrime Convention. The consultation procedure is flexible. It seeks to ensure that all parties to the Cybercrime Convention, including non-member states of the Council of Europe, could be involved in any follow-up mechanism on an equal footing, while preserving the competences of the CDPC.[60] A comprehensive review of the Cybercrime Convention must be conducted by the CDPC, in cooperation with the parties, before 1 July 2007.

---

55 This refers to the rapid and unpredictable development of new technologies and their applications. See Kaspersen "Cyber Racism and the Council of Europe's reply" found on the Internet http://www.hreoc.gov.au/racial_discrimination/cyberracism/kaspersen.html 9.

56 Article 44 of the Cybercrime Convention.

57 The Council of Europe's Explanatory Report to the Cybercrime Convention 67.

58 Article 44(5) of the Cybercrime Convention.

59 Article 45(1) of the Cybercrime Convention.

60 The CDPC must not only be kept regularly informed of the consultations taking place among the parties, but must also facilitate such consultations and assist the parties in their efforts to supplement or amend the Cybercrime Convention. Given the needs of the effective prevention and prosecution of cybercrime and the associated privacy issues, the potential impact on business activities, and other relevant factors, the views of interested parties, including law enforcement, non-governmental and private sector organisations, may be useful to these consultations. See the Council of Europe's Explanatory Report to the Cybercrime Convention 68.

3.3 Domestic search and seizure in computing environments

The domestic search and seizure mechanisms proposed in article 19 of the Cybercrime Convention[61] are considered below against the introductory overview provided in the preceding paragraph. The requirements, scope, conditions and safeguards applicable to these proposed domestic search and seizure devices are highlighted.

3.3.1 Requirements

3.3.1.1 Equivalence

Article 19 of the Cybercrime Convention provides for the procedural power at a national level to search and seize stored computer data. Article 19 aims specifically to establish, in those jurisdictions where stored computer data *per se* is not considered to be a tangible object, an equivalent power of search and seizure in respect of computer data, as opposed to tangible objects.[62] Many of the characteristics of a traditional search remain,[63] but additional procedural provisions are necessary to ensure that computer data can be obtained in a manner that is as effective as the search and seizure of a tangible data carrier.[64] Examples of such additional

---

61 In accordance with article 39(3), nothing in the Cybercrime Convention requires or invites, nor precludes, a party from establishing other powers or procedures than those contained in the Cybercrime Convention. If parties therefore wish to enact other domestic search and seizure provisions, in addition to the requirements of the Cybercrime Convention, they may do so.

62 See the Council of Europe's Explanatory Report to the Cybercrime Convention 36. Article 19 addresses the hugely problematic absence, from many jurisdictions, of laws permitting the seizure of intangible objects, such as stored computer data, which is generally secured by seizing the data medium on which the data is stored. Such national domestic legislation is necessary, not only to protect the preservation of easily destroyed data, but also to provide available law enforcement tools to assist other countries. Without these laws, a nation investigating a transborder crime is also effectively prevented from seeking international cooperation in a country that fails to authorise lawful search and seizure within its territory. Article 19 is qualified by reference to the wording "in its territory". Article 19 does not address transborder search and seizure, whereby one country could search and seize data in the territory of other countries without first having to go through the usual channels of mutual legal assistance. These search and seizure mechanisms are to be implemented at a national level and can only operate between parties to the Cybercrime Convention through the tool of international cooperation or through the channels of pre-existing mutual legal assistance arrangements. See Miquelon-Weismann 2005 *The John Marshall Journal of Computer & Information Law* 342. See paragraph 3.4. below for a discussion of transborder search and seizure devices. The requirement of equivalence between the search and seizure of tangibles and intangibles is also in the line with the second principle of the Council of Europe's Recommendation 1995(13) that preceded the Cybercrime Convention. This principle requires that criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure, should be equally applicable in the case of a search of computer systems and in the case of a seizure of data therein. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 12-15.

63 The precondition for obtaining legal authority to undertake a search and seizure remains the existence of grounds to believe, as prescribed by domestic law and human rights safeguards, that such data exists in a particular location and will afford evidence in respect of a specific criminal offence. The degree of belief required for obtaining legal authorisation to search also does not differ, whether the data is in tangible form or in electronic form. The belief and the search are in respect of data that already exists at the time of the search and that will afford evidence of a specific offence. The data sought is gathered during the course of the search in respect of data that exists at that time. See the Council of Europe's Explanatory Report to the Cybercrime Convention 36.

64 Some of the reasons underlying this need for additional procedural provisions include the fact that the data is in an intangible form. The physical medium on which the intangible data is stored must be seized or taken away. Alternatively, a copy of the data must be made either in a tangible form (such as a computer printout) or in an intangible form on a physical medium, before the tangible medium containing the copy can be seized and taken away. Where such copies are made, it must be borne in mind that a copy of the data remains in the computer system or storage device. Data may also not be stored in the particular computer that is searched, but such data may be readily accessible to that system, due to the connectivity of computer systems. The data could be stored in an associated data storage device that is connected directly to the computer, or that is indirectly connected to the computer through communication systems (such as the Internet). An extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched) might be

procedural provisions include the requirements listed below, namely a comprehensive authorisation to search, copy or access and seize or secure; an extension of the search or access; and coerced cooperation if circumstances reasonably permit.

3.3.1.2 Comprehensive legal authorisation to search or access

Article 19(1)(a) requires parties to empower law enforcement authorities to access and search computer data which is contained either within a computer system or part of it.[65] Bearing in mind the Cybercrime Convention's definition of a computer system,[66] article 19(1)(a) concerns the search of a computer system (and of related components that can be considered to form one distinct computer system).[67]

The search and seizure of an independent computer data storage medium[68] in which computer data may be stored, as envisaged in article 19(1)(b), may be undertaken by means of traditional search powers. However, the execution of a computer search requires a comprehensive legal authority to encompass the search of the computer system, as well as of any related computer storage medium in the immediate vicinity of the computer system.

3.3.1.3 Extension of the search or access

Article 19(2) is aimed at data that is physically stored in another system or storage device which can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. It covers situations involving linkages with other computer systems by means of telecommunications networks within the same territory.[69] Article 19(2) allows the investigating authorities to extend their search or similar access to another computer system or part of it, if they have reasonable grounds to believe that the data required is stored in

---

required. See also paragraphs 3.3.1.3 and 3.3.1.4 below in these respects. Alternatively, it could become necessary to use the traditional powers of search and seizure in a more coordinated and expeditious manner at both locations. See the Council of Europe's Explanatory Report to the Cybercrime Convention 36.

65 Such as a connected storage device. See paragraph 2.5.1.1 above for a reference to some of the different storage media that may contain relevant computer data.

66 See paragraph 2.5.1 above for a discussion of computer systems.

67 Such as a personal computer (PC), together with a printer and related storage devices, or a local area network (LAN). Links with other distinct computer systems by means of telecommunications networks within the same territory are addressed in article 19(2). See the Council of Europe's Explanatory Report to the Cybercrime Convention 37.

68 Such as a CD-ROM or diskette. See paragraph 2.5.1.1 above for a discussion of the various computing storage capabilities.

69 Such as a wide area network (WAN) or the Internet. See paragraph 2.6 above for a discussion of networked computing environments, including the Internet. This is reflected in the third principle of the Council of Europe's Recommendation 1995(13), which provides that, during the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction connected by means of a network, and to seize the data therein, provided that immediate action is required. From a technical point of view, it becomes increasingly complex, if not factually impossible, to establish any location of data at a given time. The relation between data and its carrier becomes nebulous. Modern information systems and networks provide the user with the opportunity to store data without the need to know where it has been put or will be put at any time. In these cases, it would take too much time, if it is possible at all, to find out where the data is located. Immediate actions may therefore be necessary to gain access to the data. Restrictions are, however, to be placed on a network search: national legislation should provide appropriate safeguards against possible abusive use of this power by the investigating authorities. One could think of limiting this power to particular information systems, or, within such systems, to the directories to which the persons usually living or working in the searched premises are entitled to have access. See Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 15-17.

that other computer system. The other computer system or part of it must, however, also be in its territory. The Cybercrime Convention does not prescribe how an extension of a search is to be permitted or undertaken.[70]

3.3.1.4 Comprehensive legal authorisation to seize or similarly secure

Article 19(3) empowers competent authorities to seize or similarly secure computer data that has been searched or similarly accessed by seizing or similarly securing both the computer systems,[71] and/or parts of them, as well as independent computer data storage media where necessary. It also provides for the alternative powers to make and retain a copy of accessed computer data; to maintain the integrity of the relevant stored computer data and to render inaccessible or remove the computer data in the accessed computer system.[72]

3.3.1.5 Coerced cooperation

Article 19(4) introduces a coercive measure to address the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. Competent authorities are empowered to order any person with knowledge about the functioning of the computer system or measures applied to protect the computer data therein,[73] to provide, as is reasonable, the necessary information to enable them

---

70 Some examples of possible conditions cited in the Council of Europe's Explanatory Report to the Cybercrime Convention include the empowerment of the judicial or other authority which authorised the computer search of a specific computer system to authorise the extension of the search or similar access to a connected system. Such authority may do so if it has grounds to believe (to the degree required by national law and human rights safeguards) that the connected computer system may contain specific data that is being sought. Searches or similar access could, alternatively, be exercised at both locations in a coordinated and expeditious manner. In all cases, however, the data to be searched must be lawfully accessible from or available to the initial computer system. See the Council of Europe's Explanatory Report to the Cybercrime Convention 37.

71 In certain cases, for instance, when data is stored in unique operating systems that cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. This may also be necessary when the data carrier has to be examined in order to retrieve from it older data which was overwritten but which has, nevertheless, left traces on the data carrier. The Council of Europe's Explanatory Report to the Cybercrime Convention 37. See paragraph 2.3.1 above for a discussion of *e*-evidence in the context of computer forensics.

72 It could be useful to render data inaccessible in situations where danger or social harm is involved (such as virus programs or instructions on how to make viruses or bombs) or where the data or its content is illegal (such as child pornography). The person concerned should be deprived of the possibility to use or disseminate the data illegally. This can be done in various ways, for example, by encrypting or deleting the data on the data carrier (also the back-ups) of the illegal owner after the data has been copied to the data carriers of the law enforcement authorities. This may also be necessary if no confiscation order is issued and the data has to be given back. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 14. The term "removal" implies that while the data is removed or rendered inaccessible it is not destroyed, but continues to exist. The temporal deprivation of the accused of the data leaves open the possibility that such data can be returned following the outcome of the criminal investigation or proceedings. See the Council of Europe's Explanatory Report to the Cybercrime Convention 38.

73 Such as system administrators, who have particular knowledge of the computer system and could therefore prove a useful source of information concerning the technical modalities about how best the search should be conducted. The Council of Europe's Explanatory Report to the Cybercrime Convention 39. Perrin contends that the Council of Europe's Explanatory Report to the Cybercrime Convention is ambiguous, because it refers to the "person" requested to cooperate as the system administrator, but it does not refer to this as an exhaustive selection of possible "persons". He argues that the example used in the Council of Europe's Explanatory Report to the Cybercrime Convention may provide the false comfort that only a third party system administrator (usually not in possession of personal keys) would be subject to this authority. If this power is, however, to be applied to other individuals (such as suspects or accused), the right against self-incrimination will need to be considered. If this power is reserved to system administrators, then additional consideration must be applied to proportionality. In either case, the Cybercrime Convention does not clarify the situation or the implications. The failure to be explicit has given rise to criticism from civil liberties organisations. See Perrin "An Analysis of International Initiatives on High-Tech Crime: A

to undertake the search measures set out in articles 19(1) and (2). This means that they can command the cooperation of knowledgeable persons that could help to make searches more effective and cost efficient, for both the law enforcement agencies and the innocent individuals affected.[74]

3.3.2 Scope

Article 19(5) provides specifically that the measures of search and seizure are subject to article 14, which sets the parameters for the scope of all the domestic procedural provisions contained in section 2 of the Cybercrime Convention.

Review of Implications for the Canadian Policy Environment" found on the Internet http://www./exinformatica.org/cybercrime/pub/perrin.pdf 22.

74 Without such cooperation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data. See Council of Europe's Explanatory Report to the Cybercrime Convention 39. Principles 9, 10 and 14 of the preceding Council of Europe's Recommendation 1995(13) are also relevant in this context. Principle 9 of the Council of Europe's Recommendation 1995(13) provides the following: "Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority." In the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), it is explained that self-incrimination is in principle contrary to human rights. Cooperation orders to submit evidentiary material may therefore not be issued in all cases against suspects or defendants or the use of the data submitted may be subject to legal restrictions. Member states should accordingly review their criminal procedural rules to ensure that investigating authorities also have the power to order persons who are not protected, as described above, to transmit data under their control, if that data is needed as evidence in a criminal proceeding. If the criminal procedural rules allow only that the delivery of tangible objects may be ordered, the rules should be changed and extended to intangible evidence such as computer data. This duty to submit data that has been ordered by law includes the obligation to present the data needed by law enforcement in a form suitable for evidentiary purposes. The recommendation allows the investigating authorities to determine the form in which the data has to be submitted. Usually this means that the person is ordered to hand over a printout and the original data carrier or a certified copy and that the data must be legible and comprehensible to the same extent as it is to the person who controls it. Encrypted or compressed data must be restored to its original condition. See Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 26.
Principle 10 of the Council of Europe's Recommendation 1995(13) states: "Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedural law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein". The Council of Europe's Explanatory Memorandum to Recommendation 1995(13) qualifies that the obligation to cooperate in a criminal procedure context is rather limited. Member states should review and, if necessary, extend the legal duties for third parties to cooperate beyond the traditional oral testimony and the orders to produce evidentiary objects and data (in terms of principle 9 of the Council of Europe's Recommendation 1995(13), referred to above). According to rules created in some member states in recent years, it should be possible, under certain conditions, for the investigating authority to have the power to order any person in possession of information on how the computer works and on how the evidence in question could be found to reveal this knowledge to law enforcement agencies. This implies that the criminal procedural rules in the field of testimony and/or production and delivery of evidence should include the power of the investigating authority to order third persons (namely, only those not protected as defendants or privileged witnesses) to give all the information needed to get access to a computer system and the information stored therein. Such persons could be the manufacturer or the importer of the computer or the computer programs, or the security expert of the computer, the program or in the field of cryptography. The cooperation of the so-called "trusted third parties", namely those independent persons or institutions who possess cryptology keys as depositories, might also be given consideration. Member states should also consider whether a general duty to act as an expert might be inserted in their criminal procedural laws, at least for problems which could not be solved otherwise. See Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 28. Principle 14 of the Council of Europe's Recommendation 1995(13) provides the following: "Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary". The conflict of interests between the needs of the users and the needs of law enforcement must be duly taken into account and a balance must be found. Irrespective of the legitimate interests of users of cryptography to transform data into a form that makes it unintelligible to third parties, this should not create insurmountable obstacles for the investigating authorities to know the content of the data during the lawful execution of a legal order to intercept a communication or to seize data. If not, criminals could benefit from these technologies to perpetrate offences with a smaller risk of being apprehended. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 35.

3.3.2.1 Specific criminal investigations or proceedings

Article 14(1) of the Cybercrime Convention looks at the procedural tools of search and seizure that must be implemented at the national level[75] in specific criminal investigations or proceedings.[76]

3.3.2.2 Categories of crimes

Subject to two exceptions,[77] article 14(2) provides that the powers of search and seizure must be applied both to offences established in accordance with the Cybercrime Convention and to other criminal offences committed by means of a computer system.

Importantly, section 14(2)(c) ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of these procedural powers. Such electronic evidence can therefore be used in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted. This warrants an equivalent or parallel capability for obtaining or collecting computer data as that under traditional powers.[78]

3.3.2.3 Stored computer data

The application of article 19 is limited to stored computer data, as opposed to data that is fluid and in movement and that must be obtained by means of an interception and monitoring intervention.[79]

3.3.2.4 Jurisdiction

The Internet has enabled corporations and individuals to extend their global reach. It goes without saying that few rules are written in black and white, and that their application has often

---

75 See also the references to "in its territory" in the Council of Europe's articles 19(1) and 19(2) of the Cybercrime Convention.

76 The drafters of the Cybercrime Convention discussed whether it should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed length of time, but did not include any such obligation, due to a lack of consensus. The Council of Europe's Explanatory Report to the Cybercrime Convention 24.

77 These exceptions are detailed in article 14(3) of the Cybercrime Convention, but they do not concern the powers of search and seizure *per se*. Article 21 provides that the power to intercept content data, in recognition of the privacy of oral communications and telecommunications and the intrusiveness of this investigative measure, is limited to a range of serious offences that must be determined by domestic law. Parties may also reserve the right to apply the measures in article 20 (the real-time collection of traffic data), only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted than the range of offences to which it applies the interception measures referred to in article 21. This exception hinges on whether a party considers the collection of traffic data equivalent to the collection of content data in terms of privacy and intrusiveness. A reservation is also afforded to parties which, due to existing limitations in their domestic law at the time of the adoption of the Cybercrime Convention, cannot intercept communications on computer systems operated for the benefit of a closed group of users that do not use public communications networks (such as the Internet and public telephone networks or other public telecommunications facilities in transmitting communications, whether or not such use is apparent to the users) and which are not physically or logically connected to other computer systems at the time when an order under articles 20 or 21 were issued. An example of such a "closed group of users" could be a set of users that is limited by association to the service provider, such as the employees of a company for which the company provides the ability to communicate amongst themselves using a computer network. See the Council of Europe's Explanatory Report to the Cybercrime Convention 25 and 26.

78 The Council of Europe's Explanatory Report to the Cybercrime Convention 25.

79 See paragraph 2.4 above for a distinction between the acts of interception and monitoring, search and seizure, production and preservation *vis-à-vis* the form or inertness of the data that the evidence collection intervention is directed at.

been inconsistent both within jurisdictions and outside them.[80] On occasion, both academics and the courts have argued that online activity creates a new environment for human interaction, thus undermining the feasibility of applying historical doctrines of jurisdiction. Some have suggested self-regulation as a precursor to international conventions. Others have favoured the creation of a new legal system and institutions to govern online activity.[81] "Cyberlaw" activists envision a judicial recognition of cyberspace as its own legal space, governed by its own legal order. When confronted with a claim arising in cyberspace, courts would defer to the law of cyberspace, much as medieval courts incorporated and deferred to the "law merchant" in the case of transnational commercial disputes. Such deference requires the displacement of a state's legal norms. At the end of every digital connection are people, and their bodies would be the normal jurisdictional predicate.[82] The Cybercrime Convention did not set out to establish a revolutionary new interpretation of jurisdiction.

Article 22 obliges parties to establish jurisdiction over the criminal offences enumerated in articles 2 to 11 of the Cybercrime Convention. Article 22(1)(a) is based on the principle of territoriality. It requires parties to assert jurisdiction if these crimes are committed in its territory.[83] Article 22(1)(b) and (c) are based upon a variant of the principle of territoriality; and it requires a party to establish criminal jurisdiction over offences committed on ships flying its flag or aircraft registered under its laws.[84]

Article 22(1)(d) is based on the principle of nationality. It obliges nationals of a state to comply with its domestic law, even when they are outside its territory. Article 22(1)(d) provides that if a national of a specific party commits an offence abroad, that party is obliged to have the ability to prosecute its national if the conduct is also an offence under the law of the state in which the offence was committed, or if the conduct has taken place outside the territorial jurisdiction of any state.

---

80 Deveci 2005 Computer Law & Security Report 464.

81 Deveci 2006 Computer Law & Security Report 45.

82 Stein 1998 The International Lawyer 1169.

83 The drafters decided that a provision requiring parties to establish jurisdiction over offences involving satellites registered in its name was unnecessary, since unlawful communications involving satellites invariably originate from and/or are received on earth. Hence, one of the bases for a party's jurisdiction set forth in article 22(1)(a)–(c) is present if the transmission originates or terminates in one of the locations specified therein in these articles. Furthermore, to the extent that the offence involving a satellite communication is committed by a party's national outside the territorial jurisdiction of any state, there is a jurisdictional basis under article 22(1)(d). The drafters also questioned whether registration was an appropriate basis for asserting criminal jurisdiction, since in many cases there would be no meaningful nexus between the offence committed and the state of registry, because a satellite serves as a mere conduit for a transmission. See the Council of Europe's Explanatory Report to the Cybercrime Convention 46.

84 Such ships and aircraft are frequently considered to be an extension of the territory of the state. If the crime is committed on a ship or aircraft that is beyond the territory of the flag party, there may quite possibly be no other state that would be able to exercise jurisdiction, barring this requirement. In addition, if a crime is committed aboard a ship or aircraft that is merely passing through the waters or airspace of another state, the latter state may face significant practical impediments to the exercise of its jurisdiction, and it is therefore useful for the state of registry also to have jurisdiction. See the Council of Europe's Explanatory Report to the Cybercrime Convention 46.

The bases of jurisdiction set forth in article 22(1) are not exclusive. Article 22(4) permits the parties to exercise other types of criminal jurisdiction as well (in conformity with their domestic law).[85]

Article 22(2) allows parties to enter a reservation to all of the jurisdiction grounds laid down in article 22(1), excluding the establishment of territorial jurisdiction under article 22(1)(a). Parties may also not enter reservations in respect of the obligation to establish jurisdiction in cases falling under the principle of *aut dedere aut judicare* in article 22(3).[86] Jurisdiction established on the basis of article 22(3) is necessary to ensure that those parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if such investigations and proceedings are sought by the party that requested extradition pursuant to the requirements of article 24(6) of the Cybercrime Convention.[87]

3.3.3 Conditions and safeguards

Article 19(5) provides specifically that the measures of search and seizure are subject to article 15, which explains certain conditions and safeguards that must be provided for under domestic law in respect of all the domestic procedural provisions contained in section 2 of the Cybercrime Convention. In applying binding international obligations and established domestic principles, national legislatures have to determine which of the procedural powers and procedures are sufficiently intrusive to require the implementation of particular conditions and safeguards.[88]

---

85 The criteria for courts to assert jurisdiction over crimes and civil actions in cyberspace have begun to take concrete form. August points out that both the drafters of the Cybercrime Convention and most of the commentators writing on cybercrime are encouraging courts to assume jurisdictions using any of the traditional nexuses, inclusive of the following: the territoriality nexus (which holds that the place where an offence is committed, in whole or in part, determines jurisdiction); the nationality nexus (which looks to the nationality or national character of the person committing the offence to establish jurisdiction); the protective nexus (which provides for jurisdiction when a national or international interest of the forum is injured by the offender); and the universality nexus (which holds that a court has jurisdiction over certain offences that are recognised by the community of nations as being of universal concern, including piracy, the slave trade, attacks on or the hijacking of aircraft, genocide, war crimes and crimes against humanity). See August 2002 *American Business Law Journal* 534 and 572.

86 Article 22(3) of the Cybercrime Convention directs that each party must adopt the measures necessary to establish jurisdiction over the offences referred to in article 24(1), in cases where an alleged offender is present in its territory and it does not extradite her to another party, solely on the basis of her nationality, after a request for extradition. Article 24(1) of the Cybercrime Convention applies to extradition between parties for the criminal offences established in accordance with articles 2-11 of the Cybercrime Convention, provided that they are punishable under the laws of both parties concerned by deprivation of liberty for a maximum of at least one year, or by a more severe penalty. However, where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the 1957 European Convention on Extradition (ETS No 24), applicable between two or more parties, the minimum penalty provided for under such arrangements or treaty applies.

87 The Council of Europe's Explanatory Report to the Cybercrime Convention 46.

88 The Council of Europe's Explanatory Report to the Cybercrime Convention 27. Article 15 was included at a rather late stage of the treaty-drafting process, i.e. the 27th draft of the Cybercrime Convention. See Perrin "An Analysis of International Initiatives on High-Tech Crime A Review of Implications for the Canadian Policy Environment" found on the Internet http://www./exinformatica.org/cybercrime/pub/perrin.pdf 19. Opponents to the Cybercrime Convention argue that the Convention appears to leave the point moot for parties who have not signed any international human rights treaties. Keyser, however, argues that the argument that the Cybercrime Convention will infringe on civil liberties appears to be an unfounded concern. He states that article 15 of the Cybercrime Convention requires member countries to establish conditions and safeguards to be applied to the governmental powers established in articles 16 to 21 of the Cybercrime Convention. Article 15, in fact, lists some specific safeguards that should be applied where appropriate in light of the power or procedure concerned. See Keyser 2003 *Journal of Transnational Law & Policy* 311 and 325. Oddis agrees with Keyser that there is little foundation for the criticism against the Cybercrime Convention that it did not attend adequately to the protection of individual human rights and that it missed an important opportunity to ensure that minimum standards consistent with the ECHR and other international human rights

3.3.3.1 Domestic conditions and safeguards

Article 15(1) provides that the establishment, implementation and application of search and seizure mechanisms are subject to the conditions and safeguards provided for under the domestic law of each party. Such safeguards include the right against self-incrimination, legal privileges and the specificity of individuals or places that are the object of the application of the measure.[89]

Parties are obligated to introduce certain procedural law provisions into their domestic law, but the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each party.[90]

3.3.3.2 Minimum international safeguards

There are, however, some common standards or minimum safeguards to which parties to the Cybercrime Convention must adhere in balancing the interests of law enforcement and a respect for fundamental human rights. These conditions or safeguards must ensure the adequate protection of human rights and liberties. They may be provided constitutionally, legislatively, judicially or otherwise.[91]

---

accords were actually implemented. She argues, *inter alia*, that the powers and procedures afforded in terms of the Cybercrime Convention must incorporate the principle of proportionality. Also, any dispute arising between the parties to the Cybercrime Convention regarding the interpretation or application of its provisions must be submitted to one of three entities for peaceful settlement. These entities are the European Committee on Crime Problems, an arbitral tribunal whose decision is binding to the parties to the dispute or the International Court of Justice itself. See Oddis 2002 *Temple International Comparative Law Journal* 510-512. Kennedy argues that the drafters of the treaty had the opportunity to address the vast privacy concerns associated with the Internet. These privacy concerns centre on the collection and possible misuse of data. The potential opportunities to exploit data are growing exponentially because technological developments are lowering the cost of data collection and surveillance, while increasing the quality and quantity of data. Consumers are concerned that governments are selling personal information (such as driver's licence data, health records and tax documents) to make a profit, and that *e*-companies are using online consumer preferences for business advantages. Today's privacy concerns, Kennedy states, encompass violations by governments, businesses and rogue individuals. In essence, the all-seeing eye from George Orwell's*1984* "need not necessarily belong to government, as many in the private sector find it valuable to conduct various forms of surveillance or to 'mine' data collected by others". See Kennedy "In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty" found on the Internet http://law.richmond.edu/JOLT/v9i1/article3.pdf 48-49. Miquelon-Weismann contends that the Cybercrime Convention, in its present form, allows state intrusions into the sphere of individual privacy rights to gather evidence for use in subsequent criminal prosecutions without adequate guarantees of procedural due process. One solution may be the addition of a Protocol to the Cybercrime Convention, modelled after the proposed Council of Europe Constitution providing minimal guidelines for procedural due process, extended to citizens of all participating nations. In this way, the Cybercrime Convention could become a blueprint for future international endeavors to harmonise penal law enforcement. See Miquelon-Weismann 2005 *The John Marshall Journal of Computer & Information Law* 361. Baron quotes the following statement made by Lawrence Lessig: "... there is a decision to be made about the architecture that cyberspace will become, and the question is how that decision will be made. Or better, where will the decision be made." According to Baron, this question posed by Lessig is being answered all too quickly and the resounding response is causing widespread difficulties. Governments are concerned with the threats of cybercrime. Hence, privacy is not perceived to be a strong concern. Without specific protections for privacy rights, nations may well enforce new standards of enforcement with little concern for outdated standards of privacy. The Council of Europe needs to clarify the vague items that remain. See Baron 2002 *The Catholic University of America CommLaw Conspectus* 278.

89 The Council of Europe's Explanatory Report to the Cybercrime Convention 27.

90 The Council of Europe's Explanatory Report to the Cybercrime Convention 26.

91 The Council of Europe's Explanatory Report to the Cybercrime Convention 26.

These minimum international safeguards include standards or minimum safeguards arising pursuant to obligations that a party has undertaken under applicable international human rights instruments. Article 15(1) specifically refers to the Council of Europe Convention on Human Rights[92] and to the more universally ratified 1966 International Covenant on Civil and Political Rights.[93] It also includes other applicable international human rights instruments in respect of states in other regions of the world.[94]

Specific reference is made in the preamble to the Cybercrime Convention of other applicable international human rights treaties which reaffirm various rights. These rights include the right of everyone to hold opinions without interference; the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers; and rights concerning the respect for privacy. The preamble also obliges parties to be mindful of the protection of personal data with specific reference to the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[95] The preamble refers to the 1989 United Nations Convention on the Rights of the Child[96] and the 1999 International Labour Organisation Worst Forms of Child Labour Convention;[97] the existing Council of Europe conventions of cooperation in the penal field, as well as similar treaties which exist between Council of Europe member states and other States[98]

3.3.3.3 Supervision by competent authorities

Article 15(2) requires specifically that the conditions and safeguards include grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof (as appropriate in view of the nature of the power or procedure, judicial or other independent supervision).

The term "competent authorities" refers to judicial, administrative or other law enforcement authorities that are empowered by domestic law to order, authorise or undertake the execution

---

92 Including its additional Protocols Nos 1, 4, 6, 7 and 12 (ETS Nos 005, 009, 046, 114, 117 and 177), in respect of European states that are parties to them. See the Council of Europe's Explanatory Report to the Cybercrime Convention 26.

93 A copy thereof can be found on the Internet http://www1.umn.edu/humanrts/instree/b3ccpr.htm.

94 Such as the 1969 American Convention of Human Rights (a copy thereof can be found on the Internet http://www.oas.org/juridico/english/Treaties/b-32.htm) and the 1981 African Charter on Human Rights and People's Rights (a copy thereof can be found on the Internet http://www.africa-union.org/official_documents/Treaties_%20Conventions_%20Protocols/Banjul%20Charter.pdf. See the Council of Europe's Explanatory Report to the Cybercrime Convention 26.

95 A copy thereof can be found on the Internet http://privacy.org/pi/intl_orgs/coe/dp_convention_1-8.txt.

96 A copy thereof can be found on the Internet http://www.unhchr.ch/html/menu3/b/k2crc.htm.

97 A copy thereof can be found on the Internet http://www.ohchr.org/english/law/childlabour.htm.

98 It must be stressed that the Cybercrime Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective, and to enable the collection of evidence of a criminal offence in electronic form. The recent developments, which further advance international understanding and cooperation in combating cybercrimes, including actions of the United Nations, the OECD, the European Union and the G8, are also welcomed. See the Council of Europe's Explanatory Report to the Cybercrime Convention 25.

of procedural measures for the purpose of collecting or producing evidence in respect of specific criminal investigations or proceedings.[99]

3.3.3.4 Proportionality

The principle of proportionality must be incorporated as a safeguard to the procedural powers of search and seizure in terms of article 19 of the Cybercrime Convention. Each party must implement proportionality in accordance with the relevant principles of its domestic law.[100]

Proportionality measures could include reasonableness requirements for searches and seizures, and limitations on overly broad search warrants and production orders. The limitation of interception measures to a range of serious offences (determined by domestic law), the legal predicates justifying the interception, and the fact that other less intrusive measures are not effective, are also examples of the application of the proportionality principle.[101]

Another application of the principle of proportionality is found in article 19(4) of the Cybercrime Convention. The mandatory provision of information only relates to information that is reasonably necessary to enable the search and seizure to be undertaken, or, similarly, to enable the computer data to be accessed or secured. In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, such disclosure in other circumstances could unreasonably threaten the privacy of other users or other data that is not authorised to be searched. Alternatively, the provision of the necessary information could entail the disclosure, in a form that is intelligible and readable, of the actual data sought by the competent authorities.[102]

3.3.3.5 Third parties

Article 15(3) brings into the equation, to the extent that it is consistent with the public interest,[103] particularly the sound administration of justice on the one hand, and the impact of search and seizure upon the rights, responsibilities and legitimate interests of third parties on the other.[104] Some of the protected legal interests include

---

99 The Council of Europe's Explanatory Report to the Cybercrime Convention 25.

100 For European countries, this will be derived from the principles of the Council of Europe Convention on Human Rights, its applicable jurisprudence and national legislation and jurisprudence, in that the power or procedure must be proportional to the nature and the circumstances of the offence. See the Council of Europe's Explanatory Report to the Cybercrime Convention 27.

101 The Council of Europe's Explanatory Report to the Cybercrime Convention 27 and 42.

102 The Council of Europe's Explanatory Report to the Cybercrime Convention 39.

103 Public interest include public safety and public health, as well as the interests of victims and the respect for private life. See the Council of Europe's Explanatory Report to the Cybercrime Convention 27.

104 Such as service providers. See the Council of Europe's Explanatory Report to the Cybercrime Convention 27. Business needs also frequently get in the way of the investigation. There may, for example, be a web server that has valuable evidence to help in an investigation, but if there is no redundancy for that server and the company cannot, or will not, take it down as it is crucial to the operation of the business, the investigation is halted and the evidence is overwritten.

(a) the integrity and the proper functioning or use of stored computer data or computer programs;[105]

(b) the interest of operators and users of computer and telecommunications systems in being able to have them function properly;[106] and

(c) the security and reliability of electronic data which may have consequences for legal relations.[107]

It must be considered whether appropriate means can be taken to mitigate the impact of a search and seizure upon the rights of third parties. Examples of such means are minimising the disruption of consumer services; protecting proprietary interests and protecting from liability for disclosure; or facilitating disclosure under chapter 2 of the Cybercrime Convention.[108] Provisions relating to the engagement and financial compensation of witnesses and experts could also be built into the domestic law of parties.[109]

The drafters of the Cybercrime Convention also discussed, in the context of article 19(5), whether interested parties should be notified that a search procedure of a surreptitious nature in the online world will be performed.[110] Where the laws of some parties do not provide for an obligation to notify a suspect even of a traditional search, the Cybercrime Convention will create a discrepancy in the laws of these parties. Other parties, on the other hand, consider notification an essential feature of a search and seizure mechanism, so as to maintain a distinction between the search and seizure of stored computer data on the one hand, and the interception of flowing data on the other hand. The issue of notification has, therefore, been left to be determined by domestic law. If parties, however, consider a system of mandatory notification of persons concerned, they should bear in mind that such notification may prejudice the investigation. If such a risk exists, postponement of the notification should be considered.[111]

---

105 The Council of Europe's Explanatory Report to the Cybercrime Convention 12.
106 The Council of Europe's Explanatory Report to the Cybercrime Convention 13.
107 The Council of Europe's Explanatory Report to the Cybercrime Convention 16.
108 The Council of Europe's Explanatory Report to the Cybercrime Convention 27.
109 The Council of Europe's Explanatory Report to the Cybercrime Convention 39.
110 It may be less apparent that data has been searched and seized, particularly if it has been copied or a copy has been diverted to another destination, than where physical items went missing. See the Council of Europe's Explanatory Report to the Cybercrime Convention 39.
111 The Council of Europe's Explanatory Report to the Cybercrime Convention 39.

3.4 Transborder search and seizure in computing environments

The Cybercrime Convention not only provides for search and seizure mechanisms at a national level, but also calls for the creation of such mechanisms at an international level.[112] The requirements, scope, conditions and safeguards applicable to these transborder search and seizure devices, proposed in articles 31 and 32 of the Cybercrime Convention, are considered below.

3.4.1 Requirements

3.4.1.1 Search and seizure specific

3.4.1.1.1 Ability to search and seize for the benefit of other parties

In terms of article 31(1), each party must have the ability, for the benefit of another party, to search or similarly access, seize or similarly secure and disclose data stored by means of a computer system located within its national territory. This mechanism includes data that has been preserved pursuant to article 29.

Article 31(2) provides that a mutual assistance request regarding the accessing of stored computer data should be responded to through the application of international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws referred to in article 23. Such cooperation must also be in accordance with the rest of chapter III of the Cybercrime Convention.

3.4.1.1.2 Expedited search and seizure for the benefit of other parties

Article 31(3) provides that a request for search and seizure must be responded to on an expedited basis where there are grounds to believe that the relevant data is particularly vulnerable to loss or modification, or otherwise where the relevant treaties, arrangements or laws provide for such expedited cooperation.

---

[112] In accordance with article 39(3), nothing in the Cybercrime Convention requires or invites, or precludes, a party from establishing other powers or procedures than those contained in the Cybercrime Convention. If parties therefore wish to enact other transborder search and seizure provisions, in addition to the requirements of the Cybercrime Convention, they may do so.

3.4.1.1.3 Access with consent or where publicly available

Article 32 addresses situations in which a party may access stored computer data in the territory of another party without that party's authorisation.[113] Two situations may be distinguished. First, article 32(a) provides that a party may access open source stored computer data, regardless of where the data is located geographically. Second, under article 32(b), if a party has obtained the lawful and voluntary consent of the person who has the lawful authority to disclose the data through a computer system in its territory, such a party may also access or receive data located outside its territory through a computer system in its territory. Persons that are lawfully authorised to disclose data may vary depending on the circumstances, the nature of the person and the applicable law.[114]

---

113 The drafters of the Cybercrime Convention explicitly deny that the treaty permits remote extraterritorial searches. See Weber 2003 *Berkeley Technology Law Journal* 233. The issue of unilateral access to computer data stored in another party's territory, without seeking mutual assistance, was a question that the drafters of the Cybercrime Convention discussed at length. They concluded that, due to a lack of concrete experience with such situations to date and recognising that the proper solution often turned on the precise circumstances of the individual case, it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. Article 32 sets out those situations in which all the parties agreed that unilateral action would be permissible. Other mechanisms, in terms of article 39(3), are neither authorised nor precluded. See Council of Europe's Explanatory Report to the Cybercrime Convention 60. Chapter VII of the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) deals with international cooperation matters. It advocates better cooperation structures to enable prompt application of law enforcement powers to investigate transborder cases. The use of transborder network searches could be a primary tool for investigating authorities; however, it may violate national sovereignty and international law. To avoid such complications, international instruments setting up precise conditions are recommended. Recognising the often time-consuming mutual assistance procedures which may be inadequate in the investigation of information technology crime, the recommendation also encourages the creation of expedited procedures and a liaison system to enable the seizure of data under foreign jurisdictions. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 10. Principle 17 of the Council of Europe's Recommendation 1995(13) accordingly provides the following: "The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted." In order to preserve the advantages of a transborder network search, additional international agreements should be negotiated, preferably on a multinational basis, for example, in the form of additional protocols to existing conventions. In this respect, nothing specific is proposed in the recommendation; this should be left to the consultations needed when drawing up such an international instrument. It does, however, propose the following conditions to be made applicable to transborder network searches: there must be reasonable suspicion that relevant data is located abroad in a system connected with the searched system; the aim of direct access must be to preserve the *status quo* of relevant data; access should only be allowed to data of private persons, enterprises and institutions including data of government entities and administrative authorities; seizure of data must only be authorised for evidentiary purposes; the modalities of seizure, for example, only copying and/or other possibilities such as making data inaccessible, must be prescribed; the state of urgency in relation to the traditional criminal procedure of letters rogatory must be explained (such as the probability or presumption that data could otherwise disappear or be altered); prompt notification must be delivered to the investigating authorities of the other state on the object and purpose of the search, as well as the kind of data seized; the data may only be used in the relevant criminal proceeding and on the basis of consent by the authorities of the other state; there must be effective remedies which would allow an affected individual to oppose the transmission of data by the searched state or the consent of the latter to use data seized by the state carrying out the search; and legal claims emerging from damages that occurred to the persons concerned must be regulated. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 39-40. In cases where a transborder network search is not possible, the creation of expedited and adequate criminal procedures to seize data in a foreign state should be envisaged. States may choose different methods to implement these expedited procedures, for example, by domestic legislation or international agreements. Principle 18 of the Council of Europe's Recommendation 1995(13) accordingly states the following: "Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorised to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorised to provide traffic data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented."

114 A person's email may, for example, be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in for in article 32(b). See the Council of Europe's Explanatory Report to the Cybercrime Convention 60.

3.4.1.2 General mutual assistance requirements

3.4.1.2.1 No separate general mutual assistance regime

The drafters of the Cybercrime Convention rejected the creation of a separate general regime of mutual assistance that would be applied in *lieu* of other applicable instruments and arrangements. In avoiding the confusion that may result from the establishment of competing regimes, chapter III is not generally intended to supersede existing mutual legal assistance frameworks. Mutual assistance practitioners are permitted to use the instruments and arrangements they are most familiar with.[115] Article 23 accordingly provides that international cooperation must be conducted in accordance with the provisions of chapter III of the Cybercrime Convention and by applying relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws.[116]

3.4.1.2.2 Minimum cooperative measures

An exception to this general principle of mutual assistance subject to the terms of both existing and future applicable mutual assistance treaties and domestic laws is that each party is obliged to provide for the cooperative measures set forth in the remaining articles of chapter III of the Cybercrime Convention.[117] These cooperative measures include the expedited preservation of stored computer data, the expedited disclosure of preserved traffic data, the accessing of stored computer data, transborder access to stored computer data with consent or where publicly available, the real-time collection of traffic data, the interception of content data and the maintenance of a 24 hour, 7 day a week network.

---

115 Most forms of mutual assistance under chapter III will consequently continue to be carried out pursuant to the European Convention on Mutual Assistance in Criminal Matters (ETS No 30) and its Protocol (ETS No 99) among the parties to those instruments (copies can be found on the Internet http://www.statewatch.org.news/2006/jan/1959-CoE-Convention.pdf and http://www.conventions.coe /int/treaty/en/Treateis/Word/099.doc). Alternatively, parties to the Cybercrime Convention who have bilateral mutual legal assistance treaties in force between them, or other multilateral agreements governing mutual assistance in criminal cases (such as between member states of the European Union), continue to apply their terms, supplemented by the specific mechanisms described in the remainder of chapter III. Parties may, however, also agree rather to apply any or all of the provisions of article 27 of the Cybercrime Convention. Mutual assistance may also be based on arrangements agreed to on the basis of uniform or reciprocal legislation, such as the system of cooperation developed among the Nordic countries (which is also admitted by the European Convention on Mutual Assistance in Criminal Matters) and among members of the Commonwealth. See the Council of Europe's Explanatory Report to the Cybercrime Convention 53.

116 The Council of Europe's Explanatory Report to the Cybercrime Convention 48.

117 Article 25(2) of the Cybercrime Convention. Other exceptions include article 27, article 25(4) and article 29(4). Article 27 must be applied to the execution of requests in *lieu* of the requested party's domestic law governing international cooperation in the absence of a mutual legal assistance treaty or equivalent arrangement between the requested and requesting parties (see paragraph 3.4.1.3 below). Article 25(4) provides that cooperation may not be denied, at least as far as the offences established in articles 2-11 of the Cybercrime Convention are concerned, on the grounds that the requested party considers the request to involve a fiscal offence. Article 29(4) provides that preservation may not be denied on dual criminality grounds, although the possibility of a reservation is provided for in this respect. The Council of Europe's Explanatory Report to the Cybercrime Convention 51.

3.4.1.2.3 Urgent mutual assistance requests

The extreme volatility of computer data may make it impossible to trace a crime to its perpetrator and it may destroy critical proof of guilt, whilst causing significant harm to persons or property.[118] Article 25(3) therefore facilitates accelerating the process of obtaining mutual assistance by empowering the parties to make urgent requests for cooperation through expedited means of communications[119] rather than through the traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems.[120] The requested party is also required to use expedited means to respond to requests in such circumstances and may require a formal confirmation sent through traditional channels to follow the expedited transmission if it so chooses.

3.4.1.2.4 24 hour, 7 day a week network[121]

Article 35 requires parties to the Cybercrime Convention to designate points of contact, available on a 24 hour, 7 day a week basis, in order to ensure the provision of immediate assistance within the scope of chapter III, including providing technical advice, preserving data and collecting evidence, locating suspects and giving legal information. Such legal information means advice to requesting parties in respect of any legal prerequisites required for providing informal or formal cooperation.[122]

The 24 hour, 7 day a week network is among the most important means provided by the Cybercrime Convention to ensure that parties can respond effectively to the law enforcement challenges of effectively combating crimes committed by means of computer systems and the effective collection of evidence in electronic form. These challenges include the need for very

---

118 The Council of Europe's Explanatory Report to the Cybercrime Convention 50.

119 Specifically referring to fax or email in article 25(3). The parties may decide among themselves how to ensure the authenticity of the communications and whether there is a need for special security protections (including encryption) that may be necessary in a particularly sensitive case.

120 The Council of Europe's Explanatory Report to the Cybercrime Convention 51.

121 It is anticipated that the structure of this 24/7 network will evolve over time. The concept is based upon the experience gained from an already functioning network, created under the auspices of the Group of 8 (G8) nations. The G8 is made up of the heads of state of eight industrialised countries (the United States, the United Kingdom, France, Germany, Italy, Japan, Canada, Russia and the European Union). The leaders have been meeting since 1975 to discuss issues of importance. Since 1995, the G8 has become increasingly involved in the issue of cybercrime. It has created working groups and issued a series of communiqués from the leaders and action plans from the justice ministers concerned. In addition, a special working group has also been working on the cybercrime agenda almost constantly for several years. See Privacy International "The Group of 8" found on the Internet http://www.privacyinternational.org/article.shtml?cmd[347]=347-65438 1. Some of the accomplishments of the G8 Subcommittee on High-Tech Crime include the following: the hosting of international computer crime training conferences; authorising the International Organisation of Computer Evidence to recommend international standards for retrieving and authenticating electronic evidence; accelerating the cooperation between law enforcement and industry representatives, including hardware manufacturers, telecommunications carriers and Internet service providers; and establishing high-tech points of contact for law enforcement officers. See Sprinkel 2002 *Suffolk Transnational Law Review* 504. In March 2004, 42 countries (including the United States, the United Kingdom and South Africa) were signed up and now actively participate in the activities of the G8 network. During the researcher's tenure at the Directorate of Special Operations of the National Prosecuting Authority, she has been designated, in person, as one of the two South African contacts. This opportunity presented her with some indispensable practical experience regarding the collection of electronic evidence.

122 The Council of Europe's Explanatory Report to the Cybercrime Convention 62.

rapid response, as a few keystrokes in one part of the world could instantly have consequences many thousands of kilometres and many time zones away.[123] Although parties are at liberty to determine the location of its point of contact within its law enforcement structure,[124] due consideration should be given to the need to communicate with points of contacts using other languages.

The 24 hour, 7 day a week contact should have the capacity to communicate with other points of contact on an expedited basis.[125] Also, a point of contact that is not part of the international mutual assistance authorities of a party must ensure that it is able to cooperate with such authorities on an expedited basis to facilitate the rapid execution of those functions that it does not directly carry out itself.[126]

Each point of contact in the network must be properly equipped. Modern telephone, fax and computer equipment are essential to the smooth operation of the network, and other forms of communication and analytical equipment must be part of the system as technology advances. Trained and equipped personnel must be made available to facilitate the operation of the network.[127]

3.4.1.3 Mutual assistance requirements in the absence of applicable international agreements

Article 25(2) requires all parties to have a legal basis to carry out the specific forms of cooperation described in chapter III, particularly those referred to in articles 29 to 35, if its treaties, laws and arrangements do not already contain such provisions.[128] The availability of these mechanisms is vital for effective cooperation in computer-related criminal matters.[129]

Although article 27 of the Cybercrime Convention reinforces the general principle that mutual assistance should be carried out through the application of existing mutual assistance regimes, it obliges the parties to apply certain mutual assistance procedures and conditions where no

---

123 The Council of Europe's Explanatory Report to the Cybercrime Convention 62.

124 Some parties may wish to house the 24/7 contact within its central authority for mutual assistance. Some may believe that it is best located with a police unit specialised in fighting computer- or computer-related crime. Yet other choices may be appropriate for a particular party, given its governmental structure and legal system. See Council of Europe's Explanatory Report to the Cybercrime Convention 62.

125 Article 35(2)(a) of the Cybercrime Convention.

126 Article 35(2)(b) of the Cybercrime Convention. If a party's 24/7 contact is part of a police unit, for example, it must also have the ability to coordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour, day or night. See the Council of Europe's Explanatory Report to the Cybercrime Convention 62.

127 Article 35(3) of the Cybercrime Convention.

128 Parties are required either to be able to treat these provisions as self-executing, or to be able to rapidly enact any legislation required if parties do not already have sufficient flexibility under existing mutual assistance legislation to carry out the mutual assistance measures established under chapter III of the Cybercrime Convention. See the Council of Europe's Explanatory Report to the Cybercrime Convention 50.

129 The Council of Europe's Explanatory Report to the Cybercrime Convention 50 and 53.

mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation is in force between the requesting and requested parties.

In the absence of a mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, the provisions of article 27 in respect of issues expressly covered by it[130] must be applied in *lieu* of otherwise applicable domestic laws governing mutual assistance. However, in respect of other issues typically dealt with in domestic legislation governing international mutual assistance,[131] article 25(4) provides that where a specific provision in chapter III of the Cybercrime Convention is absent, the law of the requested party governs specific modalities of providing that type of assistance.

The institution of central authorities is a common feature of modern instruments dealing with mutual assistance in criminal matters.[132] The direct transmission between such central authorities is speedier and more efficient than transmission through diplomatic channels. It also ensures that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested party, and that particularly urgent or sensitive requests are dealt with properly.[133]

Article 27(2) accordingly requires the establishment of a central authority or authorities responsible for sending and answering requests for assistance, executing such requests, or transmitting them to the authorities competent for their execution. Parties have the flexibility to designate more than one central authority where this is appropriate under its system of mutual assistance,[134] but the designation of a single central authority for the purpose of mutual assistance is encouraged.[135] Each party must advise and update the Secretary General of the Council of Europe on the names and addresses, including email and fax numbers, of its central authority or authorities.[136]

---

130 Such issues include establishing central authorities, imposing conditions, grounds for and procedures in cases of postponement or refusal, the confidentiality of requests and direct communications. See the Council of Europe's Explanatory Report to the Cybercrime Convention 53.

131 For example, there are no provisions dealing with the form and content of requests, taking witness testimony in the requested or requesting parties, providing official or business records, transferring witnesses in custody, or assisting in confiscation matters. See the Council of Europe's Explanatory Report to the Cybercrime Convention 53.

132 The Council of Europe's Explanatory Report to the Cybercrime Convention 53.

133 The Council of Europe's Explanatory Report to the Cybercrime Convention 53.

134 Where more than one central authority is established, the party that has done so must ensure that each authority interprets the provisions of the Cybercrime Convention in the same way, and that both incoming and outgoing requests are dealt with rapidly and efficiently. The Council of Europe's Explanatory Report to the Cybercrime Convention 54.

135 It would generally be most efficient for the authority designated for such a purpose under a party's mutual legal assistance treaty or domestic law also to serve as the central authority in terms of article 27. The Council of Europe's Explanatory Report to the Cybercrime Convention 54.

136 Article 27(2)(d) of the Cybercrime Convention.

Although central authorities must communicate directly with each other as a general rule,[137] an exception is provided for in that urgent mutual legal assistance requests may be sent directly by the judicial authorities of the requesting party to the judicial authorities of the requested party.[138] Such requests may also be channelled through the International Criminal Police Organisation (Interpol).[139] A copy of requests channelled in this way must be simultaneously sent to the relevant domestic central authority, with a view to its transmission to the central authority of the requested party.[140] Authorities of the requested party that receive a request that falls outside their field of competence must refer the request to the competent national authority of the requested party and inform the requesting party that such a transfer has been made.[141] Requests may also be transmitted directly, without the intervention of central authorities, even if there is no urgency, as long as the authority of the requested party is able to comply with the request without making use of coercive action.[142] At the time of signature or when depositing its instruments of ratification, acceptance, approval or accession, a party may inform the Secretary General of the Council of Europe that, for reasons of efficiency, direct communications are also to be addressed to the central authority.[143]

Article 27(3) aims to ensure that the technical evidentiary and procedural requirements of the requesting state can be met. It obliges the requested party to execute requests in accordance with the procedures specified by the requesting party, unless to do so would be incompatible with its own law. It has furthermore been agreed that the mere fact that the requested party's legal system knows no such a procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting party.[144] A requesting party, however, cannot require the requested party to execute a coercive power, such as a search and seizure that would not

---

137 Article 27(2)(b) of the Cybercrime Convention.

138 Article 27(9) of the Cybercrime Convention.

139 Article 27(9)(b). Interpol is an intergovernmental law enforcement association. Its headquarters are in Lyons, France. It was first established in 1923 to facilitate and develop international law enforcement and cooperation in relation to transnational crime. It was revived in 1945, after World War II. It operates through a network of National Central Bureaux staffed by law enforcement officers in each of the (by 2001) 178 member countries and a growing network of regional and subregional bureaux. The Interpol Subregional Bureau for Southern Africa started operating on 3 February 1997. It acts as the Secretariat for the Southern African Regional Police Chiefs Cooperation Organisation (SARPCCO). Cooperation with law enforcement of other countries in extradition-related matters is well-established. In the mid-twentieth century the South African Police (SAP), now the SAPS, became a member of Interpol for a time. It formally rejoined in September 1993. As for broader law enforcement cooperation in the mutual legal assistance context, liaison and cooperation in cross-border drugs matters was a standard feature of the work of the South African Narcotics Bureau (SANAB) even before the Drugs and Drug Trafficking Act 140 of 1992 came into effect. There was also wide cooperation on matters related to white-collar crime. In the 1980s an "International Office" was established at the then SAP Headquarters. In the early 1990s, the first police liaison officer was posted in London. Where Southern Africa is concerned, the formation of SARPCCO at the end of August 1995 was a significant advance on mere *ad hoc* bilateral cooperation and joint operations. See Goredema *Organised Crime in Southern Africa* 13-5 and 15-6; and also D'Oliveira 2003 *SAJCJ* 335.

140 Article 27(9)(a) of the Cybercrime Convention.

141 Article 27(9)(c) of the Cybercrime Convention.

142 Article 27(9)(d) of the Cybercrime Convention.

143 Article 27(9)(e) of the Cybercrime Convention.

144 For example, under the law of the requesting party, it may be a procedural requirement that a statement of a witness be given under oath. Even if the requested party does not have the domestic requirement that statements be given under oath, it should honour the requesting party's request. See the Council of Europe's Explanatory Report to the Cybercrime Convention 54.

meet the requested party's fundamental legal requirements. All fundamental procedural protections must remain intact.

3.4.2 Scope

3.4.2.1 Widest extent possible

In terms of articles 23 and 25(1) of the Cybercrime Convention, international cooperation must be provided among parties to the widest extent possible. Impediments thereto (such as reservations, postponements and the imposition of conditions to the provision of assistance) must be strictly limited.[145]

In order to promote the overriding principle of providing the widest possible measure of cooperation, grounds for refusal established by a requested party in terms of article 27(4) should be narrow and exercised with restraint. These grounds may not be so expansive as to create the potential for assistance to be categorically denied, or subjected to onerous conditions, in respect of broad categories of evidence or information.[146]

Article 27(7) also obliges the requested party to keep the requesting party informed of the outcome of the request, and requires reasons to be given in the case of any refusal or postponement of assistance.[147]

3.4.2.2 Categories of crime

Article 25(1) resonates with article 14(2), in that it extends the obligation to cooperate not only to all criminal offences related to computer systems and data, but also to the collection of evidence in electronic form of a criminal offence.[148] Article 25(4) also specifically provides that cooperation may not be denied, at least as far as the offences established in articles 2 to 11 of the Cybercrime Convention are concerned, on the grounds that the requested party considers the request to involve a fiscal offence.

---

145 It should, however, be noted that extradition (article 24), mutual assistance regarding the real-time collection of traffic data (article 33) and mutual assistance in respect of the interception of content data (article 34) permit the parties to provide for a different scope of application of these measures.

146 The Council of Europe's Explanatory Report to the Cybercrime Convention 54.

147 Providing reasons can, *inter alia*, assist the requesting party in understanding how the requested party interprets the requirements of article 27; provide a basis for consultation in order to improve the future efficiency of mutual assistance; and provide the requesting party with previously unknown factual information about the availability or condition of witnesses or evidence. The Council of Europe's Explanatory Report to the Cybercrime Convention 55.

148 Article 25(1) of the Cybercrime Convention.

3.4.2.3 Stored computer data

Articles 31 and 32 are aimed at stored computer data.[149]

3.4.2.4 Jurisdiction

While the Internet is borderless for criminals, law enforcement agencies must respect the sovereignty of other nations. This has impeded law enforcement efforts in ways never before contemplated. Differing legal systems and disparities in the laws of different countries often present major obstacles to international cooperation.[150]

Article 22(5) of the Cybercrime Convention provides for consultation, with a view to determining the most appropriate jurisdiction for prosecution(s), when more than one party claims jurisdiction over an offence. Duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the states concerned must be avoided, whilst the efficiency or fairness of the proceedings must be facilitated. The obligation to consult is not absolute, but consultation should take place where appropriate. A party may delay or decline consultation if one of the parties, for example, knows that consultation is not necessary because confirmation has been received that the other party is not planning to take action, or if a party is of the opinion that consultation may impair its investigation or proceedings.[151]

3.4.3 Conditions and safeguards

3.4.3.1 Domestic fundamental requirements satisfied

Article 25(4) of the Cybercrime Convention sets out the principle that mutual assistance is subject to the conditions provided for by applicable mutual assistance treaties and domestic laws. These regimes provide safeguards for the rights of persons located in the territory of the requested party that may become the subject of a request for mutual assistance. Search and seizure will not be executed on behalf of a requesting party, unless the requested party's fundamental requirements for such a measure applicable in a domestic case have been

---

149 See paragraph 2.4 above for the distinction between the acts of interception and monitoring, search and seizure, production and preservation *vis-à-vis* the form or inertness of the data that the evidence collection is directed at. Article 31(1) provides for mutual assistance regarding the accessing of stored computer data. Articles 32(a) and 32(b) provide for transborder access to stored computer data with consent or where publicly available.

150 Keyser 2003 *Journal of Transnational Law & Policy* 326. See also paragraph 3.3.2.4 above in respect of jurisdiction in cyberspace.

151 The Council of Europe's Explanatory Report to the Cybercrime Convention 47. The Cybercrime Convention has been criticised for not resolving the central jurisdictional dilemma where more than one country has a jurisdictional claim to a case. See Miquelon-Weismann 2005 *The John Marshall Journal of Computer & Information Law* 347. Hopkins also argues that the Cybercrime Convention, as drafted, does not contain a mechanism to deal with conflicts in jurisdiction. She proposes that a solution could be to establish a "priority of jurisdiction". For example, the Cybercrime Convention could establish a hierarchy where the nation that incurred the harm has jurisdictional priority over the nation where the crime was initiated. She contends that the Cybercrime Convention may yield unwieldy conflicts and inconsistent decisions, unless clear jurisdictional guidelines are put in place. See Hopkins 2003 *Journal of High Technology Law* 101-121.

satisfied. Parties may also ensure the protection of rights of persons in relation to the items seized and provided through mutual legal assistance.[152]

3.4.3.2 Dual criminality

Article 25(5) provides a definition of dual criminality for the purposes of mutual assistance under chapter III of the Cybercrime Convention. The condition of dual criminality must be deemed to have been fulfilled, irrespective of whether a requested party's laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting party, as long as the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. This provision was believed necessary in order to ensure that requested parties do not adopt too rigid a test when applying dual criminality. The double criminality standard must be applied in a flexible manner that will facilitate granting assistance.[153]

3.4.3.3 Prejudice to the sovereignty of the state and political offences

Article 27(4) provides that assistance may be refused where the execution of the request is likely to prejudice the sovereignty of the state, security, *ordre public* or other essential interests, and where the requested party considers the offence to be a political offence or an offence connected with a political offence.

3.4.3.4 Prejudice to investigations or proceedings

Article 27(5) permits the requested party to postpone, rather than refuse, assistance where immediately acting on the request would be prejudicial to investigations or proceedings in the requested party.[154]

3.4.3.5 Conditions in the discretion of the requested party

Article 27(6) provides that where the assistance sought would otherwise be refused or postponed, the requested party may instead provide assistance subject to conditions. If the conditions are not agreeable to the requesting party, the requested party may modify them, or it may exercise its right to refuse or postpone assistance. Since the requested party has an

---

152 The Council of Europe's Explanatory Report to the Cybercrime Convention 51.

153 The Council of Europe's Explanatory Report to the Cybercrime Convention 51.

154 For example, where the requesting party has sought to obtain evidence or witness testimony for the purposes of investigation or trial and the same evidence or witness are needed for use at a trial that is about to commence in the requested party, the requested party would be justified in postponing providing assistance. The Council of Europe's Explanatory Report to the Cybercrime Convention 51.

obligation to provide the widest possible measure of assistance, it was agreed that both grounds for refusal and conditions should be exercised with restraint.[155]

3.4.3.6 Confidentiality and use limitations[156]

Article 27(8) permits the requesting party to request that the fact and content of the request be kept confidential in particularly sensitive cases, or in cases in which there could be disastrous consequences if the facts underlying the request were to be made public prematurely.[157] Confidentiality may not be sought, however, to the extent that it would undermine the requested party's ability to obtain the evidence or information required.[158] If the requested party cannot comply with the request for confidentiality, it must notify the requesting party, which then has the option of withdrawing or modifying the request.

Article 28(2)(a) allows the requested party, when responding to a request for mutual assistance, to request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such a condition (for example, where the identity of a confidential informant is involved). It is not appropriate to require absolute confidentiality in cases in which the requested party is obliged to provide the requested assistance, as this would, in many cases, thwart the ability of the requesting party to investigate or prosecute crime successfully.[159]

Article 28(2)(b) provides that the requested party may also make the furnishing of the information or material dependent on the condition that it may not be used for investigations or proceedings other than those stated in the request. If the requested party, however, does not expressly invoke this condition, there is no such limitation on use by the requesting party.

Two exceptions to the ability to limit use and ensure confidentiality were recognised by the negotiators. These exceptions are said to be implicit in the terms of article 28(2).[160] Firstly, under the fundamental legal principles of many states, if material is evidence exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. In addition, once the

---

155 The Council of Europe's Explanatory Report to the Cybercrime Convention 51.

156 Both articles 27 and 28 only apply where there is no mutual assistance treaty, or arrangement on the basis of uniform or reciprocal legislation, in force between the requesting and requested parties. Where such a treaty or arrangement is in force, its provisions on confidentiality and use limitations apply in *lieu* of the provisions of article 28, unless the parties thereto agree otherwise. This avoids overlap with existing bilateral and multilateral mutual legal assistance treaties and similar arrangements. This enables practitioners to continue to operate under the normal well-understood regime, rather than seeking to apply two competing, possibly contradictory, instruments. The Council of Europe's Explanatory Report to the Cybercrime Convention 56.

157 The Council of Europe's Explanatory Report to the Cybercrime Convention 56.

158 For example, where the information needs to be disclosed in order to obtain a court order required to effect assistance, or where private persons possessing evidence need to be made aware of the request in order for it to be successfully executed. The Council of Europe's Explanatory Report to the Cybercrime Convention 56.

159 For example, by using the evidence in a public trial, including compulsory disclosure. The Council of Europe's Explanatory Report to the Cybercrime Convention 56.

160 The Council of Europe's Explanatory Report to the Cybercrime Convention 56.

3.5 *Domestic production orders in computing environments*

Article 18 of the Cybercrime Convention creates a domestic production order aimed at stored computer data.[171] The relevant requirements, scope, conditions and safeguards applicable to this production mechanism are considered below.

3.5.1 *Requirements for production orders*

3.5.1.1 Domestic production orders

A production order provides a flexible procedural measure which law enforcement can consider applying in *lieu* of measures that are more intrusive or more onerous, such as search and seizure. Third party custodians of data may often be prepared to assist law enforcement authorities on a voluntary basis by providing data under their control. A production order provides an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.[172]

Under article 18(1)(a), a party must ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or a data storage medium that is in that person's possession or control. A party must also provide for the power to order a service provider offering services in its territory to submit subscriber information in the service provider's possession or control in terms of article 18(1)(b).

3.5.2 *Scope*

Article 18(2) subjects article 18 production orders to the provisions of article 14 of the Cybercrime Convention, which sets the parameters for the scope of all the domestic procedural provisions, as contained in section 2 of the Cybercrime Convention.[173]

3.5.2.1 Specific criminal investigations or proceedings

Production orders must be used in individual cases, usually concerning particular subscribers. Article 18 does not authorise parties to issue a legal order to disclose indiscriminate amounts of

---

countries. This may create the risk that personal data from individuals within a country that is highly protective of the privacy of personal data would be transferred, pursuant to the mutual assistance obligations contained in the Cybercrime Convention, to a country that is not as protective of the privacy of personal data. See Klosek 2002 *Cyberspace Lawyer* 2.

171 In accordance with article 39(3), nothing in the Cybercrime Convention requires or invites a party to, nor precludes a party, from establishing other powers or procedures than those contained in the Cybercrime Convention. If parties therefore wish to enact other domestic production orders, in addition to the requirements of the Cybercrime Convention, they may do so.

172 The Council of Europe's Explanatory Report to the Cybercrime Convention 33.

173 See also the discussion of the scope of the domestic search and seizure devices proposed by the Cybercrime Convention, in paragraph 3.3.2. above.

the service provider's subscriber information about groups of subscribers for the purposes of data mining, for example.[174]

3.5.2.2 Categories of crimes

Production orders can be deployed for the purposes of obtaining electronic evidence in respect of all categories of crimes.[175]

3.5.2.3 Stored computer data

A production order is aimed at two particular types of stored computer data (specified stored computer data and subscriber information) as defined in article 18(3). The data in question is stored, existing data. Such data does not include data that has not yet come into existence, such as traffic data or content data related to future communications.

Stored computer data, or subscriber information that constitutes the focus of a production order, must be in the possession or control of a person or a service provider, respectively. Article 18(1)(a) either requires the stored computer data to be in the physical possession of the person to whom the production order is addressed, or if such data is outside the person's control, the person must be able to control the production of the data freely from within the ordering party's territory.[176] However, a mere technical ability to access remotely stored data does not necessarily constitute the required control within the meaning of article 18.[177] The terms "possession" or "control" in article 18(1)(b) also refer to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control.[178] Subscriber information relating to services offered in the ordering party's territory can also be the subject of a preservation order.

Article 18 is applicable only to the extent that the person or service provider maintains the required data or information. It should not be understood as imposing an obligation on service providers to keep records of their subscribers, or to ensure the correctness thereof. A service provider is therefore neither obliged to register identity information of users of so-called prepaid

---

174 For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or email address may be requested. The Council of Europe's Explanatory Report to the Cybercrime Convention 33. See also the discussion in paragraph 3.3.2.1 above.

175 See also the discussion in paragraph 3.3.2.2 above in respect of domestic search and seizure devices.

176 For example, subject to applicable privileges, a person who is served with a production order for information stored in her account by means of a remote online storage service must produce such information. In some states, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement. See the Council of Europe's Explanatory Report to the Cybercrime Convention 33.

177 For example, the ability of a user to access, through a network link, remotely stored data not within her legitimate control. See the Council of Europe's Explanatory Report to the Cybercrime Convention 33.

178 For example, at a remote data storage facility provided by another company. The Council of Europe's Explanatory Report to the Cybercrime Convention 33.

cards for mobile telephone services, nor obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.[179]

3.5.2.4 Jurisdiction

The jurisdictional provisions of article 22 also apply to article 18 production orders.[180]

3.5.3 Conditions and safeguards

Article 18(2) subjects a production order to the conditions and safeguards referred to in article 15.[181]

3.5.3.1 Domestic conditions and safeguards

The authority of domestic conditions and safeguards also applies to production orders.[182]

3.5.3.2 Minimum international safeguards

Production orders must adhere to a minimum set of international safeguards.[183]

3.5.3.3 Supervision by competent authorities

Production orders must be subjected to supervision by competent authorities.[184]

3.5.3.4 Proportionality

The proportionality principle provides some flexibility in relation to the application of production orders. In many states, for example, its application is excluded in minor cases.[185]

3.5.3.5 Third parties

The rights, responsibilities and legitimate interests of third parties must be considered when issuing production orders.[186]

---

179 The Council of Europe's Explanatory Report to the Cybercrime Convention 33 and 35.

180 See also the discussion in paragraph 3.3.2.4 above in respect of domestic search and seizure devices.

181 See also the discussion in paragraph 3.3.3 above in respect of domestic search and seizure devices.

182 See also the discussion in paragraph 3.3.3.1 above in respect of domestic search and seizure devices.

183 See also the discussion in paragraph 3.3.3.2 above in respect of domestic search and seizure devices.

184 See also the discussion in paragraph 3.3.3.3 above in respect of domestic search and seizure devices.

185 The Council of Europe's Explanatory Report to the Cybercrime Convention 34. See paragraph 3.3.3.4 above in respect of the proportionality of domestic search and seizure devices.

186 See the discussion in paragraph 3.3.3.5 above. As an individual would have no knowledge of the production of personal information held by third parties (and therefore would have no ability to challenge its reasonableness), it has been argued that search and seizure, as well as production orders, should be required to normatively incorporate a requirement of notification of the subject of the intervention. See Young "Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation: A Critical Analysis of the Council of Europe Convention on Cyber-Crime & the Canadian Lawful Access Proposal" found on the Internet http://www.ijclp.org/Cy_2004/pdf/Young_ijclp-paper.pdf 13.

3.5.3.6 Privileged categories of subscriber information

In addition to the conditions and safeguards generally applicable and depending on the domestic law of each party, privileged data or information may be excluded from the application of production orders. Different terms, different competent authorities and different safeguards may be relevant to the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. The production of publicly available subscriber information may attract less protection. Parties could accordingly allow for law enforcement agents to issue such production orders. However, in respect of other types of data a party might require, or be mandated by human rights safeguards to require, that only judicial authorities issue a production order.[187]

3.5.3.7 Confidentiality

Although article 18 does not contain a specific reference to confidentiality, it has been pointed out in the Council of Europe's Explanatory Report to the Cybercrime Convention as possibly essential for the success of an investigation. This applies especially where a production order is employed as a preliminary measure, preceding further disclosure measures, such as search and seizure or interception. With regard to the modalities of production, parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order.[188]

3.6 International variant: spontaneous production

Article 26 of the Cybercrime Convention provides for spontaneous production between parties internationally.[189] The requirements, scope, conditions and safeguards applicable to the spontaneous production of information are considered below.

3.6.1 Requirements

Article 26(1) empowers the party in possession of valuable information to forward it to the other party without a prior request if it believes such information may assist another party in a criminal investigation or proceeding, because that party will not be aware of its existence. However, a

---

187 The Council of Europe's Explanatory Report to the Cybercrime Convention 34.

188 This could include reference to a time period (within which disclosure must be made) or to form (such as that the data or information be provided in plain text, online, on a paper printout or on a diskette). Furthermore, confidentiality is not generally imposed regarding production orders in the offline world. The Council of Europe's Explanatory Report to the Cybercrime Convention 34.

189 In accordance with article 39(3), nothing in the Cybercrime Convention requires or invites a party to establish, nor precludes a party from establishing other powers or procedures than those contained in the Cybercrime Convention. If parties therefore wish to enact other transborder production devices, in addition to the requirements of the Cybercrime Convention, they may do so.

party is not obligated to spontaneously forward information to another party. It may exercise its discretion in the light of the circumstances of the case at hand. Moreover, the spontaneous disclosure of information does not preclude the disclosing party, if it has jurisdiction, from investigating or instituting proceedings in relation to the facts disclosed.

This provision is useful in a multilateral treaty, because, under the laws of some member states, a positive grant of legal authority is needed in order to provide assistance in the absence of a request.[190]

3.6.1.1 General mutual assistance requirements

Articles 23, 25 and 35 are, *mutatis mutandis*, applicable to the spontaneous production of information. No separate general mutual assistance regime is promoted. Instead, reliance on existing international instruments on international cooperation in criminal matters and arrangements agreed on the basis of uniform or reciprocal legislation and/or domestic laws is endorsed. However, provision must be made for a minimum set of cooperative measures, as set out in chapter III of the Cybercrime Convention, inclusive of the possibility of spontaneously forwarding information to another party. Spontaneous production may be facilitated in terms of article 25(3), albeit *via* the 24 hour, 7 day a week network established in terms of article 35 or otherwise.[191]

3.6.1.2 Mutual assistance requirements in the absence of applicable international agreements

The parties are obliged to apply certain mutual assistance procedures and conditions in the absence of a mutual assistance treaty or arrangement based on uniform or reciprocal legislation in force between the requesting and requested parties. Article 27 is, *mutatis mutandis*, applicable in respect of the spontaneous production of information.[192]

3.6.2 Scope

3.6.2.1 Widest possible extent

Although parties are not obliged to forward information spontaneously to other parties, international cooperation must generally be provided to the widest possible extent and impediments thereto are to be strictly limited.[193]

---

190 Keyser 2003 Journal of Transnational Law & Policy 318.
191 See the discussion in paragraph 3.4.1.2 above in respect of transborder search and seizure devices.
192 See the discussion in paragraph 3.4.1.3 above in respect of transborder search and seizure devices.
193 See the discussion in paragraph 3.4.2.1 above in respect of transborder search and seizure devices.

3.6.2.2 Categories of crime

Information in respect of all categories of crime may be spontaneously forwarded.[194]

3.6.2.3 Any computer data

Article 26 does not limit the spontaneous production of information to stored computer data, but, instead, refers to information obtained within the framework of its own investigations that may assist another party to initiate, or carry out investigations or proceedings concerning criminal offences established in the Cybercrime Convention, or that might lead to a request for cooperation by that party.[195]

3.6.2.4 Jurisdiction

Article 22 in respect of jurisdictional issues under the Cybercrime Convention is, *mutatis mutandis*, applicable to the spontaneous production of information.[196]

3.6.3 Conditions and safeguards

3.6.3.1 Confidentiality and use limitations

Article 26(2) specifically allows for circumstances in which a party only forwards information spontaneously if sensitive information will be kept confidential or other conditions can be imposed on the use of information.[197] If an advance inquiry reveals that the receiving party cannot comply with a condition sought by the providing party,[198] the receiving party must advise the providing party, which then has the option of not providing the information. However, if the receiving party agrees to the condition, it must honour it.[199]

---

194 See the discussion in paragraph 3.4.2.2 above in respect of transborder search and seizure devices.

195 Article 26(1) of the Cybercrime Convention.

196 See the discussion in paragraph 3.4.2.4 above in respect of transborder search and seizure devices.

197 In particular, confidentiality is an important consideration in cases in which important interests of the providing state may be endangered if the information were to be made public, for example, where there is a need to protect the means of collecting the information or the fact that a criminal group is being investigated. See the Council of Europe's Explanatory Report to the Cybercrime Convention 51.

198 A party may, for example, be unable to comply with a condition of confidentiality because the information is needed as evidence at a public trial. See the Council of Europe's Explanatory Report to the Cybercrime Convention 51.

199 The Council of Europe's Explanatory Report to the Cybercrime Convention 51. This article is derived from provisions in earlier Council of Europe instruments, such as article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No 141) and Article 28 of the Criminal Law Convention on Corruption (ETS No 173). Article 26 was thought useful because, under the laws of some states, such a positive grant of legal authority is needed in order to provide assistance in the absence of a request. It is foreseen that conditions imposed under this article would be consistent with those that could be imposed by the providing party pursuant to a request for mutual assistance from the receiving party.

3.6.3.2 Domestic fundamental requirements satisfied

Article 25(4) sets out the principle that mutual assistance, inclusive of spontaneously provided information, is subject to the conditions provided for by the applicable mutual assistance treaties and domestic laws.[200]

3.6.3.3 Dual criminality

Article 25(5) provides a definition of dual criminality for the purposes of mutual assistance under chapter III of the Cybercrime Convention. The dual criminality standard should be applied in a flexible manner that will facilitate granting assistance.[201]

3.6.3.4 Conditions in the discretion of the requested party

This condition is not applicable, as there is no requested party when information is spontaneously forwarded.

3.6.3.5 Prejudice to the sovereignty of the state and political offences

This condition is not applicable, as the spontaneous production of information cannot be requested and is solely at the discretion of the forwarding party.

3.6.3.6 Prejudice to investigations or proceedings

This condition is not applicable, as the spontaneous production of information cannot be requested and is solely in the discretion of the forwarding party.

3.6.3.7 Data protection

This condition is not applicable, as there is no requested party when information is spontaneously forwarded.

3.7 Domestic preservation and partial disclosure orders in computing environments

Articles 16 and 17 of the Cybercrime Convention provide for domestic preservation and partial disclosure orders.[202] The requirements, scope, conditions and safeguards applicable to these proposed preservation and partial disclosure devices are considered below.

---

200 See also the discussion in respect of the transborder search and seizure and production devices in paragraph 3.4.3.1 above.

201 The Council of Europe's Explanatory Report to the Cybercrime Convention 51. See also paragraph 3.4.3.2 above in respect of transborder search and seizure mechanisms.

3.7.1 Requirements

3.7.1.1 Domestic expedited preservation of stored computer data

Data preservation (for most countries an entirely new legal power or procedure in domestic law) is an important investigative tool in addressing especially crimes committed through the Internet.[203] A preservation order may be less disruptive to the normal activities and reputation of legitimate businesses than the execution of a search and seizure of their premises. Where the custodian of the data is trustworthy, such as a reputable business, the integrity of the data can be secured more quickly by means of an order to preserve the data.[204]

Article 16 of the Cybercrime Convention aims to ensure that national competent authorities are able to order or similarly obtain the expeditious preservation of specified stored computer data in connection with a specific criminal investigation or proceeding. Parties are required to introduce a power to order the preservation of specified computer data as a provisional measure. This will preserve data for as long as necessary, up to a maximum of 90 days.[205]

Each party may determine the appropriate manner of preservation within the context of its domestic law.[206] Preservation requires data which already exists in a stored form to be protected from anything that would cause its current quality or condition to change or deteriorate. It does not necessarily mean that the data should be frozen, or otherwise be rendered inaccessible so that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data.[207] Preservation also does not entail the disclosure of the data to law enforcement authorities at the time of preservation.[208] Preservation simply requires data to be kept safe from modification, deterioration or deletion.[209]

---

202 In accordance with article 39(3), nothing in the Cybercrime Convention either requires or invites a party to establish, or precludes a party from establishing other powers or procedures than those contained in the Cybercrime Convention. If parties therefore wish to enact other domestic preservation or partial disclosure orders, in addition to the requirements of the Cybercrime Convention, they may do so.

203 The Council of Europe's Explanatory Report to the Cybercrime Convention 29.

204 The Council of Europe's Explanatory Report to the Cybercrime Convention 29.

205 It is interesting to note that the Financial Action Task Force, for example, recommends, in the context of combating cyberlaundering, that Internet service providers not only establish log files with traffic data providing Internet protocol numbers of the subscriber and telephone numbers used for server connection, but also that Internet service providers must maintain such information for up to a year. See Money Laundering Alert "Cyberlaundering Threats Should Put All Bankers On Alert, FATF Warns" found on the Internet http://www.moneylaundering.com/MLAarticles/01Apr5.htm 3. This recommendation however, pertains to data retention and not data presentation as such. See paragraph 2.4.4 for a discussion of data preservation and retention.

206 The Council of Europe's Explanatory Report to the Cybercrime Convention 30.

207 The Council of Europe's Explanatory Report to the Cybercrime Convention 30.

208 The Council of Europe's Explanatory Report to the Cybercrime Convention 28.

209 See paragraph 2.4.4 above for a discussion of preservation.

The wording "to order or similarly obtain" in article 16(1) is intended to allow the use of other legal methods of achieving preservation, including production orders and search and seizure warrants that simultaneously facilitate the disclosure of the data to law enforcement agents. Although flexibility is intended with the use of the phrase "or otherwise obtain", it has been recommended that parties consider the establishment of powers and procedures to actually order the recipient of the preservation order to preserve the data.[210]

Article 16(2) provides that a person who receives a preservation order in respect of specified stored computer data in the person's possession or control is obliged to preserve and maintain the integrity of that computer data for a certain length of time, for as long as is necessary, up to a maximum of 90 days, to enable competent authorities to seek its disclosure. The domestic law of a party must specify a maximum period for which data subject to an order must be preserved, and the order must specify the exact length of time for which the specified data is to be preserved. This period must permit the competent authorities to undertake other legal measures, such as search and seizure, or similar access or securing, or to issue a production order to obtain the disclosure of the data.[211]

A party may also provide for such a preservation order subsequently to be renewed in terms of article 16(2).

3.7.1.2 Domestic expedited preservation and partial disclosure of traffic data[212]

In order to trace, for example, the electronic footprints embedded in computer communications to their source or destination in order to identify possible perpetrators and/or victims, traffic data regarding these past communications is required. Computer communications may also contain illegal content that constitutes critical evidence, such as child pornography, computer viruses or

---

210 The Council of Europe's Explanatory Report to the Cybercrime Convention 30.

211 The Council of Europe's Explanatory Report to the Cybercrime Convention 31.

212 Traffic data is defined in article 1 of the Cybercrime Convention. See paragraph 2.2.1.1.2 above for a discussion of the concept. The collection of traffic data easily permits the compilation of a profile of a person's interests and social context. The general laws of interception of communications in many states would appear to permit the use of techniques to identify the source and destination as a form of interception of communications or telecommunications, while in other states there is uncertainty. Some states have enacted specific provisions to permit such techniques, with conditions or safeguards different from those required for the interception of communications, in light of the qualitative difference in the data content. At present, the criminal procedural law of some member states does not clearly create a legal mechanism to collect traffic data. In other states, there is some legal authority to collect traffic data in criminal investigations, but the applicable legal conditions are sometimes too high to be useful in practice. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 23-24. Principle 12 of the Council of Europe's Recommendation 1995(13) 5-6 provides the following: "Specific obligations should be imposed on service providers who offer telecom services to the public, either through public or private networks, to provide information to identify the user when so ordered by the competent investigating authority". With the ongoing liberalisation of the telecommunications market, it may become increasingly difficult for the investigating authorities to identify the service provider to whom an order to cooperate should be issued. A solution to this problem could be to establish, at a national level, a central register of service providers offering telecom services to the public. It is evident that such a register may function only if the registration of service providers is mandatory. Taking into account the international dimension of the abovementioned liberalisation process, the international cooperation of keepers of central registers may also become desirable. See the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) 31.

other instructions that interfere with data or the proper functioning of a computer system. They may also contain evidence of other criminal activity pivotal to proving a criminal case.[213]

Obtaining stored traffic data associated with the past communications of criminals may be critical in determining the source or destination of a particular past communication that could prove to be instrumental in the identification of a perpetrator. Such traffic data is frequently stored only for short periods of time, as laws designed to protect privacy may prohibit, or market forces may discourage, the long-term storage of such data.[214] The importance of the powers of expedited preservation of computer data and the partial disclosure of traffic data vest in the volatility of the computer data sought. Electronic evidence can easily be manipulated or changed, intentionally deleted or destroyed by routine deletion of data that no longer needs to be retained, or may be lost through careless handling and storage practices.[215] Expedited preservation and partial disclosure orders are aimed at efficiently and expediently securing such volatile data.

Article 17 of the Cybercrime Convention establishes specific obligations in relation to the preservation of traffic data in terms of article 16. It provides for the expeditious disclosure of some traffic data, so as to identify other service providers that were involved in the transmission of specified communications.

Article 17(1)(a) ensures that traffic data can be expeditiously preserved among the service providers that were involved in the transmission of a communication, albeit one or multiple service providers.[216] The means by which such expeditious preservation may be achieved among multiple service providers are not specified, leaving it to domestic law to determine a means that is consistent with a party's legal and economic system. Examples of such expeditious preservation mechanisms include the following:[217]

---

213 The Council of Europe's Explanatory Report to the Cybercrime Convention 29.

214 Some states have laws that require that certain types of data, such as personal data, held by particular types of holders must not be retained and must be deleted if there is no longer a business purpose for the retention of the data. However, parties may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences. See the Council of Europe's Explanatory Report to the Cybercrime Convention 28 and 31.

215 The Council of Europe's Explanatory Report to the Cybercrime Convention 29.

216 Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination. The investigation becomes very complicated in such circumstances. See the Council of Europe's Explanatory Report to the Cybercrime Convention 32.

217 The Council of Europe's Explanatory Report to the Cybercrime Convention 32.

(a) a series of separate preservation orders, to be served expeditiously on each service provider involved;

(b) a single comprehensive preservation order, to be served sequentially, the scope of which would apply to all service providers identified subsequently as being involved in the transmission of that particular communication; and

(c) participatory preservation orders and cumulative notices which require a service provider served with an order to notify the next service provider in the chain of the existence and terms of the preservation order (the second service provider could similarly notify the next service provider in the chain); these cumulative notices could either permit the other service providers in the chain to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandate the preservation of the relevant traffic data.

Article 17(1)(b) requires a service provider who receives a preservation order or similar measure to disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service provider and the path through which the communication was transmitted. The competent authorities should specify clearly the type of crucial traffic data that must be disclosed. Receipt of this information would enable the competent authorities to determine whether also to take preservation measures in respect of other service providers to trace a communication back to its origin, or its destination, and identify the perpetrator or perpetrators of the specific crime under investigation.[218]

3.7.2 Scope

Articles 16(4) and 17(2) provide specifically that the proposed domestic preservation and partial disclosure mechanisms are subject to article 14, which sets the parameters for the scope of all the domestic procedural provisions, as contained in section 2 of the Cybercrime Convention.[219]

3.7.2.1 Specific criminal investigations or proceedings

Article 14(1) is *mutatis mutandis* applicable to and directs articles 16 and 17 at specific domestic criminal investigations or proceedings, limiting the measures to an investigation in a particular case.[220]

---

218 The Council of Europe's Explanatory Report to the Cybercrime Convention 32.

219 See also the discussion of the scope of the domestic search and seizure and production devices in paragraphs 3.3.2 and 3.5.2 (respectively) above.

3.7.2.2 Categories of crime

Article 14(2) is, *mutatis mutandis*, applicable to articles 16 and 17, allowing for the gathering of electronic evidence, irrespective of the nature of the criminal offence under investigation.[221]

3.7.2.3 Stored computer data

Articles 16 and 17 provide only for the power to require the preservation of existing computer data which has been stored by means of a computer system, pending the subsequent disclosure of such data pursuant to other legal powers, in relation to specific criminal investigations or proceedings. For preservation to take effect, it is presupposed that the data already exists, has already been collected and is stored by data holders such as service providers.[222]

Data retention is the process of storing data. Data preservation is the activity that keeps that stored data secure and safe. Articles 16 and 17 refer only to data preservation and not to data retention. The collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities are therefore not mandated. Furthermore, the obligation to ensure the preservation of data is not intended to require parties to restrict the offering or use of services that do not routinely collect and retain certain types of data, such as traffic or subscriber data, as part of their legitimate business practices. It also does not require the implementation of new technical capabilities in order to do so. The parties do not, for example, have to be able to preserve ephemeral data, which may be present on the system for such a brief time that it could not be reasonably preserved in response to a request or an order.[223]

The power to order or similarly obtain the expeditious preservation of specified computer data applies to any type of stored computer data which is specified in the preservation order.[224] Article 16(1) provides that the measures must be used where there are grounds to believe that

---

220 See also the discussion in respect of domestic search and seizure and production devices in paragraphs 3.3.2.1 and 3.5.2.1 (respectively) above.

221 See also the discussion of the scope of the domestic search and seizure and production devices in paragraphs 3.3.2.2 and 3.5.2.2 (respectively) above.

222 Accurate computer data relevant to criminal investigations may not exist, or may no longer be stored because such data has not been collected and/or maintained. Some of the reasons for this may be that data protection laws may have affirmatively required the destruction of important data before anyone realised its significance for criminal proceedings, or there may not have been any business reason for the collection and retention of data (such as where customers pay a flat rate for services or the services are free). Article 16 and 17 do not address these problems. Title 5 of the Cybercrime Convention addresses the real-time collection and retention of computer data, including future traffic data and the interception of and real time access to content data. See the Council of Europe's Explanatory Report to the Cybercrime Convention 27.

223 The Council of Europe's Explanatory Report to the Cybercrime Convention 8. See also paragraph 2.4.4 above for a discussion of data preservation versus data retention.

224 Such as business, health, personal or other records. The Council of Europe's Explanatory Report to the Cybercrime Convention 30.

the computer data, specifically including traffic data, is particularly vulnerable to loss or modification.[225] In addition, in terms of article 16(2), such specified stored computer data must actually be in the possession of the person served with the preservation order, or if stored elsewhere, must be subject to the control of this person.

3.7.2.4 Jurisdiction

The jurisdictional requirements set out in article 22 of the Cybercrime Convention are, *mutatis mutandis*, applicable to the domestic preservation and partial disclosure mechanisms provided for in articles 16 and 17.[226]

3.7.3 Conditions and safeguards

The domestic preservation and partial disclosure mechanisms are also subject to article 15 of the Cybercrime Convention, which explicates certain conditions and safeguards to be provided for under domestic law in respect of all the domestic procedural provisions, as contained in section 2 of the Cybercrime Convention. Articles 16(4) and 17(2) provide specifically that articles 16 and 17, respectively, are subject to article 15.[227]

3.7.3.1 Domestic conditions and safeguards

Article 15(1) is, *mutatis mutandis*, applicable to articles 16 and 17, rendering domestic conditions and safeguards equally applicable to preservation and partial disclosure orders.[228]

3.7.3.2 Minimum international safeguards

In terms of article 15(1), preservation and partial disclosure orders must also adhere to some common standards or minimum safeguards which must ensure the adequate protection of human rights and liberties.[229]

---

225 This can include situations where the data is subject to a short period of retention, such as where there is a business policy to delete the data after a certain length of time or the data is ordinarily deleted when the storage medium is used to record other data. It can also refer to the nature of the custodian of the data or the insecure manner in which the data is stored. However, if the custodian is untrustworthy, it would be more secure to effect preservation by means of search and seizure than by means of an order that could be disobeyed. If traffic data is collected and retained by a service provider, it is usually held only for a short period. The specific reference to traffic data in article 16(1) provides a link between the measures in article 16 and 17 and signals the particular applicability of these provisions to this type of data. The Council of Europe's Explanatory Report to the Cybercrime Convention 28.

226 See also the discussion of the jurisdiction in respect of the domestic search and seizure and production devices in paragraphs 3.3.2.4 and 3.5.2.4 (respectively) above.

227 See also the discussion in respect of the domestic search and seizure and production devices in paragraphs 3.3.3 and 3.5.3 (respectively) above.

228 See also the discussion in respect of the domestic search and seizure and production devices in paragraphs 3.3.3.1 and 3.5.3.1 (respectively) above.

229 See also the discussion in respect of the domestic search and seizure and production devices in paragraphs 3.3.3.2 and 3.5.3.2 (respectively) above.

3.7.3.3 Supervision by competent authorities

Article 15(2) requires independent supervision, grounds justifying the application of the preservation or partial disclosure order and a limitation on the scope or duration thereof.[230]

3.7.3.4 Proportionality

Article 15(1) explicitly requires the principle of proportionality to be made applicable to procedural measures, including preservation and partial disclosure orders.[231]

3.7.3.5 Third parties

Article 15(3) provides that the impact of a preservation and partial disclosure order on the rights, responsibilities and legitimate interests of third parties must be considered, to the extent that it is consistent with the public interest.[232]

3.7.3.6 Confidentiality

Article 16(3) requires parties to introduce an additional obligation of confidentiality regarding the expedited preservation of data on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period established in domestic law. A preservation order entails a dual obligation on the person to whom it is addressed not only to keep the data safe and secure, but also to maintain confidentiality of the fact that the preservation measure has been undertaken. This contributes to protecting the privacy of the data subject, or other persons who may be compromised in the data. It also accommodates the need of law enforcement agents for covertness during the initial phases of investigation, by not alerting the suspect to the investigation, and it may prevent any tampering with or deletion of data.[233]

3.8 Transborder preservation and partial disclosure orders in computing environments

The transborder expedited preservation of stored computer data and the transborder expedited disclosure of preserved traffic data is facilitated by means of articles 29 and 30 of the

---

230 The Council of Europe's Explanatory Report to the Cybercrime Convention 27 refers to the fact that although supervision by competent authorities should clearly be applied to the powers of interception, given its intrusiveness, such safeguards need not apply equally to preservation. See also the discussion in respect of the domestic search and seizure and production devices in paragraphs 3.3.3.3 and 3.5.3.3 (respectively) above.

231 See also the discussion in respect of the domestic search and seizure and production devices in paragraphs 3.3.3.4 and 3.5.3.4 (respectively) above.

232 See also the discussion in respect of the domestic search and seizure and production devices in paragraphs 3.3.3.5 and 3.5.3.5 (respectively) above.

233 The Council of Europe's Explanatory Report to the Cybercrime Convention 31.

Cybercrime Convention, respectively.[234] The requirements, scope, conditions and safeguards applicable to these proposed preservation and partial disclosure devices are considered below.

3.8.1 Requirements

3.8.1.1 Transborder expedited preservation of stored computer data

Article 29 is the international equivalent to the article 16 domestic expedited preservation mechanism. Such an international preservation mechanism is required in order to ensure the availability of volatile computer data in the territory of another party, pending the lengthier and more involved process of executing a formal mutual assistance request that will facilitate its actual disclosure. This measure is much more rapid than ordinary mutual assistance practice and it is also less intrusive. The privacy of the person whom the data concerns is protected until the criteria for the full disclosure pursuant to traditional mutual legal assistance regimes have been fulfilled.[235]

Article 29(1) authorises a party to make a request for, and article 29(3) requires each party to have the legal ability to obtain, the expeditious preservation of data stored in the territory of the requested party. The aim is to prevent the data from being altered, removed, deleted or irretrievably lost during the period required to prepare, transmit and execute a request for mutual assistance to obtain the data.[236] The preferred procedure is that the requested party ensures that the custodian preserve the data, and not necessarily obtain possession of the data from its custodian. A requested party may, however, use other legal methods, including the expedited issuance and execution of a production order or a search warrant for the data to ensure its rapid preservation.[237]

Article 29(2) details the minimum summary contents of a request for preservation to include the following:

(a) the authority seeking the preservation;

(b) the offence in respect of which the measure is sought and a summary of related facts;

---

234 In accordance with article 39(3), nothing in the Cybercrime Convention requires or invites a party to establish, or precludes a party from establishing other powers or procedures than those contained in the Cybercrime Convention. If parties therefore wish to enact other transborder preservation or partial disclosure orders, in addition to the requirements of the Cybercrime Convention, they may do so.

235 The Council of Europe's Explanatory Report to the Cybercrime Convention 57.

236 The Council of Europe's Explanatory Report to the Cybercrime Convention 57.

237 The Council of Europe's Explanatory Report to the Cybercrime Convention 57.

(c) sufficient information not only to identify the data to be preserved and its relationship to the offence, but also to identify the custodian of the data or the location of the computer system and an underscoring of the necessity of the preservation.

The requesting party must also undertake that it will subsequently submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

Article 29(7) specifies that preservation effected in response to a mutual assistance request is effective for a period no less than 60 days in order to enable the requesting party to submit a request for the production of the data. Following the receipt of such a request, the data must continue to be preserved pending a decision on that request.

3.8.1.2 Transborder expedited disclosure of preserved traffic data

Article 30 provides the international equivalent of the power established for domestic use in article 17. This international mechanism requires a party requested to preserve traffic data concerning a specific communication expeditiously to disclose to the requesting party a sufficient amount of traffic data to identify service providers in, and the paths of the communication from, other territories.[238]

If the transmission came from a third state, this information enables the requesting party to make a request for preservation and expedited mutual assistance to that state in order to trace the transmission to its ultimate source. If the transmission loops back to the requesting party, it is able to obtain preservation and disclosure of further traffic data through its domestic processes.[239]

3.8.1.3 General mutual assistance requirements

Articles 23, 25 and 35 are, *mutatis mutandis*, applicable to transborder preservation and partial disclosure orders. No separate general mutual assistance regime is therefore advocated. Instead, reliance is promoted on existing international instruments on international cooperation in criminal matters and arrangements agreed on the basis of uniform or reciprocal legislation or and domestic laws. However, provisions must be made for a minimum set of cooperative measures, as set out in chapter III of the Cybercrime Convention. Urgent mutual assistance

---

[238] Article 30(1) of the Cybercrime Convention.
[239] The Council of Europe's Explanatory Report to the Cybercrime Convention 59.

requests for production and partial disclosure are facilitated in terms of article 25(3), albeit *via* the 24 hour, 7 day a week network established in terms of article 35 or otherwise.[240]

3.8.1.4 Mutual assistance requirements in the absence of applicable international agreements

The parties are obliged to apply certain mutual assistance procedures and conditions in the absence of a mutual assistance treaty or arrangement based on uniform or reciprocal legislation in force between the requesting and requested parties. Article 27 is, *mutatis mutandis*, applicable in respect of transborder preservation and partial disclosure orders.[241]

3.8.2 Scope

3.8.2.1 Widest extent possible

International cooperation to facilitate preservation and partial disclosure must be provided to the widest extent possible and impediments thereto must be strictly limited.[242]

3.8.2.2 Categories of crime

The obligation to cooperate in respect of all categories of crime applies equally to preservation and partial disclosure orders. Facilitating preservation and partial disclosure in particular may not be denied in respect of the offences in articles 2 to 11, as established in the Cybercrime Convention, solely on the grounds that the offence concerned is considered a fiscal offence.[243]

3.8.2.3 Stored computer data

The preservation and partial disclosure devices established in terms of articles 29 and 30 of the Cybercrime Convention are aimed at stored computer data.[244]

3.8.2.4 Jurisdiction

Article 22, relating to jurisdictional issues in the Cybercrime Convention, is, *mutatis mutandis*, applicable to transborder preservation and production orders.[245]

---

240 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.1.2 and 3.6.1.1 (respectively) above.

241 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.1.3 and 3.6.1.2 (respectively) above.

242 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.2.1 and 3.6.2.1 (respectively) above.

243 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.2.2 and 3.6.2.2 (respectively) above.

244 See also the discussion in respect of the transborder search and seizure and production devices in paragraph 3.4.2.3 above.

245 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.2.4 and 3.6.2.4 (respectively) above.

3.8.3 Conditions and safeguards

3.8.3.1 Domestic fundamental requirements satisfied

Article 25(4) is, *mutatis mutandis*, applicable to preservation and partial disclosure orders, rendering these mechanisms subject to the conditions provided for by the applicable mutual assistance treaties and domestic laws.[246]

3.8.3.2 Dual criminality

The liberal definition of dual criminality for the purposes of mutual assistance under chapter III given in article 25(5) is equally applicable to transborder preservation and partial disclosure measures.[247] In addition, article 29(3) sets out the general rule that parties must dispense with any dual criminality requirement, as the principle of dual criminality is counterproductive in the preservation context, due to the volatility of the data. While the clarifications necessary to conclusively establish the existence of dual criminality are being sought, the critical data could have been deleted, removed or altered. Data could often be routinely deleted by service providers who hold it for only hours or days after the transmission has been made. If, thereafter, the requesting party were able to establish dual criminality, the crucial traffic data could be irretrievably lost and the perpetrators of the crime would never be identified.[248]

Eliminating the dual criminality requirement for all but the most intrusive procedural measures, such as search and seizure or interception and monitoring is a trend in modern mutual assistance practice. However, preservation is not seen as particularly intrusive, since the custodian merely maintains possession of data lawfully in its possession, and the data is not disclosed until or examined only after the execution of a formal mutual assistance request seeking disclosure of the data.[249]

However, a limited reservation is available in terms of article 29(4). A party that requires dual criminality for the search or similar access, seizure or similar securing, or disclosure of data, may reserve the right to refuse the preservation request in cases where it has reason to believe that, at the time of disclosure, the condition of dual criminality cannot be fulfilled. This requirement may only be imposed in relation to offences other than those defined in articles 2 to

---

246 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.3.1 and 3.6.3.2 (respectively) above.

247 See also the discussion in respect of the transborder search and seizure and production devices in paragraphs 3.4.3.2 and 3.6.3.3. (respectively) above.

248 The Council of Europe's Explanatory Report to the Cybercrime Convention 58.

249 The Council of Europe's Explanatory Report to the Cybercrime Convention 58.

11 of the Cybercrime Convention, as it is assumed that the condition of dual criminality is automatically met between the parties in respect of these offences.

3.8.3.3 Prejudice to the sovereignty of the state and political offences

In terms of both articles 29(5) and 30(2), a requested party may refuse a request for preservation where it concerns an offence which the requested party considers a political offence or an offence connected with a political offence, or where the execution of the preservation request is likely to prejudice the sovereignty, security, *ordre public* or other essential interests of the requested party. This is in accordance with article 27(4). However, it was also agreed that the assertion of any other basis for refusing a request for the preservation of traffic data is precluded, due to the centrality of this measure to the effective investigation and prosecution of crimes committed within the scope of the Cybercrime Convention, or the location of critical electronic evidence.[250]

3.8.3.4 Prejudice to investigations or proceedings

Article 27(5) permits the postponement of assistance where immediate action on the request would be prejudicial to investigations in the requested party.[251]

Article 29(6) provides, in addition, that a requested party must promptly inform the requesting party if it believes that the preservation will not ensure the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the investigation of the requesting party.[252] The latter may then assess whether to take the risk posed by nevertheless executing the request for preservation, or whether to seek a more intrusive but safer form of mutual assistance, such as production or search and seizure.[253]

3.8.3.5 Conditions in the discretion of the requested party

In terms of article 27(6), the requested party may provide assistance subject to additional conditions, where the assistance sought would otherwise have to be refused or postponed.[254]

---

250 The Council of Europe's Explanatory Report to the Cybercrime Convention 59. See also the discussion in respect of transborder search and seizure devices in paragraph 3.4.3.3 above.

251 See also the discussion in respect of transborder search and seizure devices in paragraph 3.4.3.4. above.

252 Examples of such scenarios are where the data to be preserved is held by a service provider controlled by a criminal group, or by the target of an investigation herself. The Council of Europe's Explanatory Report to the Cybercrime Convention 59.

253 The Council of Europe's Explanatory Report to the Cybercrime Convention 59.

254 See also the discussion in respect of transborder search and seizure devices in paragraph 3.4.3.5 above.

3.8.3.6 Confidentiality and use limitations

The confidentiality requirements and use limitations detailed in existing bilateral and multilateral mutual legal assistance treaties and similar arrangements, or in the absence thereof in articles 27(8) and 28, apply, *mutatis mutandis*, to preservation and partial disclosure orders.[255]

3.8.3.7 Data protection

Refusal of preservation and partial disclosure of data, on data protection grounds other than those provided for in article 28, may only be invoked in exceptional circumstances.[256]

3.9 Brouter[257] to chapter 4

The Cybercrime Convention constitutes the only existing internationally agreed upon benchmark for, inter alia, the procedural powers aimed at the collection of electronic evidence. This research is aimed at facilitating a comparative analysis between the catalogue of criminal procedural search and seizure, production and preservation devices proposed by the Cybercrime Convention compared to the devices available within the current South African legislative framework. In order to fulfil this purpose, this chapter was focused on providing an exposition of the requirements, scope and conditions and safeguards of both the domestic and international search and seizure, production and preservation devices proposed by the Cybercrime Convention.

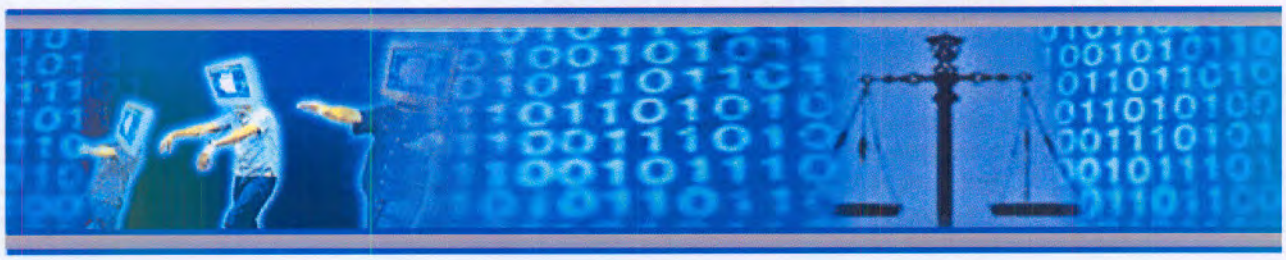
In the next chapter, the search and seizure, production and preservation mechanisms currently available within the South African legislative framework are investigated. The search and seizure, production and preservation mechanisms, as set out in this chapter, are used as the yardstick against which to measure South Africa's compliance with the requirements proposed by the Cybercrime Convention.

The findings and recommendations based on this comparative analysis between the South African devices compared to those proposed in the Cybercrime Convention are set out in chapter 7.

---

255 See also the discussion in respect of transborder search and seizure devices in paragraph 3.4.3.6 above.
256 See also the discussion in respect of transborder search and seizure devices in paragraph 3.4.3.7 above.
257 See chapter 7 for a list of the findings extracted from the contents of this chapter.

CHAPTER 4:
SEARCH AND SEIZURE, PRODUCTION AND PRESERVATION @ SOUTH AFRICA



4.1 BIOS BITS AND BYTES 153

4.2 DOMESTIC SEARCH AND SEIZURE IN COMPUTING ENVIRONMENTS 155

4.2.1 Root domain 155
4.2.2 Requirements 156
4.2.2.1 Articles susceptible to search and seizure 156
4.2.2.2 Domestic search and seizure with a warrant 159
4.2.2.3 Domestic search and seizure without a warrant 165
4.2.3 Scope 172
4.2.3.1 Particularity and specificity 172
4.2.3.2 Categories of crimes 177
4.2.3.3 Use of force in order to conduct a search 177
4.2.3.4 Jurisdiction 178
4.2.4 Conditions and safeguards 180
4.2.4.1 Right to privacy 180
4.2.4.2 Reasonable grounds 182
4.2.4.3 Proportionality 185
4.2.4.4 Supervision by competent authorities 186
4.2.4.5 Privileged data 188
4.2.4.6 Right against self-incrimination 193
4.2.4.7 Third parties 196
4.2.4.8 Consequences of unlawful action by the authorities 197
4.2.4.9 Propriety 198
4.2.4.10 Confidentiality 198

4.3 TRANSBORDER SEARCH AND SEIZURE IN COMPUTING ENVIRONMENTS 199

4.3.1 Requirements for transborder search and seizure 199
4.3.1.1 General mutual assistance framework 199
4.3.1.2 Foreign requests to South Africa, as the requested state 204
4.3.1.3 Requests from South Africa, as the requesting state 206
4.3.1.4 24 Hours a day, 7 days a week network 208
4.3.1.5 Search and seizure specific mutual assistance 208
4.3.2 Scope 211
4.3.2.1 Widest extent possible 211
4.3.2.2 Categories of crime 212
4.3.2.3 Jurisdiction 212
4.3.3 Conditions and safeguards 212
4.3.3.1 Dual criminality 212
4.3.3.2 Grounds for refusing a mutual legal assistance request 213
4.3.3.3 Costs 214
4.3.3.4 Admissibility and authentication 214

4.4 DOMESTIC PRODUCTION ORDERS IN COMPUTING ENVIRONMENTS.... 215

4.4.1 Background 215
4.4.2 Requirements 216
4.4.2.1 Section 205 of the Criminal Procedure Act 216
4.4.2.2 Archived communication-related directions 218
4.4.2.3 Sections 39(3) and 40(3) of the RICPCIA 222
4.4.3 Scope 223
4.4.3.1 Specific criminal investigations or proceedings 223
4.4.3.2 Categories of crimes 223
4.4.3.3 Stored computer data 224
4.4.3.4 Jurisdiction 225
4.4.4 Conditions and safeguards 225
4.4.4.1 Supervision by competent authorities 225
4.4.4.2 Proportionality 227
4.4.4.3 Third parties 229
4.4.4.4 Privileged categories of information 231
4.4.4.5 Confidentiality 234
4.4.4.6 Discretionary conditions 236
4.4.4.7 Consequences of unlawful action taken 236

4.5 TRANSBORDER PRODUCTION ORDERS IN COMPUTING ENVIRONMENTS. 238

4.6 DOMESTIC PRESERVATION AND PARTIAL DISCLOSURE PROVISIONAL MEASURES IN COMPUTING ENVIRONMENTS 239

4.7 TRANSBORDER PRESERVATION AND PARTIAL DISCLOSURE PROVISIONAL MEASURES IN COMPUTING ENVIRONMENTS 240

4.8 BROUTER TO CHAPTER 5 240

4.1 BIOS bits and bytes[1]

The main objective of this research is to consider whether the South African search and seizure, production and preservation measures in respect of electronic evidence need to be augmented and/or aligned in accordance with the measures set out in the Cybercrime Convention. The first step in such a comparative analysis was to contextualise the technicalities and terminology underpinning these devices.2 The second step was to give an exposition of the domestic and transborder search and seizure, production and preservation mechanisms proposed in the Cybercrime Convention to benchmark against. This was done in the previous chapter. This chapter represents the third step, as it provides an exposition of the South African search and seizure, production and preservation devices.

The domestic preservation, production and search and seizure of electronic evidence in South Africa are made possible by various legislative sources. The first of these sources is chapter 2 of the Criminal Procedure Act,[3] which provides for search warrants, the entering of premises, seizure, forfeiture and the disposal of property connected with offences. Secondly, sections 82 and 83 of the Electronic Communications and Transactions Act afford additional search and seizure powers to the cyber inspectors that other statutory bodies with the powers of inspection or search and seizure could also tap into. Thirdly, the general production of information is enabled by section 205 of the Criminal Procedure Act. Fourthly, sections 17, 19, 23, 39(3) and 40(3) of the RICPCIA allow for certain categories of communications data to be made available.[4]

---

1 In this heading, BIOS means some introductory bits and pieces with which to contextualise the primary sources of preservation, production and search and seizure mechanisms in South African law. It also broadly contextualises the relevance of this chapter within the overarching framework of this thesis. See footnote 1 of paragraph 3.1 above for a technical definition of the term "BIOS".

2 See chapter 2.

3 Chapter 2 of the Criminal Procedure Act is entitled "Search Warrants, Entering of Premises, Seizure, Forfeiture and Disposal of Property Connected with Offences". In addition to section 19, it also accommodates the following provisions, some of which are detailed in this chapter: section 20 (the state may seize certain articles); section 21 (an article to be seized under a search warrant); section 22 (circumstances in which an article may be seized without a search warrant); section 23 (search of an arrested person and seizure of an article); section 24 (search of premises); section 25 (power of the police to enter premises in connection with state security or any offence); section 26 (entering premises for the purposes of obtaining evidence); section 27 (resistance against entry and search); section 28 (wrongful search and offence, and award of damages); section 29 (search to be conducted in decent and orderly manner); section 30 (disposal by a police official of an article after seizure); section 31 (disposal of an article where no criminal proceedings are instituted or where it is not required for criminal proceedings to be instituted); section 32 (disposal of an article where criminal proceedings are instituted and an admission of guilt fine is paid); section 33 (an article to be transferred to court for purposes of trial); section 34 (disposal of an article after the commencement of criminal proceedings); section 35 (forfeiture of an article to the state); and section 36 (disposal of the article concerned in an offence committed outside the Republic).

4 Including both archived and real-time communication-related information. Due to its definition in section 1 of the RICPCIA, "real-time communication-related information" could technically have been stored by a telecommunications service provider for a period of 90 days already. This definition of real-time communication-related information obscures the meaning given to "stored" (as opposed to "real-time") computer data in the Cybercrime Convention to some extent. For the purposes of this study, real-time communication-related information is considered to the extent that it overlaps with the concept of stored computer data as *per* the Cybercrime Convention. This research is not quintessentially concerned with data in transit (real-time) data and the power to intercept and monitor but, instead, at the search and seizure, production and preservation of stored computer data. See also paragraph 2.4.1 above.

No specific and exclusive provision is made in South African law for the expedited preservation and partial disclosure of stored computer data. Preservation and disclosure must accordingly be facilitated by means of the traditional powers of search and seizure and production. Section 30(2) of the RICPCIA may, however, be relevant in considering the expedited preservation of traffic data as required by the Cybercrime Convention. To the extent that communication-related information is retained under section 30(2) of the RICPCIA it is, by default, preserved.

These procedural preservation, production and search and seizure mechanisms must be considered against the backdrop of the Constitution.[5] South Africa is a democratic state based on the values of the supremacy of its Constitution and the rule of law.[6] The basic principles of criminal procedure have been constitutionalised in the Bill of Rights in the Constitution in the form of both general provisions, which are relevant to criminal procedure,[7] and in the form of provisions which are specifically aimed at criminal justice.[8] These provisions have brought about profound changes to the law of criminal procedure in South Africa, as legislation and the common law may no longer be the only determinatives in law enforcement. Indeed, law enforcement officers empowered to prevent and bring to book crime are under a constitutional obligation always to respect, protect and promote these fundamental rights. Law enforcement agencies must act, teach and require their members to act in accordance with the Constitution.[9]

The transborder production and preservation of electronic evidence are facilitated within a broader mutual legal assistance framework. The International Cooperation in Criminal Matters Act[10] is the enabling legislation that provides the domestic legal basis upon which to provide mutual legal assistance. It deals with, *inter alia*, the mutual provision of evidence and information. Some uncertainty exists in respect of whether the mutual facilitation of searches and seizures is enabled by the International Cooperation in Criminal Matters Act or by chapter 2 of the Criminal Procedure Act, both of which are referred to below.[11]

This chapter provides an exposition of the current South African domestic and international search and seizure,[12] production[13] and preservation[14] mechanisms.

---

5 The Constitution is supreme law and applies to all law (see sections 1, 2 and 8 of the Constitution).
6 Section 1(c) of the Constitution.
7 Such as the right to dignity, the right to life, the right to freedom and security of the person and the right to privacy.
8 Such as the rights of arrested, detained and accused persons to a fair trial and to have unconstitutionally obtained evidence excluded.
9 Section 199(5) of the Constitution.
10 The International Cooperation in Criminal Matters Act 76 of 1996. Hereinafter referred to as the International Cooperation in Criminal Matters Act.
11 A discussion of this dualism in the current South African mutual legal assistance framework is provided in paragraph 4.3.1.5 below
12 See paragraphs 4.2 and 4.3 below for a discussion of the domestic and transborder search and seizure mechanisms respectively.
13 See paragraphs 4.4 and 4.5 below for a reference to the domestic and transborder production devices respectively.
14 See paragraphs 4.6 and 4.7 below for a discussion of the domestic and transborder preservation devices respectively.

4.2 Domestic search and seizure in computing environments

4.2.1 Root domain[15]

The roots of the South African criminal procedure are found in the Roman, Roman-Dutch and English law. In the seventeenth and eighteenth centuries, a crime control inquisitorial process with institutionalised torture was widespread across Europe, including the region of what is today the Netherlands. With the Dutch occupation of the Cape in 1652, the system of criminal procedure based on the Phillip II Ordinance of 1570 was introduced. The first British occupation from 1795 to 1803 saw the abolition of legalised torture in 1796, two years before it was abolished in the Netherlands. During the second British occupation from 1806 onwards, the Roman-Dutch law of criminal procedure nevertheless remained in force in the Cape. The structure of the courts was, however, subject to several amendments. This resulted in uncertainty as to which procedure the newer courts should follow. This led the Chief Justice and the members of the Court of Justice to issue a code of criminal procedure in 1819 which introduced elements of English criminal procedure. In 1827, a commission of enquiry recommended that the system of criminal procedure in the Cape should approximate even more closely the system of criminal procedure of England. The recommendations were largely accepted, resulting in the First Charter of Justice in 1827, which was replaced by a very similar Second Charter of Justice in 1832. The First Charter of Justice was followed by the 1828 Ordinance 40 on Criminal Procedure and the 1830 Ordinance 72 on Evidence. This virtually completed the Anglicisation of the law of criminal procedure and evidence. It put an end to the inquisitorial system by replacing it with the accusatorial English procedure. The last mentioned two Ordinances form the foundation of our modern law of criminal procedure. Theoretically, however, the Roman-Dutch law of criminal procedure still remains the common law underpinning the South African law of criminal procedure.[16]

The Criminal Procedure and Evidence Act[17] was enacted after the establishment of the Union of South Africa in 1910. Many amendments followed. A consolidating Criminal Procedure Act[18] replaced it in 1955. This Act was repealed by the present Criminal Procedure Act, which came into force on 22 July 1977.

---

15 The root domain is the starting point of the top level domain structure on the Internet. It is the root, or entry point, to the .com, .org, .net and other domains. Here, it means the historical origins of domestic search and seizure powers in South Africa.

16 Joubert (ed) *Criminal Procedure Handbook* 14-16.

17 Criminal Procedure and Evidence Act 31 of 1917.

18 Criminal Procedure Act 56 of 1955.

There are many statutory provisions that confer powers of search and seizure[19] and that co-exist with the criminal procedural search and seizure mechanisms established in terms of chapter 2 of the Criminal Procedure Act. Section 19 of the Criminal Procedure Act explicitly states that its chapter 2 does not derogate from any power conferred by any other act to enter any premises or to search any person, container or premises or to seize any matter forfeited or to dispose of any matter.

Due to the extensive nature of these acts, they are not discussed in this thesis, except to the limited extent that they might be drawn on in congruence to the criminal procedural provisions of search and seizure, attributed in terms of the Criminal Procedure Act, that constitute the real focus of this research. Sections 82 and 83 of the Electronic Communications and Transactions Act are, by means of exception, included in the discussion below.[20]

4.2.2 *Requirements*

4.2.2.1 Articles susceptible to search and seizure

Although section 20 of the Criminal Procedure Act does not authorise the search for any particular article, it prescribes which types of articles may be seized when a search in terms of another section of the Criminal Procedure Act takes place.[21]

The criminal procedural law power of search is conferred only where the object of the search is to find a certain person or to seize literally anything[22] which falls into one of the following three

---

19 Examples of such alternative mechanisms include: section 29 of the National Prosecuting Authority Act 32 of 1998; section 11E of the Transfer Duty Act 40 of 1949; section 9D of the Marketable Securities Act 32 of 1948; section 8E of the Estate Duty Act 45 of 1955; chapter 14 of the Firearms Control Act 60 of 2000; section 13 of the South African Police Service Act 68 of 1995 (warrantless searches and seizures for the purposes of border control, in a cordoned off area and at roadblocks); section 30 of the Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002; sections 4 and 88 of the Customs and Excise Act 91 of 1964; section 70 of the Financial Intelligence Centre Act 38 of 2001; section 17 of the Uncertified Securities Tax Act 31 of 1998; section 101 of the Correctional Services Act 111 of 1998; section 74D of the Income Tax Act 58 of 1962; section 144 of the Liquor Act 27 of 1989; section 57D of the Value-Added Tax Act 89 of 1991; sections 11 and 12 of the Drug and Drug Trafficking Act 140 of 1992; sections 9(2) and 10 of the Stock Theft Act 57 of 1959; section 28(1) of the Medicines and Related Substances Control Act 101 of 1965; section 48 of the Community Development Act 3 of 1966; sections 31 and 41 of the Arms and Ammunition Act 75 of 1969; section 6 of the Special Investigating Units and Special Tribunals Act 74 of 1996; and section 4 of the Game Theft Act 105 of 1991. Section 6(5) of the Businesses Act 71 of 1991 instructs that the provisions of any law which warrants the seizure of articles, including chapter 2 of the Criminal Procedure Act, do not apply in respect of the seizure of anything which is concerned in or suspected to be concerned in the commission of an offence in terms of the said act and relating to carrying on the business of street vendors, peddlers or hawkers, or which may afford evidence of the commission or suspected commission of such an offence, or which is intended to be used or is suspected of being intended to be used in the commission of an offence.

20 In principle, because it is a general power that is theoretically available to all statutory bodies with the powers of inspection or search and seizure via an application to a cyber inspector. Also, sections 82 and 83 of the Electronic Communications and Transactions Act are specifically tailored to include electronic evidence in its scope.

21 Article 20 is much wider than its predecessors, namely section 52 of the Criminal Procedure and Evidence Act 31 of 1917 and section 47 of the Criminal Procedure Act 56 of 1955, as it was prior to the Criminal Procedure Amendment Act 33 of 1975. These articles did not, for example, authorise a general search for books that could shed some light on the investigation. There must have been information under oath that there are specific books that are necessary as evidence (see *R v Sulski* 1935 TPD 292). Kriegler argues that sections 20 and 21 do, in fact, authorise a general search of a class of articles, without naming them specifically. See Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 38.

22 Section 20 is very wide. It is intended to assist law enforcement officers in their investigations of criminal cases. It stipulates that "anything" may be seized. Furthermore, it states that "anything" is referred to as "an article" in chapter 2 of the Criminal Procedure Act. "Anything" is indeed a very wide term and would include items such as documents, cheques and money, as is also evident from section 33(3)(a) of the Criminal Procedure Act that provides, *inter alia*, for the handling of such items by the

classes of articles:[23]

(a) articles which are concerned[24] in, or are on reasonable grounds believed to be concerned in, the commission or suspected commission of an offence, whether within South Africa or elsewhere;[25]

(b) articles which may afford evidence of the commission or suspected commission of an offence, whether within South Africa or elsewhere;[26] or

(c) articles which are intended to be used or are on reasonable grounds believed to be intended to be used in the commission of an offence.[27]

The precise nature of the articles that may be seized in terms of section 20 is unclear. As has been pointed out above,[28] the South African Law Reform Commission maintained that the provisions of the Criminal Procedure Act were developed when the idea of a location which is not a physical premises[29] or the seizure of something which is not a tangible object were inconceivable. Chapter 2 of the Criminal Procedure Act would not apply to the search of a computer and the seizure of information located on that computer. The seizure of a particular computer would, however, be allowed.[30] It has been recommended that the provisions of the

---

clerk of the court. See Du Toit *et al Commentary on the Criminal Procedure Act* 2-2A and Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 33. Watney argues that "anything" ought to be susceptible to a wide enough interpretation also to include the search and seizure of computer data. See Watney 2003 *TSAR* 67. Carstens and Lucouw also opine that the term "anything" seems wide enough to include even information. They argue further that the execution of a search warrant is made easier by the fact that the intangible information is almost always contained in a tangible object (such as a computer, CD-ROM or floppy disk). See Carstens and Lucouw *E-Commerce in Practice* 111-112. See also footnote 31 below in this respect.

23 Joubert (ed) *Criminal Procedure Handbook* (6th ed) 116.

24 The term "concerned" is also a wide term. Kriegler argues that because seizure infringes on the personal freedom of a person, the term "concerned" with the commission of an offence must be interpreted restrictively. Accordingly, he recommends that the following meaning should be attached thereto: "an article that is concerned in the commission of an offence and which is reasonably necessary to prove the offence, or which would probably be forfeited to the state". See Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 33. Steytler submits that such a reading would save section 20(a) of the Criminal Procedure Act from a constitutional challenge (Steytler *Constitutional Criminal Procedure* 86). See also *Ngubani v Divisional Commissioner, South African Police, Witwatersrand Division* 1963 (1) SA 316 (W) and *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D).

25 Section 20(a) of the Criminal Procedure Act.

26 Section 20(b) of the Criminal Procedure Act. This article may overlap with article 20(a), as some articles which may afford evidence could also have been concerned in the commission of an offence, see Joubert (ed) *Applied Law for Police Officials* 307.

27 Section 20(c) of the Criminal Procedure Act. Steytler postulates that if an article is used in an attempt to commit an offence, it may be seized because a completed, albeit an inchoate, offence has been committed. If possession of the article is illegal, then an offence is committed. If the intended use of an article is not the same as its use in the attempted commission of an offence, then this paragraph grants an additional power, namely in effect a peace-keeping power in terms of which the police may, for example, remove weapons which are in the lawful possession of a person, but which may be used in an offence in the near future. Hence, the police power is neither clearly defined nor properly structured. Steytler accordingly argues that the "intended" use of an article should be read as referring to articles that are used in the commission of an attempted offence. See Steytler *Constitutional Criminal Procedure* 86. However, Du Toit argues that section 35(1)(a) of the Criminal Procedure Act does not justify an interpretation that an article "intended to be used in connection with the commission of an offence" constitutes an article "by means whereof" the offence was committed or "which was used" in the commission of the offence. In *National Director of Public Prosecutions v Carolus* 1999 (2) SACR 27 (C), it was held that the instrumentality of an offence, referred to in section 38(2)(a) of the Prevention of Organised Crime Act 121 of 1998, by comparison, only refers to property used as a means or as an instrument in the commission of an offence or otherwise involved in the commission of an offence. The applicant had to show a link between the unlawful activity and the property. See also *S v Smith* 1984 (1) SA 583 (A) and Du Toit *et al Commentary on the Criminal Procedure Act* 2-2 and 2-15.

28 See also the introductory discussion of the problems with South African search and seizure in paragraph 1.2,1.

29 Section 1 of the Criminal Procedure Act defines "premises" to include land, any building or structure, or any vehicle, conveyance, ship, boat or aircraft.

30 The South African Law Reform Commission's *Discussion Paper 99 on Computer-related Crime* 14.

Criminal Procedure Act be aligned in order to solve problems with the restricting interpretations of the words "premises" and "article" as physical entities, as set out in sections 20 and 21 of the Criminal Procedure Act.[31]

In chapter 3 of its proposed Computer Misuse Bill,[32] the South African Law Reform Commission proposed the inclusion of new search and seizure provisions. The issue of the correct placement of these procedural provisions, particularly referring to the alternative of inserting these provisions into the Criminal Procedure Act, was left open. Section 7(1) of the Computer Misuse Bill, proposed in the South African Law Reform Commission's Discussion Paper 99 on Computer-related Crime, provides that the

> ... State may seize any computer system or take any samples or copies of applications[33] or data[34]-
>
> (a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere;
>
> (b) that may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere; or
>
> (c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

In current law enforcement practice, the provisions of chapter 2 of the Criminal Procedure Act are widely applied to facilitate the search and seizure of computer data. This practice has not been contested in court as yet.[35]

Section 82(3) of the Electronic Communications and Transactions Act stipulates that the Criminal Procedure Act applies with the necessary changes to searches and seizures in terms

---

31 Watney 2003 *TSAR* 73. However, despite this recommendation, Watney argues that section 20 of the Criminal Procedure Act ought to be susceptible to a broader application. She contends that there is no prohibition against issuing a search warrant that authorises a law enforcement officer to search a computer and to seize information stored on such a computer, provided that it qualifies to be included in one of the three groups provided for in section 20 (Watney 2003 *TSAR* 67). This is in contrast to the specific inclusion of section 82(4) of the Electronic Communications and Transactions Act. See paragraphs 4.2.2.2.3 and 4.2.3.1 below.

32 See the South African Law Reform Commission's *Discussion Paper 99 on Computer-related Crime* 66-68.

33 An "application" is defined in section 1 of the Computer Misuse Bill to mean a set of instructions that, when it is executed in a computer system, causes a computer system to perform a function. It includes such a set of instructions held in any removable storage medium which is in a computer system for the time being. A "computer system" is defined in section 1 to mean an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, one or more of which is capable of containing data; or performing a logical, arithmetical, or any other function in relation to data.

34 Section 1 of the Computer Misuse Bill circumscribes "data" as any representation of information, knowledge, facts or concepts capable of being processed in a computer system. This includes such a representation held in any removable storage medium which is in a computer system for the time being. Also see the discussion of computer data in paragraph 2.2.1 above.

35 Although there were, in fact, a few cases in which electronic evidence was adduced as evidence, the procedure by means of which such evidence was collected was not contested. The only South African case, to date, where the procedure deployed to collect the required electronic evidence came under scrutiny of the Court is *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C). See a reference to the detail of the case in footnote 135 of paragraph 4.2.3.1. below. This case is also relevant in a transborder search and seizure context (see paragraph 4.3.1.5 below).

of the Electronic Communications and Transactions Act.[36] It is interesting to note that section 82(4) provides specifically that any reference in the Criminal Procedure Act to "premises" and "article", for the purposes of the Electronic Communications and Transactions Act, includes an information system, as well as data messages.

4.2.2.2 Domestic search and seizure with a warrant

The general rule is that searches and seizures should, whenever possible, be conducted only in terms of a search warrant issued by a judicial officer, such as a magistrate, a judge or a peace officer.[37] Search warrants may be divided into general search warrants,[38] search warrants to maintain internal security and law and order[39] and cyber inspector search warrants.[40]

4.2.2.2.1 General search warrants

Section 21 of the Criminal Procedure Act provides for general searches and seizures under the authority of search warrants.[41] Section 21(1) provides that anything[42] which is susceptible to searches and seizures may be seized only by virtue of a search warrant issued in the following circumstances:

(a) by a magistrate[43] or justice of the peace,[44] if it appears to such a magistrate or justice from information under oath that there are reasonable grounds for believing that any such article is in the possession or under the control of any person or upon or at any premises within her area of jurisdiction; or

(b) by a judge or judicial officer presiding at criminal proceedings,[45] if it appears to such a judge or judicial officer that any such article in the possession or under the control of any person or upon or at any premises is required in evidence at such proceedings.

---

36 See paragraph 4.2.2.2.3 below for a discussion of searches and seizures on authority of the Electronic Communications and Transactions Act.

37 Section 21(1) of the Criminal Procedure Act reads "Subject to the provisions of sections 22, 24 and 25, an article referred to in article 20 shall be seized only by virtue of a search warrant...". Exceptions to this general rule are discussed in paragraph 4.2.2.3 below. It is interesting that section 7(2) of the proposed Computer Misuse Bill also stipulates that a computer system may be seized, or that samples or copies of applications or data referred to in section 7(1) may be taken, only by virtue of a search warrant, subject to the warrantless exceptions provided for in section 7(5).

38 See paragraph 4.2.2.2.1 below.

39 See paragraph 4.2.2.2.2 below.

40 See paragraph 4.2.2.2.3 below.

41 Note that section 7(3) of the proposed Computer Misuse Bill provides that the provisions of section 21 of the Criminal Procedure Act apply with the necessary changes to the issue and execution of a search warrant referred to in its section 7(2).

42 Referred to as "articles" in section 20 of the Criminal Procedure Act. See the discussion in paragraph 4.2.2.1 above.

43 A "magistrate", in terms of section 1 of the Criminal Procedure Act, for the purposes of the criminal code, includes additional magistrates, assistant magistrates, chief magistrates and senior magistrates. A judge or a regional magistrate may not issue search warrants at this stage. See Du Toit *et al Commentary on the Criminal Procedure Act* DEF 4.

44 Section 1 of the Criminal Procedure Act defines a "justice" as a person who is a justice of the peace under the provisions of the Justices of the Peace and Commissioners of Oaths Act 16 of 1963. Commissioned officers in the Police Service, the National Defence Force and the Correctional Services, Directors of Public Prosecutions and their senior staff, registrars and magistrates are considered justices of the peace. See Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 7.

45 This includes a judge or a regional court magistrate if she presides over the proceedings during which an application for a search warrant is made. An application is usually made by one of the parties to the proceedings, but, in terms of section

The discretion bestowed upon the judicial officer must be exercised in a reasonable and regular manner, in accordance with the law, and taking all relevant facts into account.[46] The decision by the magistrate or the justice of the peace whether to issue a warrant or not is based on information contained in a written affidavit or derived from verbal information given under oath. It is theoretically possible that, in the interests of expedience, an application for a search warrant can be made telephonically, although this is not current practice.[47] Before issuing a search warrant, the judicial officer must, on the basis of this information, decide whether the article to be searched for falls within the ambit of section 20 of the Criminal Procedure Act, and whether there are reasonable grounds to believe that the article is present at a particular place.[48] The information must also clearly indicate whether the article is under the control of a particular person and whether the search will be conducted within the area of jurisdiction of the judicial officer.

Section 21(3)(a) of the Criminal Procedure Act provides that a search warrant must be executed during the day,[49] unless the judicial officer who issues it gives written authorisation for it to be executed during the night. The reasonableness of the time when a warrant is executed is significant in terms of the Constitution, since it has an important effect on the extent to which the dignity and privacy of the person concerned is affected.[50] Night execution should be the exception. It would only be authorised where necessary for the proper administration of justice and the investigation of the case. Urgency usually constitutes a good reason for night execution.[51] In serving business continuity in a computing context, night execution may also be advisable, unless the organisation to be subjected to the search and seizure schedules, for example, large automated computing after business hours.

In terms of section 21(3)(b), a warrant may be issued and may be executed on a Sunday, as on any other day. It remains in force until it is acted upon or is cancelled by the person who issued it, or, if such person is not available, by a person with the same authority. It is, however, recommended that the issuing authority specifies a specific period in the warrant or otherwise withdraws the warrant on own initiative after a reasonable period, otherwise it is too grave an infringement on the privacy of the individual.[52]

21(1)(b) of the Criminal Procedure Act, the Court is entitled to act *mero motu*. There is no requisite of information under oath and the presiding officer will exercise her discretion on all the facts before her.

46 *Ismael v Durban City Council* 1973 (2) SA 362 (N).

47 It has been recommended that the information always be provided in written form for reference purposes. Alternatively, a transcript of the testimony under oath should be kept. See Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 37.

48 Joubert (ed) *Criminal Procedure Handbook* 116.

49 In terms of section 1 of the Criminal Procedure Act, a "day" means the space of time between sunrise and sunset and "night" means the opposite.

50 See Joubert (ed) *Applied Law for Police Officials* 310 and Joubert (ed) *Criminal Procedure Handbook* 118.

51 Du Toit *et al Commentary on the Criminal Procedure Act* 2-3.

52 Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 40.

The law enforcement officer executing the warrant under section 21 must, after such execution, upon demand of any person whose rights in respect of the search and seizure have been affected, hand a copy of the warrant to the person.[53]

4.2.2.2.2 Search warrants to maintain internal security and law and order[54]

Unlike section 21, where the application for a warrant is based on the suspected presence of an article mentioned in section 20, the reason for obtaining a warrant in terms of section 25 of the Criminal Procedure Act is linked either to state security or to the commission of an offence.[55] A magistrate or justice of the peace[56] may issue a warrant authorising a law enforcement officer to enter premises if it appears to her, from information on oath,[57] that there are reasonable grounds for believing that

(a) the internal security of the Republic or the maintenance of law and order is likely to be endangered by or in consequence of any meeting which is being held or is to be held in or upon any premises within her area of jurisdiction;[58] or

(b) that an offence has been or is being or is likely to be committed or preparations are being or are likely to be made for the commission of any offence upon any premises within her area of jurisdiction.

A law enforcement officer may enter the premises in question at any reasonable time for the purposes of

(a) carrying out such investigations and taking such steps as such a law enforcement officer may consider necessary to preserve the internal security of the Republic or to maintain law and order or to prevent any offence;[59]

---

53 Section 21(4) of the Criminal Procedure Act.

54 In *Wolpe v Officer Commanding South African Police, Johannesburg* 1955 (2) SA 87 (W), it was held that the basic duties of the police flow from the nature of the police as a civil force in the state, and that these basic duties are not confined to statutory duties. It was accordingly suggested that the legislature should define the duties and powers of the police in connection with combating what the state from time to time considers to be dangerous. This eventually led to the inclusion of section 25 in the Criminal Procedure Act, after it was first introduced in section 7 of the Criminal Procedure and Amendment Act 29 of 1955 and thereafter in sections 44(1) and 44(2) of the Criminal Procedure Act 56 of 1955. See Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 44 and Joubert (ed) *Criminal Procedure Handbook* 118.

55 Kriegler argues that (in view of the fact that all the necessary powers already exist in a combination of sections 21, 22, 23 and 24) section 25(1)(b) of the Criminal Procedure Act was inserted for the sake of convenience to facilitate issuing a single warrant, combining action in respect of the meeting with the possible seizure of evidential material (Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 44 and 45).

56 As in section 21(1) of the Criminal Procedure Act (see footnote 43 paragraph 4.2.2.2.1 above), judges and regional court magistrates are excluded. See Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 44.

57 In *Naidoo v Minister of Law and Order* 1990 (2) SA 158 (W), a search warrant was set aside, *inter alia*, because the informational basis for the search warrant was only partly provided under oath.

58 Section 25(1)(a) of the Criminal Procedure Act.

59 Section 25(1)(b)(i) of the Criminal Procedure Act.

(b) searching the premises or any person in or upon the premises for any article referred to in section 20 which such a law enforcement officer on reasonable grounds suspects to be on or upon or at the premises or upon such person;[60] or

(c) seizing any such article.[61]

A warrant issued in terms of section 25(1)(b)(i) confers wide powers on law enforcement officers, in that the officers' discretion as to what steps are necessary in this respect must be considered subjectively. The question is not whether the steps the law enforcement officer takes are objectively necessary, but whether she subjectively thinks that she has reason to believe that they are necessary.[62] If, however, the law enforcement officer enters the premises under authority of section 25(1)(b)(ii) with the purpose of searching and seizing the premises or any person thereupon for an article referred to in section 20 and which she reasonably suspects to be upon a person or on the premises, the test is an objective one.[63]

A warrant under section 25(1) may be issued on any day and remains in force until it is executed or is cancelled by the person who issued it or, if such a person is not available, by a person with the same authority.[64]

The requirement that a copy of the search warrant be handed over is equally applicable to section 25.[65]

4.2.2.2.3 Cyber inspector search warrants[66]

Chapter XII of the Electronic Communications and Transaction Act provides for the appointment of cyber inspectors within the Department of Communications.[67] Section 81(1) of the Electronic

---

60 Section 25(1)(b)(ii) of the Criminal Procedure Act.
61 Section 25(1)(b)(iii) of the Criminal Procedure Act.
62 Joubert (ed) *Criminal Procedure Handbook* 119.
63 *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D).
64 Section 25(2) of the Criminal Procedure Act.
65 Article 21(4) of the Criminal Procedure Act.
66 Altini argues that it is unlikely that the constitutionality of warrants issued to the "cyber watchdog force" will be successfully challenged, as the provisions facilitating these warrants closely mirror aspects of the Criminal Procedure Act operative today. See Altini "Commentary on the Electronic Communications and Transactions Bill, 2002" found on the Internet http://www.cliffedekker.co.za/literature/commentary/index.htm 9. This is probably a somewhat bold statement to make. See paragraphs 4.2.3 and 4.2.4 below for a discussion of the scope, conditions and safeguards applicable to searches and seizures.
67 These cyber inspectors have, to date, not been appointed. One of the CSIR recommendations regarding the implementation of chapter XII of the Electronic Communications and Transactions Act is that it would take an estimated 14 months to establish and operationalise the cyber inspectorate. These recommendations were already made in June 2002. See Malan and Venter *Cyber Inspectorate Research and Recommendations* 29. Budgetary constraints and prioritisation within the Department of Communications is stalling the appointment of the cyber inspectors. Also, the ongoing debate as to the correct placement of the cyber inspectorate has not yet been resolved. This debate is essentially linked to the pragmatic complexities of designating the cyber inspectorate to assist all law enforcement agencies, *inter alia*, with searches and seizures in computing environments (without endowing these law enforcement agencies with similar powers themselves). It is, of course, also linked to the standard "turf" disputes that so often characterise inter-departmental cooperation. During her term as the Head of the Digital Detective Unit of the Directorate of Special Operations of the National Prosecuting Authority, the researcher was given the opportunity to participate to some extent in this debate regarding the development of the cyber inspectorate. The matter was also occasionally raised at the Steering Committee level of the Office for Interception Centres

Communications and Transaction Act provides for the general powers[68] of cyber inspectors. When a cyber inspector performs any function in terms of the Electronic Communications and Transactions Act, she must be in possession of a certificate of appointment[69] which must be shown to any person who asks to see the certificate, particularly any person who is subject to an investigation, or an employee of that person.

Any statutory body with powers of inspection or search and seizure in terms of any law,[70] specifically including the South African Police Service (SAPS), may apply for assistance from a cyber inspector. Such assistance may be authorised by the Department of Communications on certain conditions.[71]

In terms of section 83(1) of the Electronic Communications and Transactions Act any magistrate or judge[72] may issue a warrant required by a cyber inspector, upon a request from a cyber inspector, but subject to the provisions of section 25 of the Criminal Procedure Act. The warrant must identify the premises or information system that may be entered and searched. It must also specify which acts may be performed under the warrant by the cyber inspector to whom it is issued.[73] Such a warrant to enter, search and seize may be issued at any time. It is valid until it has been executed or one month from the date on which it was issued. The warrant is no longer valid if the purpose for issuing it has lapsed or if the warrant is cancelled by the person

---

(established in terms of section 33 of the RICPCIA), where the researcher represented the National Prosecuting Authority. No resolution has been taken as yet. There is no indication as to when the appointment of the cyber inspectors will take place, if indeed any are appointed at all.

68 These powers include monitoring and inspecting any website or activity on an information system in the public domain and reporting any unlawful activity to the appropriate authority. Cyber inspectors may investigate the activities of cryptography and authentication service providers to ensure compliance with the provisions of the Electronic Communications and Transactions Act and they may issue written orders to that effect. Cyber inspectors may also conduct a compliance audit, as provided for in section 57 of the Electronic Communications and Transactions Act, in respect of critical database administrators. The investigation of the activities of authentication service providers that falsely claim that they, their products or their services have been accredited by the .za Domain Name Authority or recognised by the Minister of Communications also resorts within the areas of responsibility of the cyber inspectorate. Authentication is addressed in Chapter VI of the Electronic Communications and Transactions Act.

69 Section 80(4) of the Electronic Communications and Transactions Act. Section 80(2) of the said Act requires a cyber inspector to be provided with a certificate of appointment signed by or on behalf of the Director-General of the Department of Communications. The certificate must state that the cyber inspector has been appointed as such a cyber inspector. Section 80(3) allows for the signature on the certificate of appointment to take the form of an advanced electronic signature.

70 The reason for this requirement is unclear. It has been suggested that in cases where the cyber inspectors are approached to assist in a case, they will do so in an advisory capacity, without "taking over the investigation". In such cases, a search and seizure order is executed in accordance with the particular statutory body's own initiative to apply for a warrant in terms of its applicable legislation. However, if such legislation does not facilitate effective search and seizure, a cyber inspector may apply for a section 83 warrant. See Watney 2003 *TSAR* 70. The intention does not seem to allow other persons and entities who otherwise would not have been allowed to search and seize to approach the cyber inspectorate for assistance. The creation of the cyber inspectorate may also cause some economy of government effort, in that other statutory bodies, empowered also to search and seize, could tap into the centralised capacity of cyberforensic professionals. During the discussion of the Bill by the Parliamentary Portfolio Committee on Communication, it was stressed that the cyber inspectors should play a supplementary role to the SAPS. The intention is not that the functions of the police be taken over by the cyber inspectorate (Information Services: Parliament 14 June 2002 Summary of the Portfolio Committee on Communication Discussions: ECT Bill).

71 Section 81(2) of the Electronic Communications and Transactions Act. Watney argues that the fact that the SAPS cannot utilise the procedural provisions of the Electronic Communications and Transactions Act without the assistance of a cyber inspector is an anomaly. She also postulates that section 81(2) of the Electronic Communications and Transactions Act can be interpreted in such a way that, when cyber inspectors assist a specific statutory body, the investigation is subject to the legal prescripts normally applicable to such a statutory body. See Watney 2003 *TSAR* 73.

72 This does not include a peace officer, as is the case in terms of section 25 of the Criminal Procedure Act.

73 Section 83(3) of the Electronic Communications and Transactions Act.

who issued it or in that person's absence, by a person with similar authority.[74] A warrant to enter and search the premises may be executed only during the day, unless the judge or magistrate who issues the warrant authorises that it may be executed at any other time.[75]

On authority of a section 83(1) warrant and without prior notice, a cyber inspector may enter any premises or access an information system that has a bearing on an investigation at any reasonable time. The section 82(1) power to inspect, search and seize specifically mandates a cyber inspector to

(a) search the premises or the information system specified in the warrant;

(b) search any person on those premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

(c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation;

(d) demand the production of and inspect relevant licences and registration certificates as provided for in any law;

(e) inspect any facilities on the premises which are linked to or associated with the information system and which have a bearing on the investigation;

(f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence;

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;

(h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide her with such reasonable technical and other assistance as she may require for the purposes of chapter XII of the Electronic Communications and Transaction Act; or

(i) make such inquiries as may be necessary to ascertain whether the provisions of the Electronic Communications and Transactions Act, or any other law on which an investigation is based, have been complied with.

---

74 Sections 83(3) and 83(4) of the Electronic Communications and Transactions Act.
75 Section 83(5) of the Electronic Communications and Transactions Act.

A person who refuses to cooperate or who hinders a person conducting a lawful search and seizure in terms of section 82 is guilty of an offence.[76] It is interesting to note that, in addition to section 82, section 80(5)(a) also criminalises obstructing the course of justice in this context. It provides that any person who hinders or obstructs a cyber inspector in the performance of her functions in terms of chapter XII of the Electronic Communications and Transactions Act (including section 82) is guilty of an offence. A person who falsely claims to be a cyber inspector is also guilty of an offence.[77] The penalties attached to all three offences are a fine or imprisonment for a period not exceeding 12 months.[78]

4.2.2.3 Domestic search and seizure without a warrant

The following warrantless search and seizure doctrines are provided for:[79] consensual searches and seizures,[80] searches and seizures under exigent circumstances,[81] searches for the purpose of effecting an arrest,[82] searches of arrested persons,[83] entering premises for the purpose of obtaining evidence,[84] and searches of premises reasonably suspected of housing stolen stock or produce.[85] These powers of search and seizure are discussed below.

4.2.2.3.1 Consensual searches and/or seizures[86]

Section 22(a) of the Criminal Procedure Act provides that a law enforcement officer may, without a search warrant, search any person, container or premises for the purposes of seizing

---

76 Section 82 of the Electronic Communications and Transactions Act.

77 Section 80(5)(b) of the Electronic Communications and Transactions Act.

78 Section 89 of the Electronic Communications and Transactions Act. The Adjustment of Fines Act 101 of 1991 makes provision for the calculation of the fine which may be imposed by a court where the empowering legislation does not stipulate the amount thereof. Section 1(1)(a) of the Adjustment of Fines Act 101 of 1991, read with section 92(1)(a) and (b) of the Magistrate's Courts Act 32 of 1944 and Government Notice R1411 (*Government Gazette* 19435 of 30 October 1998), establishes the rate between the sentence of imprisonment and the permitted fine.

79 It is interesting to note that section 7(5) of the proposed Computer Misuse Bill provides for two warrantless search and seizure powers in respect of any computer system, application or data. These proposed powers are to some extent similar to those provided for in section 22 of the Criminal Procedure Act, but are more particularly aligned to the electronic environment. These provisions empower law enforcement officers, firstly, to conduct a search and seizure where the person in charge of, or otherwise concerned with, the operation, custody or care of a computer system, application or data consents to a search and/or seizure thereof. Secondly, it empowers a law enforcement officer to conduct a search and seizure if such a law enforcement officer believes, on reasonable grounds, that a search warrant will be issued under section 7(2) if she applies for such a warrant, and that the delay in obtaining such a warrant would defeat the object of the search. In the execution of a warrantless search and seizure in these two situations, a law enforcement officer may also avail herself of the powers provided for in section 7(4) of the proposed Computer Misuse Bill in respect of executing a search warrant. These powers entail the authorisation, at any time, to search for, have access to, and inspect and check the operation of any computer system, application or data if the law enforcement officer performing the search believes it to be necessary to facilitate the search (section 7(4)(a) of the Computer Misuse Bill). Furthermore, any person in charge of, or otherwise concerned with, the operation, custody or care of a computer system, application or data must provide such a law enforcement officer with the reasonable assistance that may be required to facilitate the execution of a search warrant (section 7(4)(b) of the Computer Misuse Bill).

80 See paragraph 4.2.2.3.1 below.

81 See paragraph 4.2.2.3.2 below.

82 See paragraph 4.2.2.3.4 below.

83 See paragraph 4.2.2.3.3 below.

84 See paragraph 4.2.2.3.5 below.

85 See paragraph 4.2.2.3.6 below.

86 See paragraphs 5.2.4.1.5 and 6.2.4.1.6 below for a discussion of consensual searches and seizures in the United States and England respectively. There are particularly interesting case law precedents in respect of consensual searches and seizures in a computing context in the United States. Useful parallels could be drawn between these and the South African context briefly set out here.

anything provided for in section 20, if the person concerned, or a person who may consent,[87] consents to such search for and seizure of the article in question. The onus in both instances is on the law enforcement officers effecting the search to prove that valid consent was given.[88]

Consent must be voluntary, thus no undue influence or duress must be exerted, such as explicit or implicit threats or a show of force.[89] Informing a person that unless she consents to the search, a search warrant will be obtained and the search will then be conducted without consent, will only be in order if the law enforcement officer has reason to believe that a search warrant will be issued to her if she should apply for it. If the law enforcement officer does not have reason to believe this, such a "threat" will amount to undue influence and the consent given as a result thereof is not regarded as valid consent.[90] The validity or voluntariness of consent must be determined from the totality of the circumstances.

It has been suggested that the law enforcement officer should also inform the person concerned of the purpose of the search, so as to empower the person to make an informed decision about whether to consent to or refuse the request for a search.[91] Where a person refuses to give consent, the exercise of this right cannot by itself give rise to reasonable grounds for suspicion. Although it may not be necessary to inform an individual that she has a right to refuse, the failure to do so may be a consideration in assessing the voluntariness of the consent.[92] Where a suspect was not specifically asked to consent, and did not specifically consent, the courts have held that quick action taken by the suspect to recover the article that was seized substantiated the argument that consent in terms of section 22(a) of the Criminal Procedure Act was not obtained.[93] Where consent is given under protest, but in an attempt to cooperate with the law enforcement agency, this conduct does not amount to consent as envisaged by section 22(a).[94]

---

87 The question of who may consent on behalf of another can become complicated. By comparison, for the purposes of consensual monitoring in terms of section 6 of the RICPCIA, a system controller could consent to the interception of an indirect communication in connection with carrying on business. Section 1 of the RICPCIA defines a "system controller" of, or in relation to, a private body, in the case of a natural person, as that natural person or any person duly authorised by that natural person; in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership; or in the case of a juristic person, the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer, or a person who is acting as such or any person duly authorised by such acting person. A "system controller" of, or in relation to, a public body means, in the case of a national department, provincial administration or organisational component mentioned in Column 1 of Schedule 1 or 3 to the Public Service Act, 1994 (Proclamation No. 103 of 1994), the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of the said Schedule 1 or 3 opposite the name of the relevant national department, provincial administration or organisational component or the person who is acting as such; or not so mentioned, the Director-General, head, executive director or equivalent officer, respectively, of that national department, provincial administration or organisational component, respectively, or the person who is acting as such; a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act 117 of 1998, or the person who is acting as such; or any other public body, the chief executive officer, or equivalent officer, of that public body or the person who is acting as such.

88 *S v Hammer* 1994 (2) SACR 496 (C) 498b.

89 *S v Madiba* 1998 (1) BCLR 38 (D).

90 Joubert (ed) *Applied Law for Police Officials* 313.

91 Steytler recommends, as an example, the following approach: "I am looking for a stolen wallet. Do you mind if I search you?" as opposed to a blanket request such as "May I search you?" See Steytler *Constitutional Criminal Procedure* 96.

92 Steytler *Constitutional Criminal Procedure* 96.

93 *Hako v Minister of Safety and Security* 1996 (2) SA 891 (TkS).

94 *Ndlovu v Minister of Police, Transkei* 1993 (2) SACR 33 (Tk).

Consent obtained from a lessee of premises to search a room that is sub-let to a person under investigation, such as a suspect or an accused person, where goods in such a room are not under the lessee's custody or control, does not constitute valid consent and would render a search and seizure unlawful.[95] An accused cannot consent on behalf of a co-accused, even if they happen to share a home.[96] Similarly, a person sharing a home with another person may not, on behalf of such a housemate, consent to a search in respect of the property of the housemate that happens to be in the shared home. Where the owner of a vehicle takes it for repairs, the owner's mere assertion of ownership *ex post facto* a seizure thereof will not nullify the valid consent to search the premises and seize the vehicle obtained from the person entrusted with the vehicle for repairs. The fact that the law enforcement officer might be informed of the fact that the vehicle belongs to somebody else will not alter this position.[97]

No specific provision has been made in chapter XII of the Electronic Communications and Transactions Act for consensual searches and seizures by the cyber inspectors, although such provision was indeed made in section 7(5) of the proposed Computer Misuse Bill.

4.2.2.3.2 Searches and seizures under urgent circumstances[98]

In terms of section 22(b) of the Criminal Procedure Act,[99] a law enforcement officer may (without a search warrant) search any person, container or premises for the purpose of seizing anything provided for in section 20, if on reasonable grounds she believes that

(a) a search warrant will be issued to her under section 21(1)(a)[100] if she applies for such warrant; and

(b) the delay in obtaining such a warrant would defeat the object of the search.

Whenever possible, even in urgent cases, a law enforcement officer should try to obtain the consent of the relevant person, since a search in terms of section 22(a) is easier to prove than a

---

95 *S v Motloutsi* 1996 (2) BCLR 220 (C) 229A-B and *S v Motloutsi* 1996 (1) SACR 78 (C).

96 In *S v Mayekiso* 1996 (2) SACR 298 (C), Accuseds One and Three shared a home. The police obtained consent from Accused One to enter their shared home and carried out a search. A bag with a pistol that belonged to Accused Three was seized. The Court held that there was no valid authority to search and seize the bag of Accused Three, since Accused One did not obtain consent from Accused Three in terms of section 22(a). It must also be kept in mind that section 35(5) of the Constitution imposes a duty on the Court to exclude evidence that in its admission would render the trial unfair or otherwise be detrimental to the administration of justice. The Court is, however, vested with a value judgement whether the admission of such evidence would have either of the two identified consequences. Sometimes fairness might require that evidence that has been unconstitutionally obtained be excluded. But there are also times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted. See *Key v Attorney-General, Cape of Good Hope Provincial Division* 1996 (6) BCLR 788 (CC) 13.

97 *Nombembe v The Minister of Safety and Security* 1998 (2) SACR 160 (Tk). See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-4A.

98 See paragraphs 5.2.4.1.3 and 6.2.4.1.4 below for a discussion of searches and seizures under urgent circumstances in the United States and England, respectively.

99 Section 22(b) of the Criminal Procedure Act was held to be constitutional in *S v Gumede* 1998 (5) BCLR 530 (D). See also *S v Sihlobo* [2004] JOL12831 (Tk).

100 See the discussion in paragraph 4.2.2.2.1 above.

search according to section 22(b) where the officer has to prove the requirement of reasonable grounds.[101] If the officer subsequently fails to obtain the required consent in terms of section 22(a), section 22(b) of the Criminal Procedure Act may be used. The unavailability of a magistrate does not render action in terms of section 22(b) of the Criminal Procedure Act lawful *per* se, but instead, a justice of the peace must be approached.[102]

The law enforcement officer must *ex post facto* be in a position to provide reasons or explanations as to why a search warrant was not obtained and why the delay in obtaining the warrant would have defeated the object of the search. Examples found in case law that validated such sufficient justification for purposes of section 22(b) include:

(a) where a suspect attempted to swallow evidence;[103]

(b) where a law enforcement officer, on the basis of her experience in dealing with illegal gambling cases, believed that gambling machines could easily be changed to amusement machines;[104] and

(c) where a law enforcement officer, acting on information that a suspect is in possession of stolen vehicles, finds that the engine and chassis numbers have been tampered with and the suspect was unable to provide full particulars of the people from whom she had purchased the vehicles.[105]

However, where a suspect had been in the undisturbed possession of a motor vehicle for almost two years and the vehicle was being used on a day-to-day basis by the suspect's wife, in the absence of any reason to believe that the suspect was about to dispose of the vehicle, a search was found unlawful.[106]

Search and seizure in terms of section 22(b) does not authorise a law enforcement officer to close down a business operating on premises which are being searched, as it could never have been the intention of the legislature to allow a law enforcement officer to hurt a person or business under suspicion more than is absolutely necessary under the circumstances. Specific authorisation to that effect must be obtained.[107] A business may also not be closed down if, in order to conduct an efficient search of the premises, the law enforcement officer would require

---

101 Joubert (ed) *Applied Law for Police Officials* 314.
102 *S v Motloutsi* 1996 (1) SA 584 (C).
103 *R v Beghin* 1933 EDL 24.
104 *Nel v Deputy Commissioner of Police, Grahamstown* 1953 (1) SA 487 (E).
105 *Mbutuma v The MEC for Safety and Security of the Eastern Province* 1998 (1) SACR 367 (Tk).
106 *Hako v Minister of Safety and Security* 1996 (2) SA 891 (TkS).
107 See *Concalves v Minister of Law and Order* 1993 (1) SA 161 (W). Sections 20 and 22 presuppose that a law enforcement officer is able to conduct the search and seizure concerned. These sections do not concern a situation where, for some reason, the officer is unable to do so and, in fact, needs to exercise additional powers to place herself in a position to conduct a search in terms of these sections.

assistance which would only be obtainable a few days later. This is the position even if, according to such a law enforcement officer, to allow the business to remain open would render the intended search and seizure partially or wholly ineffective. The destruction of an economically healthy business concern is clearly not envisaged by the section.[108]

Section 22 does not mention when the search and seizure must be executed, which implies that it may be executed during the night.[109]

Section 25(3) of the Criminal Procedure Act contains provisions that are similar to those in section 22(b), in respect of the commission of offences and instances where the state's security is endangered. A law enforcement officer may accordingly act without a search warrant in terms of section 25(1)(i), (ii) or (iii) if there are reasonable grounds to believe that a warrant will be issued to her under section 25(1)[110] when she applies for one, but that the delay in obtaining the warrant would defeat the object of the search. The objective test as to reasonable grounds must be applied.[111]

Watney[112] argues that section 25(3) of the Criminal Procedure Act, by virtue of section 82(3) of the Electronic Communications and Transactions Act, is also applicable to the cyber inspectors. This argument is supported by the fact that section 83(1) of the Electronic Communications and Transactions Act specifically incorporates section 25 of the Criminal Procedure Act.[113]

4.2.2.3.3 Searches of arrested persons[114]

In terms of section 23(1)(a) of the Criminal Procedure Act, any peace officer[115] who arrests a suspect may search the person who has been arrested and seize any article referred to in section 20 in possession of or under the control of the arrested person. However, there must be

---

108 Du Toit *et al Commentary on the Criminal Procedure Act* 2-4A.

109 However, in *Hako v Minister of Safety and Security* 1996 (2) SA 891 (TkS), where the search was executed in the middle of the night, it was considered a factor prejudicial to the reasonableness of law enforcement conduct.

110 See the discussion in paragraph 4.2.2.2.2. above. It has been submitted that section 25 must, in particular, be executed with caution, as it could infringe on the constitutional rights to dignity, privacy, freedom of expression, freedom of religion, political rights and freedom of association (see Joubert (ed) *Applied Law for Police Officials* 314).

111 *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D), *S v Boshoff* 1981 (1) SA 393 (T) 397F-H and *Control Magistrate, Durban v Azanian Peoples Organisation* 1986 (3) SA 394 (A). See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-7.

112 Watney 2003 *TSAR* 73.

113 With the specific inclusion of section 25 of the Criminal Procedure Act, it is doubtful, however, whether all the search and seizure provisions in the Criminal Procedure Act could *ipso facto* be made applicable to the cyber inspectors on the basis of section 82(3) of the Electronic Communications Act.

114 See paragraphs 5.2.4.1.1 and 5.2.4.1.2 below for a discussion of the search and seizure of arrested persons in the United States. Paragraphs 6.2.4.1.1 and 6.2.4.1.2 address the position in English law. There are interesting case law precedents applicable in a computing context in respect of the search and seizure of arrested persons, particularly in the United States. Some useful parallels could be drawn between these precedents and the South African context briefly set out here.

115 Section 1 of the Criminal Procedure Act defines a "peace officer" as any magistrate, justice, police official or correctional official, as defined in section 1 of the Correctional Services Act 8 of 1959, and, in relation to any area, offence, class of offence or power referred to in a notice issued under 334(1) of the Criminal Procedure Act, any person who is a peace officer under that section. It has been held that this definition will be interpreted strictly (*R v Debele* 1956 (4) SA 570 (A)). In *Rabie v Minister of Police* 1984 (1) SA 786 (W), it was ruled that a sergeant in the then South African Police force, who was employed as a mechanic to repair law enforcement vehicles, was to be considered a peace officer.

reasonable grounds for an arrest before the law enforcement officer may search an arrested person in terms of section 23.[116] Where a peace officer is not a law enforcement officer, she must deliver any seized article to a law enforcement officer forthwith. Section 23(1)(b) provides that a person (other than a peace officer) who arrests a suspect may not search the person, but may seize a section 20 article[117] in the possession or under the control of the person who is arrested. When any person is arrested, the person making the arrest may place in safe custody any object which is found on the person who is arrested and which may be used to cause bodily harm to the arrestee or others.[118] The power to search the person of an arrestee without probable cause or a warrant appears to be constitutionally inoffensive.[119] The following principles should, however, be observed when applying section 23:[120]

(a) The search should pursue an object consistent with the proper administration of criminal justice.

(b) Although it might be constitutionally permissible to search the environment in which the accused is arrested, section 23 provides statutory authority only for a search of the person of an arrestee, not the area within which the search takes place.

(c) The seizure, without searching, of section 20 articles in the possession, custody or control of the arrestee is permissible, provided that they are in the immediate environment where the arrest took place. Possession, custody and control should be given a restrictive interpretation.[121] Articles which may afford evidence and which are in the custody or under the control of the arrestee may be seized, but no prior search for such articles is explicitly authorised. Allowing for seizure presupposes that the articles must be in the plain view[122] of the arrestor.[123] Anything under the arrested person's immediate control may be seized. As any limitation of the right to privacy should have a legal basis, it is, for example, doubtful whether section 23(1) covers the search of a vehicle which the arrestee drove or in which she was a passenger.

---

116 Justice College *Search and Seizure* 9.

117 See paragraph 4.2.2.1 above for a reference to what constitutes an article that may be seized in terms of section 20 of the Criminal Procedure Act.

118 Section 23(2) of the Criminal Procedure Act.

119 Section 23 was held constitutional in *S v Gumede* 1998 (5) BCLR 530 (D). See also Steytler *Constitutional Criminal Procedure* 97.

120 Steytler *Constitutional Criminal Procedure* 99.

121 Steytler *Consitutional Criminal Procedure* 101.

122 See paragraphs 5.2.4.1.4 and 6.2.4.1.5 in relation to the plain view warrantless exceptions in the United States and England in the legislative frameworks.

123 Steytler *Consitutional Criminal Procedure* 101. See, however, *S v Nader* 1963 (1) SA 843 (O) and *S v Mataung* 1962 (3) SA 611 (O). In these cases, the Court held that articles that are in the custody or under the control of an arrested person do not only refer to items on the person, but would include articles found in a motor vehicle, flat or premises that the arrested person is in or on. If a person, for example, is arrested at her home, the home may be searched. It was held that where a person was arrested at a café and waste business, seizure of articles found in a storeroom on the property and in the back yard of the premises was justified in terms of section 23. If, however, a person is arrested on the street, her home may not be searched. Kriegler advances that "possession" in terms of section 36 of the General Law Amendment Act 62 of 1955 may be used for comparative purposes. See Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 42.

4.2.2.3.4 Searches for the purpose of effecting arrests

According to section 48 of the Criminal Procedure, peace officers and private individuals who are authorised by law to arrest anyone in respect of any offence and who know or reasonably suspect such a person to be on any premises may break open, enter and search such premises for the purposes of effecting the arrest. However, they must first audibly demand entry into such premises and state the purpose for which they seek entry and have failed to gain entry.[124]

4.2.2.3.5 Entering premises for the purpose of obtaining evidence

Section 26 of the Criminal Procedure Act authorises law enforcement officers investigating an offence or alleged offence to enter any premises without a warrant to obtain evidence. The law enforcement officer must reasonably suspect that a person who may furnish information with reference to an offence is on the premises. Such a person may be interrogated and a statement obtained from her. However, the law enforcement officer may not enter a private dwelling without the consent of its occupier. The occupier of the private dwelling is allowed to eject the officer from her house and her premises, because such entry without consent would be unlawful.[125]

The right of the law enforcement officer to interrogate the person on the premises is clear. It is not necessary to obtain her consent before questions are put to the person, but the person has the right to remain silent.[126]

4.2.2.3.6 Searches of premises reasonably suspected of housing stolen stock or produce

Section 24 of the Criminal Procedure Act enables any person who is lawfully in charge or occupation of premises and who reasonably suspects that stolen stock or produce[127] is on or in the premises to enter and search such premises or any person in or on such premises at any

---

124 See the discussion in Joubert (ed) *Criminal Procedure Handbook* 122, where it is stated that a number of court decisions on the forerunner of section 48 of the Criminal Procedure Act still apply to section 48. In *S v Jackelson* 1926 TPD 685, it was held that persons who had ejected a law enforcement officer who had entered premises without first demanding and being refused admission could not be convicted of obstructing such an officer in the execution of her duty. However, in *Rudolf* 1950 (2) SA 522 (C), the Court held an arrest effected when the accused attempted to rescue a suspect fleeing from the law enforcement officer who failed first to demand admission to the premises to be a lawful arrest. It was contended, *inter alia*, that the law enforcement officer had made an unlawful entry and that the arrest was consequently an unlawful one. The Court distinguished *Jackelson* mainly on the grounds that the accused in *Jackelson* had ejected the constable before he had effected an arrest, while in *Rudolf* the arrest had been effected when the accused attempted to rescue the suspect. See also *Andresen v Minister of Justice* 1954 (2) SA 473 (W).

125 *Minister van Polise v Gamble* 1979 (4) SA 759 (A) 764D.

126 See *Gosschalk v Rossouw* 1996 (2) SA 476 (C). The law enforcement officer may only forcibly obtain a statement from a witness in terms of section 205 of the Criminal Procedure Act. Law enforcement officers may attempt to persuade the person to be interrogated to cooperate, but in view of the right to silence, such attempts will have to be, in the words of Kriegler "behoorlik, taktvol en betreklik kortstondig" [appropriate, tactful and relatively brief] (Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 47). Also see Du Toit *et al Commentary on the Criminal Procedure Act* 2-7.

127 As defined in any law relating to the theft of stock or produce (section 24 of the Criminal Procedure Act). It must be borne in mind that although this section is aimed at tangible stolen stock or produce, at the very least, significant amounts of electronic evidence may be generated in respect of such tangibles (as opposed to data being an instrumentality or object of the offence that the search and seizure is aimed at).

time, if a law enforcement officer is not available. Entering and searching is also allowed where an article has been placed in or on such premises or is in the custody or possession of any person upon or in such premises in contravention of the law relating to intoxicating liquor, dependence-producing drugs, arms and ammunition or explosives. The person who performs the search and takes possession of such stock, articles or produce must deliver it to a law enforcement officer forthwith.

Those who may enter the premises include the owner of the premises, a lessee or an employee who has been put in charge of the premises by the owner or lessee.[128] The articles that may be seized are specifically mentioned in section 24. This implies that the scope regarding such articles is not as wide as that allowed by section 20.[129]

4.2.3 Scope

4.2.3.1 Particularity and specificity[130]

It is an important principle of the law of criminal procedure that all directives in a warrant must be strictly interpreted to protect any individual against excessive interference by the state.[131] There must be precision in respect of the authorisation with regard to, *inter alia,* the official to whom the warrant is addressed, the individual and/or premises that constitute the object of the search and seizure, the articles to be seized, the purpose of the search and seizure, the period during which it is allowed and the acts authorised under the warrant. [132]

Precision of the authorisation with regard to both the objects that are sought and the places to be searched give meaning to the protection which prior judicial authorisation affords.[133] South African courts have consistently required the content of a warrant to be certain. Articles that are sought must be described in sufficient detail, lest the warrant be declared void for vagueness.[134]

---

128 Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 43.

129 See paragraph 4.2.2.1 above for a discussion of section 20 of the Criminal Procedure Act.

130 See paragraphs 5.2.3.1 and 6.2.3.2 below for a discussion of the application of the specificity and particularity requirements in the United States and England respectively. Interesting precedents of the application of these requirements in a computing context have been set in the United States and could be drawn on for purposes of the application thereof in the South African legislative framework.

131 See Joubert (ed) *Criminal Procedure Handbook* 117. This was also the position in pre-Constitution South Africa. See, for example, *Minister of Justice v Desai* 1948 (3) SA 473 (W); *S v Pogrund* 1974 (1) SA 244 (T) and *National Union of South African Students v Divisional Commissioner, South African Police, Cape Western Division* 1971 (2) SA 553 (K). In *Zuma v NDPP* [2006] JOL 16755 (D) the Court held that a warrant must specify the offences and convey intelligibly the ambit of the search. The investigating officer's reference to the suspected offences was held to be vague. A catch-all paragraph for searchers to seize any item "which might have a bearing on the investigation" is invalid.

132 In *Smit and Maritz Attorneys v Lourens NO* 2002 (1) SACR 152 (W), it was ruled that a warrant addressed to "all law enforcement officers" was invalid, in that the decency and order required by section 29 of the Criminal Procedure Act also require that the warrant be addressed to a specific officer. The restrictive interpretation of a "law enforcement officer" must be an identified officer so as to provide a further safeguard to the rights of persons subject to seizure. In *De Wet v Willers NO* 1953 (4) SA 124 (T), a distinction was made between a juristic person and the secretary of such a juristic person.

133 Steytler *Constitutional Criminal Procedure* 93. Carstens and Lucouw argue that in the case of "pure information" it will probably be impossible to clearly describe the "article" to be seized. They advise that the tangible "containers" of the information should be specified. See Carstens and Lucouw *E-Commerce in Practice* 112.

134 See *SA Police v SA Associated Newspapers* 1966 (2) SA 503 (A) and *Naidoo v Minister of Law and Order* 1990 (2) SA 158 (W)). In *Powell v Van Der Merwe* 2005 (5) SA 62 (SCA) a search and seizure in terms of section 29(5) of the National

Once the warrant has been issued, the person executing the warrant cannot widen its scope, even if the statute authorises wider powers than those included in the warrant.[135] However, this rule should not preclude the seizure, as such, of objects not mentioned in the warrant which may afford evidence of the commission of an offence.[136]

It is imperative that warrants be clearly worded.[137] The search warrant must clearly define specific articles to be seized. If the search warrant only specifies the articles to be seized in broad and general terms, it might be construed as indicative of the fact that the judicial officer did not apply her mind properly.[138] The description of articles in the warrant must be sufficiently clear, so as to empower the person executing the warrant to determine with reasonable certainty what has to be seized.[139] Every article does not have to be described in detail, but categories or classes of articles may be identified, as long as reasonably clear descriptions are given.[140] A search warrant that authorises the seizure of documents has, for example, been

---

Prosecuting Authority Act 32 of 1998 was scrutinised. The Court held that the warrant "had been riddled with imprecision and vagueness, and it had to be set aside on that ground alone" (at 85). It has been held that South African law has had a long history of scrutinising search warrants with (sometimes technical) rigour and exactitude. These common law rights are now enshrined in section 14 of the Constitution (the right to privacy). In *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C), the Court held the search warrants to be invalid, *inter alia*, on the ground that the warrants themselves were not sufficiently specific. The searches that were carried out on the basis of them went beyond their scope and were therefore unlawful. Of particular interest is the fact that the three warrants in question referred to "documentation" which "is on reasonable grounds believed to be intended to be used in the commission of an offence" and which is to be seized if found. The warrants all have attached to them an "Annexure A". In the case of two of the three warrants, the annexure also referred to "any computer hardware containing information relating to the abovementioned entities and structures; all computer media storage devices; all computer hardware and software; all computer data and erased data; all computer periferals (sic); all stiffies, CD's, DVD's". It was held that it is not entirely correct to say that "in terms of the warrant, the search team was authorised to remove the CPU's and other equipment for storing electronic information at Mowbray in order to copy the information off-site". The search warrant itself authorised only a search for, and seizure of, "documentation" (at 36-37). The Court noted that "by no stretch of the imagination could all the computer hardware, software, and 'peripherals' mentioned in annexure 'A' to the Mowbray and Table View search warrants be classified as 'documentation'". The Court refused to accept that an off-site search became the standard way of searching for electronically stored information in South Africa and elsewhere in the world, as advanced by the respondents. It was held that it was unnecessary for the police to remove the items from the applicants' premises as a computer systems administrator deposed to a replying affidavit for the applicants that the electronic data found at Mowbray could effectively have been searched and copied at the premises within a few hours, using technology that is readily available. Instead, the applicants' business operations were "seriously disrupted for several days" while the police were searching and copying the data "off-site". It is axiomatic that search and seizure of this kind must be carried out in the least intrusive and disruptive manner possible (at 39). The Court concluded that the removal by the police of the bulk of electronic material from the Mowbray premises was unlawful for this reason alone, even if for no other, and was not properly authorised by the search warrant (at 39).

135 See, for example, *NUSAS v Divisional Commissioner South African Police* 1971 (2) SA 553 (C); *Cheadle, Thompson & Haysom v Minister of Law and Order* 1986 (2) SA 279 (W) and *Naidoo v Minister of Law and Order* 1990 (2) SA 158 (W).

136 Steytler *Constitutional Criminal Procedure* 93.

137 *World Wide Film Distributors (Pty) Ltd v Divisional Commissioner, South African Police* 1971 (4) SA 312 (K) and *S v Pogrund* 1974 (1) SA 244 (T).

138 *Smith, Tabata & van Heerden v Minister of Law and Order* 1989 (3) SA 627 (E). The defect of vagueness would not be cured by an instruction that a law enforcement officer must search for documents which "may" afford evidence of the commission of the crime (*Minister of Justice v Desai* 1948 (3) SA 395 (A)). If a warrant is worded too broadly, it will be set aside (see *World Wide Film Distributor v Divisional Commissioner* 1971 (4) SA 312 (K)). See also Joubert (ed) *Criminal Procedure Handbook* 117.

139 *SASOL III (Edms) Bpk v Minister van Wet en Orde* 1991 (3) SA 766 (T). Articles that were taken unlawfully must be returned. The law enforcement officer may be instructed to pay for the costs, including costs *de bonis propriis;* but where articles were taken *bona fide*, no cost orders will be made against the law enforcement officer (see *Pullen v Waja* 1929 TPD 838; *Hodes v Deputy Commissioner of Police* 1959 (4) SA 650 (K) and Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 40). In *Powell NO v Van Der Merwe* 2005 (5) SA 62 (SCA), the Court ruled that the search warrant was "breathtaking in its scope". The search warrant authorised the examination of "any object" and the seizure of "anything" that could be relevant to "the preparatory investigation concerned" (at 79-80). No offence was mentioned in the search warrant or in the application for the warrant. The Court ruled that it was no cure for an overbroad warrant to say that the subject of the search knew or ought to have known what was being looked for. The warrant must itself specify its object and must do so intelligibly and narrowly within the bounds of the empowering statute. A warrant must convey intelligibly to both searcher and searched the ambit of the search authorised (at 85).

140 *Cine Films (Pty) Ltd v Commissioner of Police* 1972 (2) SA 254 (A).

found adequate to be authorisation also to seize books.[141] However, even though the person subjected to the search and seizure must be informed as clearly as reasonably possible of what she must surrender, the investigations of the law enforcement officers may not be hampered by a duty to provide technical detail in respect of the articles they are seeking to find and seize.[142]

Section 21(2) of the Criminal Procedure Act stipulates that a warrant must direct a law enforcement officer to seize the article in question. To that end the warrant must specifically authorise such an officer to search any person identified in the warrant, or to enter and search any premises identified in the warrant and to search any person found on or at such premises. A search warrant must empower the law enforcement officer executing the search to identify the person identified in the warrant.[143] If the search warrant is aimed at the search of premises, such premises must be clearly and accurately identified. It would be in order also to authorise the search of all persons on or at such premises, without further providing detailed descriptions of such persons. It is, however, recommended that there must be an apparent connection between these persons and the activities happening on the premises, as a casual bystander should not be included in the scope of the authorisation.[144]

Although section 21 does not require the suspected offence to be set out in the warrant, it is desirable to do so in order to facilitate the interpretation of the warrant.[145] The warrant must also clearly define the purpose of the search.[146] Steytler suggests[147] that, in the context of criminal justice, the search for and seizure of articles should only be regarded as legitimate for the following purposes:[148]

---

141 *Seccombe v Attorney General* 1919 TPD 270.

142 Du Toit *et al Commentary on the Criminal Procedure Act* 2-3.

143 It is not necessary to identify the person to be searched by name. The person may also be described in another way, as long as the description is detailed and precise. See Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 38. In *Community Repeater Services CC v Minister of Justice* 2000 (2) SACR 592 (SE), the Court referred to the general language in which the warrants were couched (there was no reference to the personal entity from whom the apparatus concerned was to be seized) and, *inter alia,* for that reason held the warrants to be invalid.

144 Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 38.

145 *Cine Films (Pty) Ltd v Commissioner of Police* 1971 (4) SA 574 (W) 581.

146 In *Community Repeater Services CC v Minister of Justice* 2000 (2) SACR 592 (SE), the validity of a search warrant was considered where there was a seizure of a radio apparatus in order to exact the payment of a license fee. This was held to be an improper purpose for the issuance of a warrant and the warrant was therefore invalid.

147 Steytler *Consitutional Criminal Procedure* 86.

148 In *Highstead Entertainment (Pty) Ltd t/a 'The Club' v Minister of Law and Order* 1993 (2) SACR 625 (C), an interdict against a further search and seizure was granted, as it could not be said to be necessary in respect of the pending prosecution. The State was ready to proceed with its case in the prosecution of an accused for the alleged contravention of section 6(1) read with section 8(d)(i) of the Gambling Act 51 of 1965. The State had no need to procure further articles which could have been of use in proving its case. The accused, on the basis of expert opinion, had made out a *prima facie* case, although disputed by the State, that the games played at the accused's club were not games of chance. The accused was willing to make admissions necessary to ensure that all that would be in issue at the criminal trial was whether the games in question were games of chance in terms of the Gambling Act 51 of 1965. See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-2A. The argument that it could be objectively determined whether the relevant articles really were necessary for the evidential purposes in the trial was rejected in the case of *Mandela v Minister of Safety and Security* 1995 (2) SACR 397 (W) and *Van Der Merwe v Minister van Justisie* 1995 (2) SACR 471 (O) cases. Kriegler also supports the argument accepted in the latter two cases that the authorising magistrate's decision can only be set aside if the grounds upon which the application for the warrant were based were not actually considered (Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 37).

(a) to be confiscated because their possession is unlawful,[149]

(b) to return them to their rightful owner,[150]

(c) to be forfeited to the state if they were used in the commission of an offence,[151] and

(d) to be used as evidential material in a prosecution, as provided for in section 20(b) of the Criminal Procedure Act.[152]

Kriegler[153] advances that not only the purpose for, but also the period during which the law enforcement officer may keep the articles, as provided for in subsequent sections of chapter 2 of the Criminal Procedure Act, regulate the exercise of the power of search and seizure. A higher court may intervene to prevent abuse.[154] Section 31 has to be read as an adjunct to section 20, in that both sections are aimed at facilitating the investigation and at finding proof of some offence with which the confiscated article was connected. However, it is imperative that the State acts with reasonable expedition in instituting criminal proceedings.[155] The State bears the onus to prove that a reasonable time has not lapsed.[156] Once it appears that an article seized under section 20 and as envisaged under section 30(c) is not to be used at a future trial, it must be returned to the person from whom it was seized.[157]

A warrant which purports to authorise the seizure of anything which does not fall within the description of articles, as set out in section 20, is invalid.[158] If an article does not fall within the

---

149 Section 31 of the Criminal Procedure Act.

150 Section 30(b) of the Criminal Procedure Act.

151 Section 35(5) of the Criminal Procedure Act.

152 Steytler argues that the other two grounds, as set out in sections 20(a) and 20(c) of the Criminal Procedure Act, are constitutionally suspect because their purpose is unclear (Steytler *Constitutional Criminal Procedure* 86).

153 Kriegler *Hiemtra Suid-Afrikaanse Strafproses* 32.

154 In *Dyani v Minister of Safety and Security* 2001 (1) SACR 634 (Tk), the law enforcement officer seized a motor vehicle that had allegedly been stolen. The seizure was in terms of sections 20 and 22. It was held that where the seizure was unlawful, the Court would set the seizure aside, notwithstanding the fact that the applicant could not lawfully possess the vehicle. The Court also set aside affidavits where the commissioner of oaths before whom the statements were attested to had an interest in the proceedings.

155 In *Hako v Minister of Safety and Security* 1996 (2) SA 891 (Tk S), it appeared in an application for an order directing the release of a motor vehicle unlawfully seized by the law enforcement officer that the officer had intended to institute criminal proceedings against the applicant. The Court ordered the State to release the vehicle to the applicant, but interdicted the applicant from disposing of or altering the vehicle pending the institution of criminal proceedings against him by the State within one month. See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-2A and 2-2B. In *Choonara v Minister of Law and Order* 1992 (1) SACR 239 (W), the Court ordered a vehicle to be returned to the applicant, as the law enforcement officer had not shown that the applicant could not legally possess the vehicle and the time taken to investigate had become so extended as to constitute an act oppressive of the rights of the applicant without offering any real prospect of further advance by the state in the investigation. In *Datnis Motors (Midlands) (Pty) Ltd v Minister of Law and Order* 1988 (1) SA 503 (N), it was decided that the vehicles should be returned to the possessor prior to the seizure where he is entirely blameless and section 37(1) of the General Law Amendment Act 62 of 1955 was not applicable. Also the law enforcement officer was unable to discover whether the vehicles were stolen, and by whom, after two years of investigation, and the then Attorney-General declined to prosecute. In *Lavers v Hein & Far BK* 1998 (3) SA 195 (SCA), it was decided that in a matter where a vehicle was seized in terms of section 20, prescription commences to run not at the time of the seizure, but at the time when the person becomes aware of the fact that the article will not be returned to her. Also see *Dookie v Minister of Law and Order* 1991 (2) SACR 153 (D) 156f, *Booi v Minister of Safety and Security* 1995 (2) SACR 465 (O) 468g-469e and Du Toit *et al Commentary on the Criminal Procedure Act* 2-2A and 2-2B.

156 *Ntoyakhe v Minister of Safety and Security* 1993(2) SASV 625 (OK).

157 *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D). Also see Du Toit *et al Commentary on the Criminal Procedure Act* 2-2A.

158 A warrant could be partially valid and partially invalid. See, for example *Cine Films (Pty) Ltd v Commissioner of Police* 1972 (2) SA 254 (A) (it must be borne in mind that the current section 20 is much wider than its predecessor, which was applicable in this case) and *Divisional Commissioner, SAP v SAAN* 1966 (2) SA 503 (A). See also Kriegler *Hiemtra Suid-Afrikaanse Strafproses* 38.

authorisation of the search warrant, but is relevant to the crime, it should not be seized until a search warrant is obtained to seize the article.[159] However, in those exceptional circumstances when the circumstances would have justified a search without a warrant, the article should be seized.[160]

The conduct of the law enforcement officer executing the warrant must be reasonable at all times and she must act only as authorised throughout the execution.[161] It is necessary for the warrant to authorise both the search and the seizure before the seizure can take place.[162] A warrant for a search` and seizure may be combined with an arrest warrant, but it may not be made provisional on locating incriminating evidence.[163]

The scope of the articles that may be seized under section 24 of the Criminal Procedure Act is not as wide as that of section 20, as the articles that may be seized are specifically mentioned in section 24.[164]

Section 83(3) of the Electronic Communications and Transactions Act provides that a warrant authorising a cyber inspector to enter, search and seize must identify the premises or information system that may be entered and searched. Such a warrant must also specify which acts the cyber inspector to whom the warrant is issued may perform under that warrant.

Section 82(1)(f) empowers cyber inspectors to have access to and inspect the operation of any computer or equipment that forms part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence. Section 82(1)(f) of the Electronic Communications and Transactions Act has been pointed out as the only section that does not refer to a specific investigation, but, instead, refers to "any offence".[165]

---

159 It is important to note that the authorisation determines which articles may be seized, and not the application for the search warrant (*Van Der Merwe v Minister van Justisie* 1995 (2) SACR 471 (O) 488a-b and 488f-g).

160 Joubert (ed) *Applied Law for Police Officials* 310.

161 See *Divisional Commissioner, South African Police v SAAN* 1966 (2) SA 503 (A) and *De Wet v Willers NO* 1953 (4) SA 124 (T).

162 *NUSAS v Divisional Commander, South African Police* 1971 (2) SA 533 (C).

163 Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 40. It is interesting to note that sections 45 and 330 of the Criminal Procedure Act allow for the execution of a warrant for arrest when a telegram is sent stating that a warrant has been issued. If the warrant itself is transmitted telegraphically or by means of a similar written or printed communication and a copy of the telegram or such written communication is executed in the prescribed manner, it has the same effect as the execution of the warrant itself. A telephonic message, however, does not comply with section 330. See Du Toit *et al Commentary on the Criminal Procedure Act* 33-2. No similar provision is made for search and seizure warrants.

164 See paragraph 4.2.2.3.6 above.

165 Note that the Bill published on 1 March 2002 in Government Gazette 23195 also allows cyber inspectors to have access to and inspect any computer or equipment forming part of an information system which the cyber inspector has reasonable cause to suspect "is or has been used in connection with any offence".

Watney[166] contends that it appears that the legislature authorises cyber inspectors to proceed with a search and seizure even when such a search and seizure is not specifically authorised in the warrant. Such a situation may arise where a cyber inspector, in the course of a search and seizure in terms of a warrant, forms a reasonable suspicion that an offence has been or is being committed using computer equipment on the premises, where the investigation of this equipment was not specified in the warrant. Watney[167] argues further that section 82(1) is a practical arrangement to further the investigation of crime, in that a suspension of a search and seizure to acquire a new or additional warrant may cause or allow valuable evidence to be destroyed. This argument must, however, be considered in the light of the fact that the general introduction to section 82(1) allows the cyber inspectors to "enter any premises or access an information system that has a bearing on an investigation". It is submitted that section 82(1)(f), in the first instance, is initiated within the context of an initially specified investigation, but that the scope of this investigation may be extended to access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material reasonably suspected to be used or to have been used "in connection with any offence".

4.2.3.2 Categories of crimes

Search and seizure in terms of the chapter 2 of the Criminal Procedure Act[168] and section 83 of the Electronic Communications and Transactions Act are aimed at all categories of crimes, including the harvesting of electronic evidence relating to any offence.

4.2.3.3 Use of force in order to conduct a search

Section 27(1) of the Criminal Procedure Act empowers a law enforcement officer who is entitled to search any person or premises, or lawfully enter premises, to use such force as may be reasonably necessary[169] to overcome any resistance against such a search or entry of the premises, including breaking any door or window of such premises.

---

166 See Watney 2003 *TSAR* 71.

167 See Watney 2003 *TSAR* 71.

168 "Offence" in section 25(1)(b) of the Criminal Procedure Act is not limited only to offences relating to state security and the maintenance of law and order. See Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 45.

169 This will meet the constitutional requirement of proportionality. See Steytler *Constitutional Criminal Procedure* 100. It is interesting to note the two conflicting judgments of *Minister of Safety and Security v Gaqa* 2002 (1) SACR 654 (C) and *Minister of Safety and Security v Xaba* 2003 (2) SA 703 (D) in respect of the nature and extent of the force to be used in terms of section 27. In *Minister of Safety and Security v Gaqa* 2002 (1) SACR 654 (C), the surgical removal of a bullet from the leg of an accused for the purposes of ballistic tests was ordered on the basis that the law enforcement officers are entitled to use reasonable force to remove the bullet. The accused refused to consent to the removal of the bullet from his leg. The Court, however, considered the bullet to be a section 20 article referred to in the search warrant. In *Minister of Safety and Security v Xaba* 2003 (2) SA 703 (D), in respect of identical circumstances, it was ruled that since a law enforcement officer was not entitled to search a suspect by operating on the suspect's leg, the officer could not use reasonable force authorised by section 27 to do so. Also, it was held that a law enforcement officer could not delegate the officer's powers to search to a doctor, who would then execute the search instead. See also Watney 2003 *TSAR* 587-594 for a discussion of these two judgments. Watney refers, by comparison, to the practice of co-opting individuals with specialised knowledge in information technology and forensic accountancy to assist with investigations where such specialised skills are required (593). Search and seizure warrants authorising private individuals to assist law enforcement officers during a search and seizure have been applied for and granted on the basis that good cause was shown for private individuals, specified by name, to assist (see *Smit and Maritz*

Section 27(1) is also applicable where no warrant has been issued, but where the urgent circumstances of sections 22(b) and 25(3) are present.[170] Section 83(1) of the Electronic Communications and Transactions Act is, in turn, subject to the provisions, *inter alia*, of section 25(3) of the Criminal Procedure Act. The proviso to section 27(1) is that admission to the premises must first be demanded audibly and that the purpose for which the law enforcement officer wants to enter the premises must be announced loudly.[171] The exception to this proviso is the so-called "no-knock" clause contained in section 27(2). If a law enforcement officer is of the opinion, on reasonable grounds, that any article which is the subject of the search may be destroyed or disposed of[172] if entry needs to be audibly demanded first, she may enter unannounced. However, if the only reason for non-compliance with the said proviso is that the law enforcement officer is in a hurry, section 27(2) does not apply and it does not authorise entry to the premises.[173]

If no one is on the premises, entry in terms of this section would depend on the circumstances of the case. Factors that would be taken into consideration include the seriousness of the crime, the urgency of the search, seizure or entry, the period the law enforcement officer would have to wait for the occupier to return, and the nature of the articles to be searched or seized.[174]

4.2.3.4 Jurisdiction

Section 20 of the Criminal Procedure Act specifies which articles may be searched for and seized. Sections 20(a) and (b) of the Criminal Procedure Act both refer to an article that is either concerned in or that may afford evidence of the commission or suspected commission of an offence, either within South Africa or "elsewhere". This means that the offence linked to the article to be searched for or seized could have been committed or could be intended to be committed in any country. Section 20(c) does not state where the offence must be intended to be committed. From this deliberate omission, one may deduce that the offence should be intended to be committed only within South Africa.[175]

Attorneys v Lourens NO 2002 (1) SACR 152 (W)). She warns that there can be no doubt that surgical intervention as a method of obtaining evidence in the investigation of crime is a drastic step that may impact severely on the constitutionally protected rights of the individual. She concludes, however, by stating that this should not be seen as a deterrent to using the available statutory provisions in crime investigation, as society has a vested interest in the effective and comprehensive investigation of crime.

170 The test will be an objective one (*S v Boshoff* 1981 (1) SA 393 (T)). See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-7.

171 Joubert (ed) *Applied Law for Police Officials* 318.

172 For example, swallowed or flushed away, as in the case of drugs or uncut diamonds. Section 13(3)(b) of the South African Police Services Act states that where a law enforcement officer is authorised by law to use force, she may use "only the minimum force which is reasonable in the circumstances". Joubert (ed) *Applied Law for Police Officials* 318 and 319. See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-8.

173 *S v Boshoff* 1981 (1) SA 393 (T). The Court also held that a law enforcement officer who enters premises on the basis of section 25(3)(a) and (b) may not make use of reasonable force as provided for in section 27 of the Criminal Procedure Act. Kriegler, however, argues that this conclusion cannot be supported, as it is considered a *casus omissus* that entry in terms of section 25(1)(b)(i), (ii) and (iii) is not mentioned. See Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 49.

174 Joubert (ed) *Applied Law for Police Officials* 319.

175 Joubert (ed) *Applied Law for Police Officials* 307.

Section 21(1)(b) empowers a judge or judicial officer presiding over criminal proceedings to issue a search warrant for articles required in evidence at such proceedings without qualifying that such an article should specifically be in her area of jurisdiction. Sections 21(1)(a) and 25(1) stipulates that a magistrate or justice[176] may issue warrants within her specific area of jurisdiction. This becomes problematic in networked computing environments, in that multiple warrants may have to be obtained from different magistrates in different jurisdictions. It has been recommended that these jurisdictional requirements be updated to address the associated logistical problems that are not conducive to efficient law enforcement.[177]

Section 83(2) of the Electronic Communications and Transactions Act provides that where a cyber inspector requests a magistrate or a judge to issue a warrant in terms of section 83(1), such a magistrate or judge may issue a warrant where

(a) an offence has been committed within the Republic;

(b) the subject of an investigation is a South African citizen or ordinarily resident in South Africa;

(c) the subject of an investigation is present in South Africa at the time when the warrant is applied for; or

(d) information pertinent to the investigation is accessible from within the area of jurisdiction of the Court.[178]

Section 83(2) of the Electronic Communications and Transactions Act significantly broadens the jurisdictional requirements, as set out in section 25 of the Criminal Procedure Act, namely the restrictive territorial requirement that the offence has been committed or is being committed within the jurisdiction of the issuing magistrate.

---

176 The jurisdiction of commissioned officers in the SAPS includes the whole of the country. See Joubert (ed) *Applied Law for Police Officials* 309.

177 Watney 2003 *TSAR* 73. In this respect, also see paragraphs 5.2.3.4.3 and 6.2.3.5.2 below for a discussion of the multiple warrant requirements in the United States and England.

178 The information does not even need to be within the jurisdiction of the Court, but must merely be accessible from such jurisdiction. This approach will alleviate the problems identified in respect of the jurisdictional requirements contained in sections 21 and 25 of the Criminal Procedure Act (see Watney 2003 *TSAR* 71). It is interesting to note that one of the general provisions contained in chapter XIV of the Electronic Communications and Transactions Act is section 90, which deals with the jurisdiction of courts. Section 90 provides that a Court in the Republic trying an offence in terms of the Electronic Communications and Transactions Act has jurisdiction where the offence was committed in the Republic, where any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic; where the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or where the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed. Examples of other statutes which create extraordinary jurisdictions in respect of certain statutory offences include section 128(5) of the Correctional Services Act 111 of 1998, section 4(3) of the Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002, section 35 of the Prevention and Combating of Corrupt Activities Act 12 of 2004 and section 15 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004. See generally Du Toit *et al Commentary on the Criminal Procedure Act* 16-1 to 16-4C for a reference to jurisdiction in criminal matters.

4.2.4 Conditions and safeguards[179]

Some of the fundamental rights[180] that might come into play when performing searches and seizures include the right to dignity,[181] the right to freedom and security,[182] the right to privacy,[183] the right to freedom of expression,[184] the right not to be deprived of property,[185] the right to freedom of movement,[186] the right to administrative fairness,[187] and the rights of arrested, detained and accused persons, particularly the right against self-incrimination entrenched in the right to a fair trial.[188] The exclusionary rule[189] and the limitations[190] and interpretation[191] clauses are instrumental to making a constitutionally sound assessment.

Some of the most pertinent conditions and safeguards include the right to privacy, the requirement of reasonable grounds, the principle of proportionality, supervision by competent authorities, the protection of privileged data, the right against self-incrimination, safeguarding the legitimate interests of third parties, the consequences of unlawful actions by law enforcement, propriety and confidentiality. These conditions and safeguards are aimed at balancing the interests of law enforcement and respect for fundamental human rights in a search and seizure context. They are discussed below.

4.2.4.1 Right to privacy[192]

The basic human right to privacy is enshrined in section 14 of the Constitution, which includes

---

179 It is interesting to note that section 7(6) of the proposed Computer Misuse Bill specifically provides that, in seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in section 7(4) of the Computer Misuse Bill, whether by virtue of a search warrant or in terms of section 7(5) of the Computer Misuse Bill, a law enforcement officer must have due regard for the rights and interests of any person affected thereby to carry on her normal activities.

180 These relevant fundamental rights are also listed in paragraph 1.1 above. Rautenbach argues that although the right to national security embodied in section 198 of the Constitution is not listed as a fundamental right in the Bill of Rights, it is, in fact, a right of all citizens and should be treated as such. See Rautenbach 1999 *SAPL* 473-474. Van der Merwe points out that "'n Turksvy sal waarskynlik wees om the prosedurele maatreëls in ooreenstemming te hou met die Suid-Afrikaanse Grondwet" [It is likely to be a thorny matter to keep the procedural measures in line with the South African Constitution] (see Van der Merwe 1996 *THRHR* 237).

181 Section 10 of the Constitution. In *Fedics Group (Pty) Ltd v Matus* 1997 (9) BCLR 1199 (C) 1221C, the Court held that, although the search of the office of an employee infringed upon the employee's rights to dignity and privacy, there were reasonable grounds present to justify such infringements.

182 Section 12 of the Constitution.

183 Section 14 of the Constitution.

184 Section 16 of the Constitution.

185 Section 25 of the Constitution. Rautenbach, however, argues that section 25 of the Constitution is not concerned with the seizure of articles during police roadblocks. The "deprivation" of property is to be clearly distinguished from the narrower term "expropriation". "Deprivation" refers to taking away property (by expropriation or compulsory acquisition). Section 25(1) is concerned with the "beperking op eiendomsreg" [limitation of the right to property] rather than the "ontneming" [limitation] thereof. See Rautenbach 1999 *SAPL* 470. For an opinion that seizures do, in fact, have an impact on the right to property, see Itzikowitz 1995 *SAJHR* 281.

186 Section 21 of the Constitution.

187 Section 33(1) of the Constitution. In *Roman v Williams NO* 1997 (9) BCLR 1267 (K), it was held that the conduct of law enforcement officers must be justifiable in relation to the reasons given. The conduct must be suitable, necessary and proportional (1275F).

188 Section 35(3)(j) of the Constitution.

189 Section 35(5) of the Constitution.

190 Section 36 of the Constitution.

191 Section 39 of the Constitution.

192 See paragraphs 5.2.2 and 6.2.2 below for a discussion of the right to privacy within the legislative frameworks of the United States and England.

the right not to have one's person, home[193] or property[194] searched, possessions[195] seized or the privacy of one's communications[196] infringed. Although other areas of privacy warranting protection may emerge, legitimate expectations have crystallised in three spheres of privacy,[197] which coincide with the enumerated rights in section 14 of the Constitution, namely one relating to the body of a person, a second to a territorial or spatial aspect and the third occurring in the context of communication or information transfer.

A two-part test aimed at practically defining the "amorphous and elusive"[198] concept of privacy has been accepted by the courts. First, a person has to exhibit a subjective expectation of privacy. Second, it must be shown that this expectation is one that society is prepared to recognise as reasonable. Any claim to privacy is accordingly confined to aspects with regard to which a legitimate expectation of privacy can be harboured.[199] Such a legitimate expectation demands a subjective expectation of privacy which society recognises as objectively reasonable.[200] Legitimate expectation varies considerably, depending on the zone and nature of the privacy expectation and the activity that brings a person into contact with the State.[201] Whilst privacy is acknowledged in the truly personal realm, the scope of personal space shrinks as a person moves into communal relations and activities such as business and social interaction.[202] Also, within a particular sphere of privacy, the right to be left alone may have more than one facet.[203]

---

193 Section 14(a) of the Constitution. It is widely accepted that a person's home is subject to the highest expectation of privacy, reflecting the old adage that a person's home is her castle. See paragraph 1.1 above and Steytler *Constitutional Criminal Procedure* 99. As no definition of a private dwelling is given in the Criminal Procedure Act, Kriegler suggests that any premises where a person lives, however modest, falls within the definition (Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 46). A restricted interpretation of the term "home" would be contrary to the essential object of article 14, which is to protect the individual against arbitrary interference with her privacy. A person may therefore have a reasonable expectation of privacy in her workplace. The extent of its protection depends on the nature of the workplace and the object of the search (see *Mistry v Interim National Medical and Dental Council of South Africa* 1997 (7) BCLR 933 (D) and *Fedics Group (Pty) Ltd v Matus* 1997 (9) BCLR 1199 (C) 96). Also see Goodburn and Ngoye *Privacy and the Internet* 171-196 and Michalson *The Use of E-mail and the Internet in the Workplace* 193-226.

194 Section 14(b) of the Constitution. "Property" would include, as a minimum, movable property, either in the control of a person or over which she has ownership. The search of motor vehicles gives rise to particular circumstances which make inappropriate the standard approach to the protection of privacy. Such circumstances include the licensing requirement and the extensive regulation of vehicles that result in a significantly reduced expectation of privacy and the need for routine inspections of vehicles for roadworthiness. The general mobility of vehicles also most often presents exigent circumstances. Steytler *Constitutional Criminal Procedure* 101.

195 Section 14(c) of the Constitution.

196 Section 14(d) of the Constitution.

197 *Bernstein v Bester NO* 1996 4 BCLR 449 (CC) 89, *Protea Technology Ltd v Wainer* 1997 (9) BCLR 1225 (W) 12391. Also see Cachalia *et al Fundamental Rights in the New Constitution* 43-49 and Steytler *Constitutional Criminal Procedure* 83.

198 *Bernstein v Bester NO* 1996 (4) BCLR 449 (CC) 65.

199 *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271C-E.

200 *Protea Technology v Wainer* 1997 (9) BCLR 1225 (W) 1239H.

201 Steytler *Constitutional Criminal Procedure* 83.

202 *Bernstein v Bester NO* 1996 (4) BCLR 449 (CC) 661E.

203 Privacy of the home, for example, requires the State to refrain both from entering the home and from prescribing permissible conduct in the confines of a person's home, rendering article 14 of the Constitution very important in the review of the substantive content of specific offences. See, for example, *Case v Minister of Safety and Security: Curtis v Minister of Safety and Security* 1996 (5) BCLR 609 (CC), Aschke 1995 *SACJ* 109 and Steytler *Constitutional Criminal Procedure* 84. In *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division* 2003 (12) SACR 445 (CC) it was held that there is no right to privacy to commit an indecent act with a minor in the sanctum of a person's own home and, similarly, that there is no right to privacy to view child pornography. The Court noted that " ... since child pornography is frequently being imported via the Internet and possessed on computers, the ease with which such possessors may become distributors at the touch of a button, as it were, should be taken into account" (1359). The Court accordingly ruled that the limitation of both the rights to freedom of expression and the right to privacy is justifiable in the context of child pornography. See in this respect also

In terms of its nature and the duties imposed, the right to privacy appears capable of and suitable for horizontal application because it also binds private persons.[204] This is highly relevant in the area of criminal justice, because private persons play an important role in gathering information that is used in criminal trials.[205] A juristic person is also entitled to the right to privacy, to the extent required by the nature of that juristic person and the nature of the right.[206] There could, however, be a low or no legitimate expectation of privacy in documents which the law may require a company to keep.[207]

4.2.4.2 Reasonable grounds[208]

The various statutory provisions providing for the power to conduct searches and to seize articles repeatedly refers to reasonableness in their description of the circumstances in which these powers may be exercised.[209] Section 20 of the Criminal Procedure Act provides that certain articles may be seized if they are "on reasonable grounds believed to be" articles of a certain nature. Section 21(1)(a) authorises the issuing of search warrants where it appears from information on oath that there are "reasonable grounds for believing" that certain articles will be found at a certain place. Section 21(1)(b) of the Criminal Procedure Act, which grants a presiding judicial officer the power to issue a search warrant, makes no mention of the

---

Watney 2006 *THRHR* 227-237 and the follow-up to be published in volume 3 of the 2006 *THRHR* (which was kindly made available to the researcher by the author herself).

204 Steytler *Constitutional Criminal Procedure* 86. In line with the extensive common law protection of privacy in the private sphere, the High Court held that the constitutional right to privacy also binds private persons. See *Protea Technology Ltd v Wainer* 1997 (9) BCLR 1225 (W) 1238 and *Fedics Group (Pty) Ltd v Matus* 1997 (9) BCLR 1199 (C) 97. For a contrary view under the *interim* Constitution, see *Mistry v Interim Medical and Dental Council of South Africa* 1997 (7) BCLR 933 (D) 948C.

205 An example is *S v Botha* (1) 1995 (2) SACR 598 (W), where a public company (ESKOM) was responsible for the entire investigation (603c).

206 Article 8(4) of the Constitution. Steytler argues that the nature of the right to privacy can be extended to juristic persons, a principle recognised in comparative constitutional jurisprudence, as well as in South African common law. He also refers to the omission of the qualifying word "personal" in the *interim* Constitution, which indicates that juristic persons are not explicitly excluded from claiming the right to privacy (Steytler *Constitutional Criminal Procedure* 84). See also *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 460. In *Investigating Directorate: Serious Economic Offences v Huyndai Motors Distributors (Pty) Ltd* 2000 (2) SACR 349 (CC), the constitutionality of seizure in terms of section 29(5), read with sections 28(13) and (14) of the National Prosecuting Authority Act 32 of 1998, was considered. The Court held that although the provisions invaded the right to privacy, they were not unconstitutional. It was also held that the right to privacy was applicable, where appropriate, to a juristic person and that a search warrant would be granted under the said Act for the purposes of a preparatory investigation only if there is a reasonable suspicion that an offence, which might be a specified offence, has been or is being committed, or that an attempt was or had been made to commit such an offence. It follows that no warrant may be applied for or be issued in the absence of a reasonable suspicion that an offence has been committed. It is interesting to note that a search and seizure procedure under section 46 of the Competition Commission Act 89 of 1998 has been ruled tainted by an infringement of the right to privacy due to the fact that a television crew was invited to accompany the search team (see *Pretoria Portland Cement Co Ltd v The Competition Commission* [2002] JOL 9808 (A)).

207 *Bernstein v Bester NO* 1996 (4) BCLR 449 (CC) 85.

208 There are exceptions to the general rule that reasonable grounds are required for a search and seizure intervention. Criminal law is increasingly used to enforce social legislation, thereby seeking to regulate and control the activities of both natural and legal persons when they engage in public intercourse. Examples of provisions where reasonable grounds prior to a search are not required include searches near borders, searches on areas that are cordoned off, and searches at roadblocks and checkpoints (sections 13(6); 13(7) and 13(8) of the South African Police Service Act 68 of 1995). Steytler, however, submits that while the requirement of reasonable grounds for the search of individual premises may be abandoned, a particular area should only be cordoned off based on reasonable grounds. He also contends that the length, objectivity and intrusiveness of the search should be reasonably justifiable. See Steytler *Constitutional Criminal Procedure* 89, 91 and 95. This point of view is supported in Rautenbach 1999 *SAPL* 462. See paragraphs 5.2.3.3 and 6.2.3.4 below for a reference to the requirement of reasonable grounds in the United States and England.

209 Reasonableness is also consistently required in respect of the power to arrest persons. See sections 41 to 43, which empower certain persons to arrest persons "reasonably suspected" of having committed certain offences. Section 48 authorises the entry of premises where the person "reasonably suspects" that a certain state of affairs exists; and section 49 allows for such force as may be "reasonably necessary" to overcome resistance against an arrest or to prevent the arrested person from fleeing.

requirement of reasonable grounds, but this requirement is inherent in a judicial decision.[210] Section 25(1) authorises issuing search warrants where it appears that there are "reasonable grounds for believing" that a certain type of meeting is to be held or that an offence has been, is being or is likely to be committed. Sections 22(1)(b) and 25(3) empower a law enforcement officer to conduct a search if "on reasonable grounds [she] believes" that certain circumstances exist. Section 26 authorises the entry of premises where the person "reasonably suspects" that a certain state of affairs exists. Section 27 authorises the use of such force as may be "reasonably necessary" to gain entry to premises. Similarly, warrants issued under section 83 of the Electronic Communications and Transactions Act are subject to the reasonable grounds requirements contained in section 25 of the Criminal Procedure Act.

The requirement of reasonableness may be described as a requirement that there be reasonable grounds from which a certain inference can be drawn.[211] A person is only said to have "reasonable grounds" to believe or suspect that something or that certain action is necessary if

(a) the person really "believes" or "suspects" it;

(b) the person's belief or suspicion is based on certain "grounds" from which she has drawn an inference; and

(c) any reasonable person would have held the same belief or suspicion within the same circumstances and in view of the existence of those grounds.[212]

Any statute which permits a search warrant to be issued where there are no reasonable grounds for believing that an offence has been committed is in conflict with the Constitution and consequently invalid.[213] The existence of a belief based upon reasonable grounds prior to the search must relate to three issues:[214]

(a) that an offence has been committed;

(b) that the articles sought may afford evidence of the commission of that offence; and

(c) that the articles are likely to be on the premises that are to be searched.

---

210 Steytler *Constitutional Criminal Procedure* 87.

211 It can, for instance, only be said that force is "reasonably necessary" to achieve a certain goal if there are "reasonable grounds" to believe that such force is actually necessary to achieve the goal. A person can also only be said to have a "reasonable suspicion" that a certain state of affairs exists if she has "reasonable grounds" to believe that that state of affairs exists. See *"LSD" Ltd v Vachell* 1918 WLD 127 34.

212 Joubert (ed) *Criminal Procedure Handbook* 80.

213 *Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2000 (1) SACR 503 (T).

214 *Van Der Merwe v Minister van Justisie* 1995 (2) SACR 471 (O) 476d-e, *Mistry v Interim National Medical and Dental Council of South Africa* 1997 (7) BCLR 933 (D) 953H-I and *Mandela v Minister of Safety and Security* 1995 (2) SACR 397 (W) 400-404.

It has been held an insufficient standard to merely ask whether the articles are only possibly concerned with the offence.[215] On the other hand, the constitutional standard should not be as high as whether the article will be used as evidence. The appropriate test is that set by section 20(b) of the Criminal Procedure Act, namely that article may be seized "which may afford evidence of the commission or suspected commission of an offence".[216] Reasonable grounds do not amount to a belief that a criminal case has been made out, but that, reasonably, there are grounds for a belief that a person may have in her possession, or under her control, an article which can be of use in proving a criminal case.[217]

In court, a law enforcement officer has to show satisfactorily that she believed reasonable grounds to have existed, by stating the grounds upon which she formed the belief.[218] Whether the law enforcement officers' suspicion or belief was reasonable is an objective question and must be answered objectively on the basis of all the facts before the Court.[219] In respect of warrantless searches and seizures, the official executing such a search will have to show that the reasonable grounds existed at the time when she decided to act without a warrant.[220] The actions of the person conducting the search may be reviewed by a court of law on the merits of the case.[221]

Although the essence of reasonable grounds is that they must be objective[222] and reviewed by a court,[223] the requirement of reasonable belief does not appear always to need to measure up to an objective standard in South African law. The courts appear to distinguish between the reasonable belief formed by a magistrate or justice when issuing a search warrant[224] and that of a law enforcement officer acting without a search warrant.[225] When a magistrate or justice has issued the warrant, it has been held that reasonable grounds for believing are not grounds measuring up to an objective standard, but grounds which are reasonable in the subjective opinion of the magistrate.[226] The effect of this subjective standard is that a magistrate or

---

215 *Mandela v Minister of Safety and Security* 1995 (2) SACR 397 (W) 400-404.
216 Steytler *Constitutional Criminal Procedure* 87.
217 *Cine Films (Pty) Ltd v Commissioner of Police* 1971 (4) SA 574 (W). Also see Du Toit *et al Commentary on the Criminal Procedure Act* 2-3.
218 Joubert (ed) *Applied Law for Police Officials* 307.
219 *S v Mayekiso* 1996 (2) SACR 298 (C), *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D) and Du Toit *et al Commentary on the Criminal Procedure Act* 2-2A.
220 An example can be found in *Mbutuma v The MEC for Safety and Security of the Eastern Province* 1998 (1) SACR 367 (Tk), where it was held that where vehicles were seized in terms of section 22(b) of the Criminal Procedure Act after an inspection that revealed that the engine and chassis numbers were falsified, the fact that the numbers had been tampered with constituted grounds for a reasonable belief that the motor vehicle had been stolen and that such a vehicle afforded evidence of the commission or suspected commission of theft. Also see *Alex Cartage (Pty) Ltd v Minister of Transport* 1986 (2) SA 838 (E) and Du Toit *et al Commentary on the Criminal Procedure Act* 2-4 and 2-4A
221 Joubert (ed) *Criminal Procedure Handbook* 122.
222 Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 33.
223 *Highstead Entertainment (Pty) Ltd t/a "The Club" v Minister of Law and Order* 1994 1 SA 387 (C) 393A.
224 Section 21(1)(a) of the Criminal Procedure Act.
225 Section 22(b) of the Criminal Procedure Act.
226 *Control Magistrate, Durban v AZAPO* 1986 (3) SA 394 (A) 400F. In *Divisional Commissioner of SA Police, Witwatersrand Area v SA Associated Newspapers Ltd* 1966 (2) SA 503 (A), it was held that the merits of the decision by a justice of the peace that there are objective grounds upon which a warrant may be issued may not be contested in court (511G-H). This

justice's decision can only be reviewed on the narrow administrative grounds that she did not apply her mind properly to the facts[227] or acted improperly or *mala fide* and not on the merits. However, where a law enforcement officer acts without a warrant, the standard is objective,[228] with the onus of proof on the State.[229] In so far as this reasoning is based on the wording of the legislation, equating the phrase "if it appears to a magistrate" with a subjective discretion, it can no longer prevail under the Constitution, and the same standard of objective grounds should be applied in both instances.[230]

For the effective protection of privacy rights, the information on which reasonable grounds are based may not itself have been obtained in violation of section 14.[231] The information need not comply with the strict rules of evidence. Subject to a cautionary rule, hearsay evidence of traps, informers and anonymous tips may be relied on as a basis for a search.[232] While the identity of informers needs not be disclosed, information should be placed before the independent arbiter in terms of which the reliability of such hearsay evidence can be assessed. The word of a law enforcement officer cannot be a substitute for the decision of the issuing authority. Where the grounds are based on information which has been obtained both constitutionally and unconstitutionally, the search may nevertheless pass constitutional muster if the untainted information establishes reasonable grounds.[233]

4.2.4.3 Proportionality

At first glance, search and seizure seem to go against the spirit and content of at least some of the rights bestowed upon individuals by the Bill of Rights. However, in terms of the limitations clause,[234] these rights may be limited by law of general application, provided that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.[235] The limitations clause institutes a proportionality test, which requires

---

decision was quoted with approval in *Cresto Machines (Edms) Bpk v Die Afdeling Speuroffisier SA Polisie, Noord-Transvaal* 1972 (1) SA 376 (A) 396. Also see *Cine Films (Pty) Ltd v Commissioner of Police* 1971 (4) SA 574 (W) 581, *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D) 513 C-D, *Mandela v Minister of Safety and Security* 1995 (2) SACR 397 (W) 404h, *Van Der Merwe v Minister van Justisie* 1995 (2) SACR 471 (O) 476f and 477i and Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 38.

227 *Mandela v Minister of Safety and Security* 1995 (2) SACR 397 (W) 405.

228 *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D) 511D-E; 513D, *S v Boshoff* 1981 (1) SA 393 (T) 397F-H and *S v Mayekiso* 1996 (2) SACR 298 (C) 305*f*.

229 *S v Mayekiso* 1996 (2) SACR 298 (C) 305f.

230 Steytler *Constitutional Criminal Procedure* 89.

231 Steytler *Constitutional Criminal Procedure* 88.

232 Kriegler *Hiemstra Suid-Afrikaanse Strafproses* 38. If a law enforcement officer is of the opinion that hearsay evidence is true and correct, such hearsay evidence may be regarded as sufficient information for the purposes of section 21(1)(a) of the Criminal Procedure Act (*Van Der Merwe v Minister van Justisie* 1995 (2) SACR 471 (O) 482i). However, Joubert recommends that it is preferable for the law enforcement officer to confirm the information received from an informer or an anonymous person, before applying for the warrant on account thereof (Joubert (ed) *Applied Law for Police Officials* 308). Steytler argues that the test that, in applying for a warrant, the law enforcement officer must express in her affidavit only the opinion that the tendered hearsay evidence is true or correct is too low (Steytler *Constitutional Criminal Procedure* 87).

233 Steytler *Constitutional Criminal Procedure* 87.

234 Section 36 of the Constitution.

235 In *Park-Ross v Director: Office for Serious Economic Offences* 1995 (2) SA 148 (C), section 6 of the Investigation of Serious Economic Offences Act 117 of 1991, authorising search and seizure in pursuance of an enquiry under section 5 of the said Act, was held to violate the right to privacy protected by section 13 of the *interim* Constitution. It was specifically held that

taking into account all relevant factors and striking a reasonable and justifiable balance between them.[236] The relevant factors include the nature of the right, the importance of the purpose of the limitation, the nature and the extent of the limitation, the relation between the limitation and its purpose and whether less restrictive means could be deployed to achieve the same purpose. The listed considerations are not exhaustive and the courts are allowed to take other considerations into account as well. Section 36 of the Constitution is not intended to be a stringent and rigid clause, but allows the courts to develop a differentiated balancing test over time.[237]

A balance must be struck between, on the one hand, the vital interest of society to uphold and to protect human rights (particularly the rights of persons being investigated for, or accused of, or convicted of crime) and, on the other hand, the interests of society, which the state must protect from crime.[238] It is in essence a balancing act between crime control and due process. The way in which this is done in a search and seizure framework is by limiting law enforcement powers to search and seize, because unlimited or absolute powers to search and seize negate many of the human rights involved. At the same time, these fundamental rights are also limited by requiring of a citizen sometimes submitting herself to a search and the seizure of her property.[239] It stands to reason that the powers under section 19 to 36 of the Criminal Procedure Act should be exercised carefully, and only when necessary, as any abuse of these powers will not be countenanced by our courts. These powers must be interpreted restrictively and in favour of the individual.[240] The impact of a search and seizure upon the rights, responsibilities and legitimate interests of third parties must also be brought into the equation when the proportionality of a search and seizure intervention is assessed.[241]

4.2.4.4 Supervision by competent authorities[242]

Prior judicial authorisation is aimed at preventing unreasonable searches rather than at remedying unconstitutional breaches of privacy after the event. A person other than the official who requests a warrant to intrude upon an individual's privacy must make two judgement calls: first, to consider whether there are reasonable grounds for the intrusion, and second, even if

---

such a violation cannot be qualified as a reasonable and justifiable limitation of rights. The creation of the Office for Serious Economic Offences and the special powers of search and seizure given to the Office were considered necessary in the light of the serious dangers that white-collar crime poses to the economic wellbeing of the country. See Steytler *Constitutional Criminal Procedure* 87.

236 See *S v Makwanyane* 1995 (6) BCLR 665 (CC) 104 and *S v Coetzee* 1997 (4) BCLR 437 CC) 11.

237 Rautenbach & Malherbe *Constitutional Law* 313.

238 *S v Makwanyane* 1995 (6) BCLR 665 (CC) 249, *Ferreira v Levin NO* 1996 (1) BCLR 1 (CC) 152, *S v Melani* 1996 (2) BCLR 174 (E) 191H, *S v Nombewu* 1996 (12) BCLR 1635 (E) 1663F, *Key v Attorney-General Cape of Good Hope Provincial Division* 1996 (6) BCLR 788 (CC) 13 and *S v Desai* 1997 (1) SACR 38 (W) 42e-f.

239 Joubert (ed) *Applied Law for Police Officials* 306.

240 Du Toit *et al Commentary on the Criminal Procedure Act* 2-1.

241 See paragraph 4.2.4.7 in respect of the rights of third parties.

242 Exceptions to the general rule of prior authority are accepted in, for example, exigent circumstances (see section 22(b) and 25(3) of the Criminal Procedure Act). The South African Police Service Act 68 of 1995 also provides for various searches without a warrant (including sections 13(6); 13(7) and 13(8)). See paragraphs 5.2.3.3 and 6.2.3.3 below for a reference to the requirement of supervision by competent authorities in the United States and England.

such grounds exist, to determine whether the intrusion is justified under the circumstances.[243] The conflicting interests of the State and the individual must be assessed by an impartial, independent, detached and responsible arbiter to guard against unwarranted infringements of basic human rights.[244] Such an independent judicial officer, empowered with the discretion to decide whether or not there are reasonable grounds for a search, is positioned between the citizen and the law enforcement officer.[245]

As a general rule, a search should be authorised by a judicial officer, although it is not unambiguously required that the decision-maker should in all circumstances be a judicial officer.[246] If a law enforcement officer needs to obtain a search warrant and a magistrate is not available, a justice of the peace should be approached first, instead of conducting the search without a warrant. However, it is advisable to have a warrant issued by a commissioned law enforcement officer who is not directly involved in the case.[247] Where it is considered reasonable for members of the executive to issue warrants, both the objective and subjective impartiality and independence of the decision-maker have to be assessed.[248]

Steytler[249] argues that the principle that a decision-maker must be a neutral and detached person who is capable of acting judiciously is not fully adhered to in South African law, in that the power to issue a search warrant is extended to justices of the peace, including commissioned officers in the SAPS, South African National Defence Force or Correctional Services, Directors of Public Prosecutions and state advocates.[250] He reasons that where the person issuing the warrant is part of the office of the executing officer, then, objectively speaking, there is no neutral or detached officer.[251] It is interesting to note that section 83(1) of

---

243 Steytler *Constitutional Criminal Procedure* 91.

244 *SA Police v SA Associated Newspapers* 1966 (2) SA 503 (A).

245 Joubert (ed) *Criminal Procedure Handbook* 116. Also see *Park-Ross v Director: Office for Serious Economic Offences* 1995 (2) SA 148 (C) 172.

246 Sections 21(1) and 24 of the Criminal Procedure Act.

247 *S v Motloutsi* 1996 (1) SA 584 (CPD). Joubert argues that it is a fallacy that a warrant issued by a magistrate is "more legitimate" than one issued by a justice of the peace. She contends that it is always better to search with a search warrant than without one (Joubert (ed) *Applied Law for Police Officials* 308).

248 Steytler *Consitutional Criminal Procedure* 92.

249 Steytler *Constitutional Criminal Procedure* 91.

250 Section 21(1)(a) of the Criminal Procedure Act.

251 In *Park-Ross v Director: Office for Serious Economic Offences* 1995 (2) SA 148 (C), section 6 of the Investigation of Serious Economic Offences Act 117 of 1991, authorising search and seizure in pursuance of an enquiry under section 5 by the Investigating Director, was declared to be in violation of the right to privacy protected by section 13 of the *interim* Constitution. It could also not be saved by the limitations clause in section 33(1) of the Constitution. It was accordingly recommended that section 6 provides that, prior to the search and seizure, authority be obtained from a magistrate or judge of the Supreme Court in chambers and that such an application should set out, at least, under oath or a firm declaration, information such as the nature of the enquiry and suspicions giving rise to such enquiry. The Court, exercising its powers in terms of section 98(5) of the *interim* Constitution, required Parliament to correct the defects in section 6 in accordance with the Court's recommendations. Du Toit *et al Commentary on the Criminal Procedure Act* 2-2B. Also see *Minister of Justice v Desai* 1948 (3) SA 395 (A) 405, where it was said that the investigating officer in a case should not issue the warrant. Although Steytler supports the suggestion by Tebbutt J in *Park-Ross v Director: Office for Serious Economic Offences* that a warrant in terms of the said Act should have been issued by a magistrate or judge, he adds that it may be impractical in South Africa to extend this principle to all cases. Steytler asks whether it is not constitutionally objectionable that members of the executive are granted the power to search and seize where the person issuing the warrant is part of the office of the executing officer. Steytler also levels criticism against area searches, authorised by the National or Provincial Commissioner of Police in terms of section 13(7) of the South African Police Service Act 68 of 1995. Even though, as *per* section 15(1)(a) of the said Act, this power may not be delegated, Steytler suggests that there may be inadequate safeguards to secure the necessary balance

the Electronic Communications and Transactions Act empowers only magistrates and judges to issue warrants to cyber inspectors.

Even where all the statutory requirements for a warrant are met, including reasonable grounds, the issuing authority should have a constitutionally protected residual discretion to apply a proportionality test. This underpins the issuing authority's independence and impartiality in that the judicial officer may not act as a mere "rubber stamp".[252] This principle is also contained in section 25 of the Criminal Procedure Act. It states that a magistrate or a justice may issue a warrant if it appears to her that reasonable grounds mentioned in section 25(1) exist. Although there is no specific reference in section 21 to such a residual discretion, it would be consistent with the judicial discretion which a magistrate or a justice should exercise.[253]

The protection against unreasonable invasions of privacy is fortified if the issuing authority's decision is also subject to review.[254] In the light of the constitutionalisation of the right to privacy, there can no longer be a presumption of the reasonable exercise of discretion. On the contrary, the onus is on the party that has intruded or authorised the intrusion.[255]

4.2.4.5 Privileged data[256]

Information that is privileged and in respect of which the holder of the privilege[257] has not yet relinquished her privilege may not be seized by the State. This requirement becomes very

---

between the rights of citizens and law enforcement concerns, given the broad purpose of such a search. He argues that there are not sufficient reasons to abandon the principle that an impartial and independent person should be the final arbiter before such a drastic measure is taken. The National Commissioner or a Provincial Commissioner, although she may be of the highest rank in the Police Service, is not detached from the search. This makes it difficult to bring an independent discretion to bear on the matter. In view of the serious inroads on the right to privacy, it is submitted that a judicial officer would be a more suitable person to make the decision whether the public order or safety has been disturbed or threatened and whether the search to be conducted will assist in remedying the situation. Since the decision to cordon off is not made on the spot, the objectives of the search will not be defeated by obtaining such prior judicial authorisation. See Steytler *Consitutional Criminal Procedure* 91, 92 and 95. See also LaFave and Israel *Criminal Procedure* (2nd ed) 156, who argue for a clear rule that only judicial officers should be entitled to issue search warrants.

252 With reference to the issuing of a warrant for the interrogation of a witness in terms of section 205 of the Criminal Procedure Act, it was held in *S v Cornelissen; Cornelissen v Zeelie NO* 1994 (2) SACR 41 (W) that where the jurisdictional facts exist, the magistrate nevertheless has the discretion to refuse to issue a warrant where a person's right to privacy outweighs the interests of justice. Moreover, the judge commented that this decision is the most important aspect of the discretion (69i). Also see *R v Parker* 1966 (2) SA 56 (RA) 58.

253 Steytler *Constitutional Criminal Procedure* 92.

254 However, South African law has in the past precluded effective review. The presumption of the reasonable exercise of a discretion presupposed that an act is conducted in a correct way until the contrary is proved (*S v Cornelissen; Cornelissen v Zeelie NO* 1994 (2) SACR 41 (W) 72d). If there was no specific claim of improper conduct, it is not incumbent on the magistrate to answer any allegation (*SA Police v SA Associated Newspapers* 1966 (2) SA 503 (A)). Where the legality of a warrant is disputed, the appropriate remedy would be an application to the High Court for review (*Matison v Additional Magistrate, Cape Town* 1980 (2) SA 619 (C) 627F-H; *S v Matison* 1981 (3) SA 302 (A) 313B-F). The onus here would rest on the applicant to prove, on a balance of probabilities, that the magistrate or justice who issued the warrant has acted improperly with regard to any of the limited powers of review (*Control Magistrate, Durban v AZAPO* 1986 (3) SA 394 (A); *Van Der Merwe v Minister van Justisie* 1995 (2) SACR 471 (O) 478j-479a; *National Transport Commission v Chetty's Motor Transport (Pty) Ltd* 1972 (3) SA 726 (A) 735G). As a result, the reasonableness of the issuing authority's decision was effectively placed beyond review, save in exceptional circumstances. See Steytler *Constitutional Criminal Procedure* 93.

255 In *S v Naidoo* 1998 (1) BCLR 46 (D), the High Court held that, as a trial court, it had the power to pronounce on the validity of a direction issued in terms of the Interception and Monitoring Prohibition Act 127 of 1992 (at 871-J). It also held that, since any intrusion on a constitutionally protected sphere of privacy is *prima facie* unconstitutional, the onus is on the issuing authority to justify the authorised search.

256 See paragraphs 5.2.3.4.5 and 6.2.3.5.3 below for a reference to the "search and sift" powers applicable to legally privileged material in the United States and England.

complex in computing environments where legally privileged data are often commingled with vast amounts of other so-called unprotected data, which law enforcement may indeed lawfully access. Instances where information is considered legally protected are referred to below.

4.2.4.5.1 Spousal privilege

A spouse is entitled to refuse to disclose communications from her spouse made during the marriage.[258] These communications are considered privileged. If, for example, it is in a written or stored electronic format, it cannot be seized by the State. The privilege persists after divorce with regard to communications between the couple while the couple were still married.[259] The husband or wife is, however, competent and compellable to give evidence for the prosecution at proceedings where the accused is charged with certain specified offences.[260]

In terms of section 199 of the Criminal Procedure Act, each spouse may refuse to answer a question or to disclose material that the other spouse could not have been compelled to answer or disclose. This privilege can only be claimed by the spouse to whom the communication is made. If the spouse who received the communication wishes to disclose its content, the spouse who sent the communication cannot prevent such a disclosure.[261] A third person who hears or intercepts the communication cannot be prevented from disclosing it.[262]

4.2.4.5.2 Legal professional privilege

Under paragraph 3.2 of the South African Police Service Search and Seizure National Instruction,[263] the only exception to the general rule that any article "that is in some way

---

257 Privileges relating to particular witnesses are found in, *inter alia*, section 195 in respect of spouses; section 197, which covers the privileges of the accused when giving evidence; section 198, which covers privileges arising out of the marital state; section 201, which deals with the privilege of a legal practitioner; and section 202, which deals with privilege from disclosure on the grounds of public policy or interest. See in general sections 192 to 207 of the Criminal Procedure Act, which are concerned with the competence, compellability and privileges of witnesses.

258 Section 198 of the Criminal Procedure Act. Section 195(2) of the Criminal Procedure Act provides that for the purposes of the law of evidence in criminal proceedings, the term "marriage" includes a customary marriage or customary union concluded under indigenous law and the customs of any of the indigenous peoples of the Republic of South Africa or any marriage concluded under any system of religious law.

259 Section 198(2) of the Criminal Procedure Act. Widows and widowers cannot claim this privilege (see Schwikkard and Van der Merwe *Principles of Evidence* 142).

260 These offences are stipulated in section 195(1)(a)-(i) of the Criminal Procedure Act. They include the following offences: any offence committed against the person of either of them or of a child of either of them; any offence under Chapter 8 of the Child Care Act 74 of 1983 committed in respect of any child of either of them; any contravention of any provision of section 31(1) of the Maintenance Act 99 of 1998, or of such a provision as applied by any other law; incest; abduction; any contravention of any provision of sections 2, 8, 9, 10, 11, 12, 12A, 13, 17 or 20 of the Sexual Offences Act 23 of 1957; and perjury committed in connection with or for the purpose of any judicial proceedings instituted or to be instituted or contemplated by one of them against the other, or in connection with or for the purpose of criminal proceedings with regard to any offence included in this subsection.

261 Schwikkard and Van der Merwe *Principles of Evidence* 142.

262 Zeffertt, Paizes and Skeen *The South African Law of Evidence* 620.

263 South African Police Service *National Instruction 2/2002: Search and Seizure* 3. It is interesting to note that section 3(7) of the proposed amendments to the then operative Interception and Monitoring Prohibition Act 127 of 1992 specifically provides the following: "No communication between a legal representative and his or her client may be intercepted or monitored, except if on reliable information, the judge is satisfied that such a legal representative is involved in, or aiding or abetting a serious offence" (see the South African Law Reform Commission *Discussion Paper 78 on the Interception and Monitoring Prohibition Act* 127). No such explicit similar provision is made in respect of the search and seizure, production or preservation of legally privileged (electronic) evidence. Section 29(11) of the National Prosecuting Authority Act 32 of 1998, however, affords a person being searched a right to object to the inspection or removal of any item found on the premises on

connected to an offence" may be seized relates to legally privileged material. It provides that documents exchanged between a legal representative and her client or prepared by the client for her legal representative may not be seized. Section 201 of the Criminal Procedure Act governs the legal professional privilege in criminal proceedings in so far as it concerns the competence of a legal practitioner[264] to testify against any person by whom such a legal practitioner is professionally employed or consulted without the consent of such a person. The law in this regard is the English law as it was on 30 May 1961.

If, however, a fact, matter or thing came to the knowledge of a legal practitioner before she was professionally employed or consulted with reference to the defence of the person concerned, the situation is different. A legal practitioner is competent and compellable to give evidence as to any such fact, matter or thing which relates to or is connected with the commission of any offence with which the person by whom such a legal practitioner is professionally employed or consulted, is charged.

Since legal privilege is a substantive rule of law and not merely a rule of evidence, the public interest demands that no inroads should be made on legal privilege, whether in the course of court proceedings of a judicial or quasi-judicial nature, or in proceedings falling outside the ambit of this description. If the State had the power to seize such information, the whole object of the privilege would be defeated.[265] Legal professional privilege is a right necessary for the proper functioning of the adversary system and is therefore a fundamental right which can be claimed not only in actual litigation, but also to prevent seizure by warrant.[266]

---

the ground that it is privileged. The section provides that, in the face of such a claim, the person executing the warrant must request the Registrar of the High Court to seize and remove the item and keep it until a court has ruled on the issue of privilege. In *Zuma v NDPP* [2006] JOL 16755 (D) 36-43 the Court stated that an application for a search warrant to undertake a search of the offices of an attorney to obtain evidence against his accused client is a "drastic step – in fact a step which ... was without precedent in this country". The Court argued that special steps should have been taken to prevent "a blunder that might have jeopardised the prosecution, let alone to avoid undue infringement of the applicant's' right to confidential communication and privacy". The Court added that "in a prosecution for an offence such as money-laundering 'financial records' may well comprise, or contain, 'privileged material". Lastly the Court ruled that constitutional considerations have superseded the considerations which led the Appellate Division in, *inter alia*, *Cine Films v Commissioner of Police* 1972 (2) SA 254 (A) 268 to hold that the offending portions of a warrant could be severed from the acceptable portions, A submission that the warrants can be saved by pruning them down to acceptable limits *ex post facto* cannot be sustained.

264 Qualified to practise in any court, whether within South Africa or elsewhere (section 201 of the Criminal Procedure Act).

265 The correctness of *Andresen v Minister of Justice* 1954 (2) SA 473 (W), which endorsed the search and seizure trump of legal professional privilege, has been debated over several decades (in support of this viewpoint, also see *Prinsloo v Newman* 1975 (1) SA 481 (A) 493F-G and *Mandela v Minister of Prisons* 1983 (1) SA 938 (A)). In *H Heiman, Maasdorp & Barker v Secretary for Inland Revenue* 1968 (4) SA 160 (W), *Cheadle, Thompson & Haysom v Minister of Law and Order* 1986 (2) SA 279 (W) and *Sasol III (Edms) Bpk v Minister van Wet en Orde* 1991 (3) SA 766 (T), strong arguments to the contrary were advanced. In *S v Safatsa* 1988 (1) SA 868 (A), it was decided that legal professional privilege is more than a mere rule of evidence, as it encapsulates the fundamental right to consult freely with a legal advisor prior to, as well as in and out of, court. The Court held that any claim to a relaxation of the legal professional privilege must be approached with the greatest circumspection. In *Blue Chip Consultants (Pty) Ltd v Shamrock* 2002 (3) SA 231 (W), the Court reasoned that the necessary trust between the legal advisor and the client could only be achieved if inroads upon the privilege were "confined to clear cases of greater competing interests" (235 I-J).

266 See *Mohamed v President of the Republic of South Africa* 2001 (2) SA 1145 (C) 453C-D. In *Bogoshi v Van Vuuren NO; Bogoshi v Director, Office for Serious Economic Offences* 1993 (2) SACR 98 (T), it was held that section 6 of the Investigation of Serious Economic Offences Act 117 of 1991 also does not trump legal professional privilege. On appeal, the Court held that it "could safely be assumed that, because of the fundamental nature of the rule, those documents in the files which were privileged would normally be protected from seizure under section 6 of that Act" (793D-E). In the opinion of the Court *a quo*, no inroads into the right of privilege would be made if the document was sealed in the presence of the person claiming the privilege and was then delivered to a neutral person (such as the Registrar of the Supreme Court), who would hold it until the

The requirements that have traditionally been laid down for a successful claim of legal professional privilege are that

(a) the legal adviser must have been acting in her professional capacity;

(b) she must have been consulted in confidence;

(c) the communications must have been made for the purposes of obtaining legal advice; and

(d) the advice may not facilitate the commission of a crime or fraud.

The increased stature of the privilege as a constitutional right may cause courts to be less prepared to hold that the privilege is lost as easily as the common law would seem to allow.[267] As the privilege belongs solely to the client, it is only the client who may waive the privilege.

Subject to the Constitution, there is no inherent power in a court to override a legitimate claim of privilege.[268] There is, however, a judicial discretion to exclude technically admissible evidence on the grounds that its reception would operate unfairly against the accused.[269] A court has an inherent power to examine any document in respect of which privilege is claimed. This inherent power of the court does not impinge upon the freedom of communication between legal advisors and their clients, but is merely a procedural step to determine whether the party claiming privilege was justified in raising the objection against discovery.[270] The test that should be employed in determining when a court should exercise this power is whether there are special circumstances present, in the sense that the legally privileged material is necessary and desirable for a just decision, or whether there is some reason to cast doubt on the claiming of the privilege.[271] The court has the power to excise from an otherwise privileged document

---

question of privilege had been resolved (also see *H Heiman, Maasdorp, & Barker v Secretary for Inland Revenue* 1968 (4) SA 160 (W)). In *Smit and Maritz Attorneys v Lourens NO* 2002 (1) SACR 152 (W), it was held that although there was no evidence that the documents seized from the attorneys contained privileged information, they could be safely assumed to have contained privileged information. In the light of the prior offer of cooperation by the attorney, the documents should not have been seized without notice. As a result, the seizure of the documentation was accordingly set aside. See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-4, 2-8. In *Mahomed v National Director of Public Prosecutions* 2006 (1) SA 127 (W) 129 law enforcement officers seized a number of documents, files and a laptop computer from the applicant's offices and residence. The applicant had occasionally acted as the former deputy-president's attorney and brought an urgent application to the court to set aside the warrants and to release her possessions. The application was based, *inter alia*, on the fact that the respondents failed to alert the Judge in chambers to the potential violation of attorney-client privilege and so obtained a warrant in the widest terms possible. The Court held this to be a material non-disclosure which had the effect of steering the Judge away from any concerns over a breach of attorney-client privilege. The application to set aside the warrants, the Court held, had to succeed on this ground alone. The Court also ordered (already at the first hearing of this application, before having ruled on the application) that the applicant's laptop computer be returned to her "after a mirror image of the hard drive was made".

267 Du Toit *et al Commentary on the Criminal Procedure Act* 23-36E, 23-37 and 23-38.

268 *S v Mpetha* (1) 1982 (2) SA 253 (C) 259.

269 *S v Forbes* 1970 (2) SA 594 (C).

270 See *Mohamed v President of the Republic of South Africa* 2001 (2) SA 1145 (C) 1151A-B, *South African Rugby Football Union v President of the Republic of South Africa* 1998 (4) SA 296 (T) and *Lenz Township Co (Pty) Ltd v Munnick* 1959 (4) SA 567 (T) 574.

271 Du Toit *et al Commentary on the Criminal Procedure Act* 23-36E.

portions which are not covered by the privilege. This power should be sparingly exercised so as not to dilute the protection afforded by the privilege.[272]

Where a law enforcement officer purporting to act in terms of a warrant issued under section 21 seizes a document compiled by attorneys from notes of a consultation with a prospective witness, the warrant must be restrictively interpreted. The law enforcement officer should also afford the attorney of the client an opportunity to have the warrant set aside prior to the seizure of such documents.[273] However, the seizure of legally privileged material would not *per se* lead to the staying of criminal proceedings, as it is only at the end of the case that the Court would be in a position to make a proper decision as to whether any prejudice had been caused to the holder of the privilege by the seizure of the material.[274]

4.2.4.5.3 Other professional privileges

Professional privilege is confined to legal advisers. There is no such privilege, for example, for journalists,[275] insurers,[276] members of the clergy,[277] or doctors.[278] The post-constitutional position may be that, in protecting the right to privacy, the courts would hold that the privilege

---

272 *Mohamed v President of the Republic of South Africa* 2001 (2) SA 1145 (C) 1159I-J.

273 *Cheadle, Thompson & Haysom v Minister of Law and Order* 1986 (2) SA 279 (W).

274 In *S v Du Toit* 2004 (1) SACR 341 (T), law enforcement officers had seized a privileged document in the possession of the accused with the knowledge that the document was privileged. The accused claimed that their constitutional rights had been irreparably violated and that they could not receive a fair trial. Accordingly, the accused applied for an order staying the proceedings against them. The application was unsuccessful. The prosecuting authorities undertook not to use the document during the trial in any way. The defence alleged that, because of the statements, the police had altered or supplemented existing statements or even obtained new statements to replace previous statements, but the Court held that it would be premature at that early stage to decide whether the procurement of the privileged statement had brought about that result. The Court held that that could only be done after the relevant witnesses had testified and been subjected to cross-examination. As a result, judgment on the application would only be given at the end of the case when a proper decision could be made about the credibility of the witnesses and whether any prejudice had been caused to the accused by the seizure of the privileged document. The Court confirmed, in any event, that the seizure of such a document would not *per se* lead to the staying of proceedings. In *Klein v Attorney-General, Witwatersrand Local Division* 1995 (2) SACR 210 (W), the applicant's privilege, as well as the applicant's fundamental constitutional right to privacy in terms of section 13 of the *interim* Constitution had been violated (see also *S v M* 2000 (2) SACR 474 (N)). It was held that the nature and the degree of this violation was not such as to warrant a stay of the ensuing criminal trial, despite the fact that the content of the privileged material had come to the attention of the then Attorney-General, since the prejudice suffered by the applicant (the accused in the subsequent criminal trial) was slight and the Attorney-General had undertaken not to use any of the privileged material during the course of the trial. In *Harksen v Attorney-General of the Province of the Cape of Good Hope* 1998 (2) SACR 681 (C), the applicant's claim for the permanent staying of an inquiry in terms of section 10(1) of the Extradition Act 67 of 1962 was dismissed on the ground that the breach of privilege was insufficiently serious, and that it had not been established that the applicant would be prejudiced, if at all, to such an extent as to warrant such a radical measure. What particularly swayed the Court was that the material could not be used in evidence and that there was a vast amount of material before the Court, not protected by privilege, and much information was known to the prosecution from its own investigations. See generally Du Toit *et al Commentary on the Criminal Procedure Act* 23-39.

275 In *S v Pogrund* 1961 (3) SA 868 (T) it was held that a journalist's plea that professional ethics prevented him from disclosing his sources in respect of any alleged offence was not a just excuse. Although it was reiterated in *S v Cornelissen; Cornelissen v Zeelie NO* 1994 (2) SACR 41 (W) that there was no legal privilege in terms of which journalists had immunity from the compulsory giving of evidence on information which they had obtained in the course of their work, it was also held that a refusal by a journalist to disclose sources may amount, depending on the circumstances, to a just excuse. *In casu,* it was not a proven necessity for the welfare of the community that the information be specifically required from the appellant. The Court concluded that the potential public advantage to be gained from subjecting the journalist to such questioning was outweighed by the potential public prejudice such a step would cause. In *Munusamy v Hefer NO* 2004 (5) BCLR 508 (O), it was decided that there is no rule which exempts a journalist from complying with a witness subpoena by reason of a supposed constitutional protection relating to confidential sources, nor is there any rule that gives a journalist *qua* journalist the right to be called as a witness of last resort.

276 *Howe v Mabuya* 1961 (2) SA 635 (D) 636A.

277 *Smit v Van Niekerk NO* 1976 (4) SA 293 (A).

278 *Botha v Botha* 1972 (2) SA 559 (N). In *Davis v Additional Magistrate Johannesburg* 1989 (4) SA 299 (W), it was held that whilst there was no recognised privilege in respect of the confidential communications between a doctor concerning or obtained from his patient, the confidential relationship between doctor and patient had to yield to wider considerations of public interest (303H-I).

should be extended to other professions on a case-by-case basis.[279] If the existence of a general discretion to exclude technically admissible evidence is upheld by the courts, this will be a fertile area for its application.[280] However, such an extended privilege may be denied if the State is able to establish that the requirements of the limitations clause have been met.[281]

4.2.4.6 Right against self-incrimination

The privilege against self-incrimination not only enjoys constitutional protection, but constitutes part of our common law. It is also reflected in a number of statutory provisions.[282] The application of the privilege to the accused and to witnesses in criminal proceedings is considered below.

At common law it is well recognised that a person should not be compelled to incriminate herself.[283] There are a number of provisions in section 35 of the Constitution which are directed at securing the privilege against self-incrimination.[284] However, the distinction made between arrested, detained and accused persons in section 35 gives rise to some anomalies regarding the application of these provisions.[285] This distinction also gives rise to some uncertainty regarding the application of the privilege against self-incrimination. The privilege against self-incrimination is only specified in relation to the accused's right to a fair trial.[286] The right to a fair trial, however, does not begin in the Court, but at the inception of the criminal process.[287]

---

279 See, for example, Zeffertt, Paizes and Skeen *The South African Law of Evidence* 589 and Du Toit *et al Commentary on the Criminal Procedure Act* 23-51.

280 Du Toit *et al Commentary on the Criminal Procedure Act* 23-39.

281 Schwikkard and Van der Merwe *Principles of Evidence* 141.

282 See, for example, sections 203, 217 and 219A of the Criminal Procedure Act.

283 The pre-constitutional nature and scope of the privilege were considered in *Magmoed v Janse van Rensburg* 1993 (1) SACR 67 (A). It was held that the privilege could be described as a "personal right to refuse to disclose admissible evidence" (104b). The privilege is that of the witness and has to be claimed by her (104c). See also *S v Sheehama* 1991 (2) SA 860 (A).

284 Sections 35(1)(a)-(c), section 35(2)(b)-(c) and 35(3)(f)-(i) of the Constitution. The interrelatedness of the presumption of innocence and the right to silence is apparent in section 35(3)(h). It was explored in *S v Zuma* 1995 (4) BLCR 401 (SA). In *S v Nombewu* 1996 (2) SACR 396 (E), it was held that the overriding objective of the equivalent provisions in the *interim* Constitution was "to protect persons against unfairly made self-incriminating statements" (403c).

285 See Schwikkard 1997 *SAJHR* 446.

286 Section 35(3)(j) of the Constitution. An accused can remain silent even if her answers would not be self-incriminating. This applies to the pre-trial stage (i.e. the investigative or police phase, as well as the pleading phase), the trial phase and also the sentencing stage (*S v Dzukuda* 2000 (2) SACR 443 (CC)). In *Park-Ross v Director: Office for Serious Economic Offences* 1995 (1) SASV 530 (K), the Court held that the right against self-incrimination does not extend to persons who are not arrested, detained or accused. In *Ferreira v Levin NO and Vryenhoek v Powell NO* 1996 (1) BCLR (CC), the Constitutional Court, with reference to section 25(3)(d) of the *interim* Constitution, adopted the view that the right against self-incrimination only applies to accused persons. It was held that no general right against self-incrimination is to be found in the *interim* Constitution and that the common law privilege against self-incrimination is excluded from constitutional protection (159, 195, 203, 247). Ackermann J held a dissenting view and contended that the privilege against self-incrimination was a residual right of a broadly defined right to freedom.

287 Rautenbach points out that the decision in *Park-Ross v Director for Serious Economic Offences* 1995 (1) SASV 530 (K) is in contrast to the common law position as set out in, for example, *R v Camane* 1925 (AC) 510 575 and *S v Kumalo* 1992 (2) SASV 411 (N) (Rautenbach 1999 *SAPL* 472). See also generally *S v Mpetha* (2) 1983 (1) SA 576 (C); *S v Lwane* 1966 (2) SA 433 (A); *R v Kuzwayo* 1949 (3) SA 761 (A); *S v Dlamini* 1973 (1) SA 144 (A); *S v Agnew* 1996 (2) SACR 535 (C); *S v Mathebula* 1997 (1) SACR 10 (W) 19f-20a; *S v Sebejan* 1997 (1) SACR 626 (W); *S v Khan* 1997 (2) SACR 611 (SCA); *S v Melani* 1996 (1) SACR 335 (E) 348i-349a.

Although a witness's common law privilege against self-incrimination receives no constitutional protection, an accused's right against self-incrimination cannot be circumvented by compelled testimony prior to the trial.[288] If evidence is obtained in breach of the privilege against self-incrimination, it is generally inadmissible.[289]

The critical question, when self-incriminating evidence is tendered by the prosecution in a criminal trial, is whether or not such evidence was compelled in prior (including non-criminal) proceedings. Where a respondent, for example, points out and discloses information in terms of an Anton Pillar order,[290] such information is not admissible in subsequent criminal proceedings, because the necessary element of voluntariness was absent.[291] Excluded from the ambit of the rule is a situation where an accused makes a voluntary statement to law enforcement officials.[292]

Although the ascertainment of bodily features in terms of section 37 of the Criminal Procedure Act may incriminate an accused, it is not generally considered to be in conflict with the privilege against self-incrimination or any other constitutional right.[293] Bodily features can become relevant in a biometrics context.[294]

---

288 In *Ferreira v Levin NO and Vryenhoek v Powell NO* 1996 (1) BCLR 1 (CC), the constitutional validity of section 417(2)(b) of the Companies Act 61 of 1973 (which requires an examinee to answer, under pain of fine or imprisonment or both, any question put to her notwithstanding that any answer to any such question might be used in evidence against her in subsequent criminal proceedings) was examined. The Court held that section 417(2)(b) of the Companies Act 61 of 1973 infringed the rule against self-incrimination (1090B). The rule against self-incrimination was "not simply a rule of evidence", but a right which, by virtue of the provisions of section 25(3) of the *interim* Constitution was, as far as an accused person was concerned, entitled to the status of a constitutional right (159). The right against self-incrimination was inextricably linked to the right of an accused to a fair trial and it existed to protect that right. If that right was not threatened, the rule had no application, which explained why a person who had been indemnified against prosecution or a person who had been convicted of a crime and was subsequently called to give evidence against a co-conspirator would not be entitled to claim the privilege in respect of evidence covered by the indemnity or the conviction. The Court's ruling that evidence given by an examinee at an enquiry held under section 417(2) of the Companies Act 61 of 1973 could not be used against her if she was subsequently prosecuted flows from this connection between the privilege and the right to a fair trial (now contained in section 35(5) of the Constitution). This line of reasoning was also followed in *Parbhoo v Getz NO* 1997 (4) SA 1095 (CC) and in *Mitchell v Hodes NNO* 2003 (1) SACR 524 (C).

289 Section 35(5) of the Constitution. See also *S v Lottering* 1999 (12) BCLR 1478 (N) and *S v Seseane* 2000 (2) SACR 225 (O).

290 See footnote 564 in paragraph 4.6 below for a reference to Anton Pillar orders.

291 See *Dabelstein v Hildebrandt* 1996 (3) SA 42 (C) 66H-I. One of the questions considered in this case was the test which our courts should apply in deciding whether to provide in Anton Pillar orders for an obligation on the part of the respondent to point out and disclose documents and other objects falling within a certain description. The test, in view of the privilege against self-incrimination, was whether there was a real and appreciable risk of criminal proceedings being taken against the respondent relating to any of the matters dealt with in the founding affidavit if the respondent complied with the order given (66E-F). The Court held that a statement made under compulsion, whether judicial or otherwise, will not be admissible against the person who made the statement, because of the provisions of section 25(3) of the *interim* Constitution, which gives all accused persons the right to a fair trial. The admissibility of any derivative evidence (evidence indirectly obtained by reason of a fact or document discovered as a result of a disclosure made by a respondent) fell to be determined by the exercise of a judicial discretion. The Court is obliged to exclude such evidence if this is necessary to ensure a fair trial. Steytler argues that any legislative instruction that evidence so obtained is admissible at subsequent proceedings will meet the same fate as section 417(2)(*b*) of the Companies Act 61 of 1973 (Steytler *Constitutional Criminal Procedure* 337). In this respect, he refers to examples of other such statutes that authorise inquiries against juridical persons and which specifically exclude a witness' common law privilege against self-incrimination (see, for example, sections 28 and 28*bis* of the Insurance Act 27 of 1943; sections 3, 4, 6, 8 and 9(1)(*b*) of the Inspection of Financial Institutions Act 38 of 1984; section 65 of the Insolvency Act 24 of 1936; section 66(1) of the Close Corporations Act 69 of 1984 and sections 7, 9, and 17 of the Maintenance and Promotion of Competition Act 96 of 1979).

292 *S v Schoor* 1993 (1) SACR 202 (E).

293 In *S v Huma* 1995 (2) SACR 411 (W), the accused objected to his fingerprints' being taken during the course of the trial, *inter alia*, on the basis that it would infringe the privilege against self-incrimination as contained in section 25(3)(c) of the *interim* Constitution. The Court found it unnecessary to invoke the limitations clause. It was held that taking fingerprints did not constitute testimonial evidence by the accused and was therefore not in conflict with the privilege against self-incrimination. In *Levack v The Regional Magistrate, Wynberg* 1999 (2) SACR 151 (C), in adopting a purposive approach to the interpretation of

Where a witness retains the common law privilege against self-incrimination, the privilege may be waived. When such evidence is then later tendered at a criminal trial, the question is whether the waiver met the constitutional standard of voluntariness, knowledge and intelligence.[295] Witnesses should be aware of their right to refuse to answer questions which may incriminate them at subsequent criminal proceedings.[296] Where a witness is aware (or is assumed to be aware) of the privilege, no duty to inform such a witness of the right against self-incrimination arises.[297]

In terms of section 203 of the Criminal Procedure Act, a witness may refuse to answer a question if it would expose her to a criminal charge. However, the refusal is not justified if it is based on a fear that it may give rise to a civil claim.[298] Presiding officers are required to warn witnesses in criminal proceedings of their rights under section 203. A failure to do so will ordinarily render the incriminating evidence inadmissible in a prosecution against the witness.

The extent of the privilege set out in section 203 is modified by section 204 of the Criminal Procedure Act, which is designed to encourage accomplices to testify as state witnesses against their co-offenders by providing an avenue for indemnity. The privilege against self-incrimination may also be claimed when an inquiry is held in terms of section 205 of the Criminal Procedure Act. However, the privilege falls away if the section 204 procedures are invoked during such an inquiry.[299]

Due consideration must be given to the right against self-incrimination when applying the coerced assistance provision in the Electronic Communications and Transactions Act. Section 82(1)(h) of the Electronic Communications and Transactions Act[300] empowers a cyber inspector

---

section 37 of the Criminal Procedure Act, the Court held that a voice fell within the parameters of section 37. However, the Court noted that it was difficult to envisage how law enforcement officers could be empowered to obtain a voice sample from an unwilling suspect. Consequently, the Court in an *obiter dictum* held that section 37(1)(c) had to be interpreted to imply that the law enforcement officers were not empowered to forcibly extract voice samples from an unwilling suspect.

294 Biometrics is the study of automated methods for uniquely recognising humans based upon one or more intrinsic physical or behavioral traits. It entails the measurement of physical characteristics, such as fingerprints, DNA, facial patterns, hand geometry, voice or iris and retinal patterns for use in verifying the identity of individuals. Biometrics not only deals with static patterns, but action as well. The dynamics of actually writing a signature can be analysed, not just the resulting pattern. Biometrics are a more secure form of authentication than typing passwords or even using smart cards, which can be stolen. However, methods can be circumvented; for example, fingerprints can be captured from a water glass and fool scanners. See Answers.com "Biometrics" found on the Internet http://www.answers.com/biometrics 1-9.

295 See Steytler *Constitutional Criminal Procedure* 338.

296 In *S v Lwane* 1966 (2) SA 433 (A), the Appellate Division required that a witness should be informed about the privilege against self-incrimination, as a waiver postulates knowledge of the right (443D). See also *S v Botha (2)* 1995 (2) SACR 605 W 609*f-g*.

297 *Magmoed v Janse van Rensburg* 1993 (1) SA 777 (A) 826.

298 Section 200 of the Criminal Procedure Act.

299 In *S v Maunye* 2002 (1) SACR 266 (T) paragraph [21], the Court noted *obiter* that section 204 appeared to be a justifiable limitation on the constitutional right not to give self-incriminating evidence. It was noted that this is "no doubt because it affords a person who is under suspicion a very fair and reasonable deal".

300 Note that a similar provision has been recommended in the proposed Computer Misuse Bill. With regard to both warrantless searches and searches under a warrant, section 7(4)(b) of the South African Law Reform Commission's proposed Computer Misuse Bill requires any person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data, to provide the law enforcement officer performing the search with the reasonable assistance that may be required to facilitate the execution of a search warrant. Section 7(7) criminalises obstructing, hindering or threatening an investigating official in the performance of her duties or the exercise of her powers. In the as yet

to require reasonable technical and other assistance for the purposes of chapter XII of the Electronic Communications Act from

(a) the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or

(b) any person in control of, or otherwise involved with the operation of the computer or information system.

A person who refuses to cooperate or hinders a person conducting a lawful search and seizure in terms of section 82 is guilty of an offence.[301]

4.2.4.7 Third parties

The impact of a search and seizure upon the rights, responsibilities and legitimate interests of third parties must be considered. Section 21(4) of the Criminal Procedure Act provides that a law enforcement officer executing a search warrant under both sections 21(4) and 25 must, after such execution, upon demand of "any person whose rights in respect of any search or article seized under the warrant have been affected", hand over a copy of the warrant. As search warrants issued under section 83(1) of the Electronic Communications and Transaction Act are subject to the provisions of section 25 of the Criminal Procedure Act,[302] notification is also required in respect of cyber inspector search warrants.

The person whose rights are affected by a search and seizure intervention is not entitled to a copy before the search starts, or the seizure takes place, but only after it becomes clear that she has been affected by such a search or seizure. Is it submitted that the person is, however, entitled to view and inspect the original warrant before the search commences, or before the seizure takes place.[303]

It has been held that search and seizure in terms of section 22(b) of the Criminal Procedure Act does not authorise a law enforcement officer to close down a business operating on premises which are being searched, as it could never have been the intention of the legislation to allow a

---

unreported Constitutional Court decision in *Magajane v The Chairperson, North West Gambling Board* Case CCT 49/05 delivered on 8 June 2006 the Constitutional Court noted that there "may well be some merit in the concerns raised by the applicant" (58). These concerns were raised by the applicant who argued that section 65(1)(b)(ii) and (c)(iii), read with section 82 of the North West Gambling Act 2 of 2001, required him to provide potentially self-incriminating information in violation of the right to freedom and security of the person (section 12(1) of the Constitution) and the right to a fair trial (section 35 of the Constitution). The applicant acknowledged that section 82 could be read so as not to create an offence for the failure to answer questions, but he contended that the possibility that section 82(a) created an offence placed the questioned person in the impossible situation of checking whether to risk self-incrimination or violate section 82(a). The applicant asserted that the provisions should at least contain a proviso that information obtained is not admissible in any ensuing criminal proceedings (at 57).

301 See also paragraph 4.2.2.2.3 above.

302 In terms of section 83(1) of the Criminal Procedure Act.

303 Du Toit *et al Commentary on the Criminal Procedure Act* 2-4.

law enforcement officer to hurt a person or business under suspicion more than is absolutely necessary under the circumstances. Specific authorisation to that effect must be obtained.[304] A business may not even be closed down if, in order to conduct an efficient search of the premises, the law enforcement officer would require assistance which would only be obtainable a few days later and even if to allow the business to remain open would, according to such a law enforcement officer, render the intended search and seizure partially or wholly ineffective. The destruction of an economically healthy business concern is clearly not envisaged by the section.[305]

Section 35(4)(b) of the Criminal Procedure Act provides that any forfeiture to the State of an article seized in terms of chapter 2 of the Criminal Procedure Act is subject to certain rights of third parties. Third parties should be informed of the intention to forfeit in order to afford such parties an opportunity to address the Court and to lead evidence if they so wish.[306]

4.2.4.8 Consequences of unlawful action by the authorities

The formal law consequences of unlawful action by the authorities are encapsulated in article 35(5) of the Constitution, which instructs that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice. This so-called exclusionary rule signals clearly to all state officials that it is futile to gather evidence in an unlawful manner, since evidence obtained unlawfully will not be taken into account by the Court in reaching a verdict.[307]

Section 28 of the Criminal Procedure Act illustrates the desire of the legislature that the powers of search, entry and seizure be used carefully and within the boundaries of the empowering sections by creating certain substantive law consequences of unlawful action by the authorities.[308] In terms of section 28(1), a law enforcement officer is guilty of an offence while exercising her powers to search and seize in terms of the Criminal Procedure Act if she acts contrary to the authorisation of a search warrant issued in terms of section 21(1) or 25(1). This is, for example, the case where the law enforcement officer does not limit her search to the articles mentioned in the search warrant or where she searches any person, container or premises, or seizes any article, or performs any act contemplated in section 25(1)(i)-(iii), without

---

304 See also paragraph 4.2.2.3.2 in respect of searches under exigent circumstances.

305 Du Toit *et al Commentary on the Criminal Procedure Act* 2-4A.

306 *S v Matsane* 1978 (3) SA 821 (T) 828B; *S v Hlangothe* 1979 (4) SA 199 (B) 202C and *S v Mongale* 1979 (3) SA 669 (B) 675F. See also Du Toit *et al Commentary on the Criminal Procedure Act* 2-15.

307 *S v Motloutsi* 1996 (1) SA 584 (C); *S v Mayekiso* 1996 (2) SACR 298 (C) and Joubert (ed) *Criminal Procedure Handbook* 124. In *Key v Attorney-General, Cape of Good Hope Provincial Division* 1996 (2) SACR 113 (CC), it was held that fairness may require that unconstitutionally obtained evidence sometimes be admitted and other times be excluded (in accordance with section 35(5) of the Constitution). In *S v Madiba* 1998 (1) BCLR 38 (D), the Court held that the extent to which the accused's right to privacy was infringed upon was less important than achieving the purpose of the particular search in this instance.

308 See Du Toit *et al Commentary on the Criminal Procedure Act* 2-8 and Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 51.

being authorised to do so by the law. A law enforcement officer therefore commits an offence if she searches a person who has not been arrested without the person's consent and without reasonably believing that the officer will obtain a search warrant if she applies for one. These offences are sanctioned with a fine or imprisonment for a period not exceeding six months. In addition to criminal liability, law enforcement officers may also be held liable in terms of section 28(2), which provides that the Court may award compensation in terms of section 300 of the Criminal Procedure Act upon the application of any person who has suffered damage[309] in consequence of the unlawful search or seizure.

It must be borne in mind that other charges, such as *crimen iniuria,* assault, malicious injury to property and housebreaking may also be brought against law enforcement officers who abuse the power of search and seizure.[310]

4.2.4.9 Propriety

Section 29 of the Criminal Procedure Act stipulates that a search of any person or premises must be conducted with strict regard to decency and order. Also, a woman may only be searched by a woman, and if no female law enforcement officer is available, the search must be made by any woman designated for that purpose by a law enforcement officer. In terms of the general principles of the interpretation of statutes, it can certainly be assumed that a male person should also only be searched by a male. Any divergence from these provisions would be unlawful and "consent" by the person being searched to this divergence would be invalid, as it would be *contra bones mores.*[311]

4.2.4.10 Confidentiality

Section 84 of the Electronic Communications and Transactions Act, contrary to chapter 2 of the Criminal Procedure Act, specifically provides for the preservation of confidentiality. Section 84(1) provides that a person, who pursuant to any powers conferred under chapter XII of the Act, has obtained access to any information, may not disclose such information to any other person. Exceptions are provided for in that such information may be disclosed for the purposes of the Electronic Communications and Transactions Act and for the prosecution of an offence or pursuant to an order of court. Unauthorised disclosure is criminalised by section 84(2) and sanctioned with a fine or imprisonment for a period not exceeding six months.

---

309 Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 51. Damages also include *contumelia* suffered by the complainant as a result of the unlawful infringement on her privacy.

310 See *S v Boshoff* 1981 (1) SA 393 (T) and Kriegler *Hiemstra Suid-Afrikaanse Strafprosesreg* 42.

311 Joubert (ed) *Criminal Procedure Handbook* 123.

4.3 Transborder search and seizure in computing environments

Due to the central doctrine of international law that enforcement jurisdiction is strictly territorial in nature, an effective domestic legal basis to provide mutual legal assistance[312] is imperative, particularly in the realm of coercive measures such as search and seizure. The general legal framework enabling mutual legal assistance and the mutual provision of evidence or information, with South Africa as the requested and requesting state respectively, are considered below. Reference is also specifically made to the position with regard to the facilitation of mutual searches and seizures.

4.3.1 Requirements for transborder search and seizure

4.3.1.1 General mutual assistance framework

Mutual legal assistance is the fastest growing component of international co-operation.[313] Proust[314] points out that there has been an explosion of instruments providing for such assistance and substantial developments in the principles surrounding its application and practice in the last 15 years. During the last decade, South Africa has moved rapidly to make its legal processes available to the international community and to enhance its own mechanisms for seeking assistance from abroad.[315] South Africa's current mutual assistance measures meet the main requirements of international practice, although there are a number of

---

312 Mutual legal assistance is a broad concept and exists to promote the administration of justice, broadly understood. It has grown out of extradition practice, supplemented by international law enforcement cooperation and stimulation by cooperation in civil matters. Examples of informal (consensual) assistance include giving or sharing information; locating persons; making available public documents including copies of judgments and orders; obtaining the statements of witnesses who agree to be interviewed or to make depositions; and facilitating the personal appearance in foreign proceedings of persons who agree to cooperate. Formal (coercive) assistance involves a formal request, which requires intrusive measures or legal compulsion, such as a court or judicial order. Formal assistance can only be rendered if the domestic law of the requested state specifically provides for that possibility and the judicial authority is engaged. Examples of formal assistance include search and seizure; obtaining a deposition from an unwilling witness; the restraint or confiscation of the proceeds of crime; or the enforcement of an order of a foreign court. Mutual legal assistance requests are often mixed, in that some assistance can be rendered without judicial intervention (for example, police-to-police cooperation) and other assistance must be dealt with by a judicial authority. Contemporary international mutual legal assistance requires that all possible avenues of informal assistance should be exhausted and that formal requests should be reserved for the coercive realm. International cooperation is really a matter of common sense and goodwill. It is characterised by initiative and flexibility, subject both to the requirements of the foreign state and to the domestic requirements of constitutionality and legality. See *Reuters Group PLC v Viljoen NNO* 2001 (12) BCLR 1265 (C) 127 and D'Oliveira 2003 *SAJCJ* 324, 337 and 369.

313 Extradition is, however, the oldest and most familiar face of international cooperation. See Proust 2003 *SACJ* 306.

314 Proust 2003 *SACJ* 306.

315 Apart from the treaty-making drive referred to in footnote 326 below, South Africa has also committed itself to the most topical area of the restraint, confiscation and recovery of the proceeds of crime. Although the lifespan of the Proceeds of Crime Act 76 of 1996 was brief, the Prevention of Organised Crime Act 121 of 1998 introduced into South Africa both a conviction-based restraint and confiscation regime (see chapter 5) and a civil preservation or property and forfeiture regime (see chapter 6). The definitions in the International Cooperation in Criminal Matters Act of both restraint and confiscation orders were amended to make clear that any reference thereto is a reference to orders made under the Prevention of Organised Crime Act (see section 79(a)). Definitions in the Drugs and Drug Trafficking Act 140 of 1992 were also amended (see section 79(b)). The incorporation into its domestic law of the Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002 has further deepened South Africa's immersion into the practice of international legal assistance. The general law applies to states and not to international bodies such as the International Criminal Tribunals for the former Yugoslavia and Rwanda. The Implementation of the Rome Statute of the International Criminal Court 27 of 2002 relates only to crimes that fall within the competence of the International Court and contains wide-ranging measures of cooperation and judicial assistance to that court. The assistance provisions are very comprehensive and could serve as a compendium of assistance measures for reference purposes. D'Oliveira advises that these provisions may also be seen as an example of how South African general mutual assistance law could be consolidated. See D'Oliveira 2003 *SAJCJ* 364 and 349.

aspects that require attention, mainly in the area of role-player coordination and administrative arrangements. There are also some legislative and regulatory *lacunae*.[316]

Although the International Cooperation in Criminal Matters Act[317] did not intend to comprehensively regulate mutual assistance law, it remains a very important piece of enabling legislation.[318] It was designed as a supplementary facilitative measure and deals with three categories of assistance:

(a) the mutual provision of evidence or information;[319]

(b) the mutual execution of sentences and compulsory orders;[320] and

(c) the confiscation and transfer of the proceeds of crime, as well as restraint orders.[321]

In each category, provision is made for requests to and requests from a foreign state, [322] in accordance with the principle of reciprocity, and for legal coercion.

The Director-General of Justice and Constitutional Development is the South African central authority.[323]

---

316 There is, for example, no provision in the International Cooperation in Criminal Matters Act or other prior law for the transfer of persons in custody to assist with investigations or to testify in a requesting state. No such enabling provision has, as yet, been inserted into domestic legislation pertaining to correctional services. The Correctional Services Act 111 of 1998 will have to be amended. See D'Oliveira 2003 *SAJCJ* 323 and 365.

317 Parliament enacted the International Cooperation in Criminal Matters Act and the recalled Proceeds of Crime Act 76 of 1996 so as to give effect to the principal recommendations contained in the South African Law Reform Commission *Project 98 Report on International Cooperation in Criminal Prosecutions* (1995) [hereinafter referred to as the South African Law Reform Commission *Project 98 Report on International Cooperation*]. The said report proposed two bills, dealing with, respectively, international cooperation and the proceeds of crime. As far as mutual legal assistance is concerned, the South African Law Reform Commission *Project 98 Report on International Cooperation* did not constitute a comprehensive review of international cooperation, but was targeted at two main areas, namely the obtaining and providing of the evidence of witnesses (see chapters 1 and 2) and the restraint and confiscation of the proceeds of crime, including the subject of money-laundering and the execution of foreign sentences (see chapters 4 and 5). The opportunity was taken to recommend the widening of the scope of assistance beyond pending judicial proceedings so as to also encompass the investigation phase, to introduce the central authority structure (thus rendering the use of the diplomatic channel unnecessary), to provide formally for the immunity of persons appearing and to empower the President to enter into mutual legal assistance treaties.

318 Section 36, read with Schedule II of the International Cooperation in Criminal Matters Act, repeals certain pre-existing legislative provisions: sections 171 to 173 of the Criminal Procedure Act are now restricted to witnesses within South Africa; section 2 of the Foreign Courts Evidence Act 80 of 1962 and section 33 of the Supreme Court Act 59 of 1959 have been made applicable solely to civil proceedings. Concomitantly, the restrictive section 1 of the Protection of Businesses Act 99 of 1978 only applies in respect of the enforcement of process or requests emanating from abroad and the provision of evidence or information in civil matters; section 1 of the Enforcement of Foreign Civil Judgments was amended to exclude any reference to criminal proceedings in its definition of judgment; the provisions in the Drugs and Drug Trafficking Act 140 of 1992 that provided for measures of restraint and confiscation within South Africa, as well as assistance in the execution of foreign confiscation orders, were repealed. See D'Oliveira 2003 *SAJCJ* 347.

319 Chapter 2 of the International Cooperation in Criminal Matters Act.

320 Chapter 3 of the International Cooperation in Criminal Matters Act.

321 Chapter 4 of the International Cooperation in Criminal Matters Act.

322 A foreign state is defined in section 1 of the International Cooperation in Criminal Matters Act as any state outside the Republic. This includes any territory under the sovereignty or control of such state. This implies that formal mutual assistance cannot be rendered to international tribunals such as the International Criminal Tribunals for the former Yugoslavia or Rwanda. See D'Oliveira 2003 *SAJCJ* 349.

323 See the role and functions of the Director-General in chapters 2, 3 and 4, read with the definition of "Director-General" in section 1 of the International Cooperation in Criminal Matters Act. D'Oliveira opined that it was understandable that the Director-General of Justice was made the central authority at the time of the promulgation of the said Act, which was before the creation of the National Prosecuting Authority, as there were still close structural links to the prosecution service and coordination with criminal law practitioners was a matter of course. Due to constitutional and administrative changes, however, a hiatus has developed since that time. Liaison between the responsible section in the Department of Justice and the National Prosecution Service of the National Prosecuting Authority takes therefore place in the interests of best practice. It was suggested that the Minister of Justice and Constitutional Development should either by directive or by regulation require

The mutual legal assistance field is broader than is often realised. Whilst the more recent conventions tend to contain elaborate mutual assistance provisions, the older ones have to invoke the general mutual assistance law, as in the case of instruments not yet ratified by South Africa.[324] Furthermore, through practice and enabling legislation and based on international comity, South Africa has positioned itself to render assistance unilaterally, even in the absence of a treaty relationship.[325]

In any given case where coercive assistance is involved, it must first be determined whether South Africa is a convention or treaty partner with the requesting or requested state concerned. Bilateral or multilateral treaties,[326] underpinned by domestic law, constitute an enhanced and flexible basis for international cooperation. Notwithstanding the accession to the United Nations Conventions, states are encouraged to consider concluding bilateral or multilateral treaties, agreements or arrangements to enhance the effectiveness of international cooperation and they have been assured that the related convention provisions do not affect existing or future treaties

---

collaboration as a matter of course, until circumstances permit for the central authority to accommodate practitioners on its staff. Since a number of agencies (including the Department of Foreign Affairs; SAPS; Interpol; Correctional Services; and the National Prosecuting Authority, which includes the National Prosecution Service, Asset Forfeiture Unit and the Directorate of Special Operations) are involved in some facet of cooperation, it would be good practice to establish some coordinating mechanism at an operational level that could contribute greatly in achieving the aim of prompt and speedy action. Section 15(4) of the Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002 acknowledged this necessary collaboration in that the Director-General: Justice, again as the central authority, is required to submit any mutual legal assistance request not only to the magistrate within whose area of jurisdiction the witness resides or is believed to be present, but also to the National Director of Public Prosecutions. See D'Oliveira 2003 *SAJCJ* 350 and 366. Officials channel each request for compulsory assistance to the Director-General and thence to the Minister. Given the relative newness of mutual legal assistance legislation and the government's priority in developing international relationships, this is perhaps understandable at this stage. As most of the requests are standard and not politically contentious, it may be asked whether approval need as a rule be sought from the highest level. To eliminate delays and the volume of administrative work entailed, the delegation provisions of sections 28 and 29 of the International Cooperation in Criminal Matters Act should be put into use, as *per* the recommendation of the South African Law Reform Commission (see the South African Law Reform Commission *Report on International Cooperation in Criminal Matters* 86). See D'Oliveira 2003 *SAJCJ* 363.

324 South Africa must still ratify, for example, the 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents; the 1979 International Convention Against the Taking of Hostages; the 1979 Convention on the Physical Protection of Nuclear Materials; and, of course, the Cybercrime Convention. See also paragraph 1.1 footnote 77 above in respect of the delayed ratification of the Cybercrime Convention.

325 D'Oliveira 2003 *SAJCJ* 324.

326 In terms of section 27(1) of the International Cooperation in Criminal Matters Act 75 of 1996 and sections 83(1), read with 231(1) of the Constitution, the President, as head of the national executive, may, on such conditions as he deems fit, enter into any agreement with any foreign state for the provision of mutual assistance in criminal matters and may agree to any amendment of such agreement. After Parliament has agreed to the ratification of, accession to or amendment or revocation of such an agreement, the Minister of Justice and Constitutional Development must give notice thereof in the Government Gazette in terms of section 27(2) of the International Cooperation in Criminal Matters Act. By February 2006 South Africa had entered into the following bilateral treaties (Lesotho: 19 April 2001, Egypt: 11 November 2002, Algeria: 11 November 2002, Nigeria: 28 March 2002, France: 31 May 2001, the People's Republic of China: 20 January 2003, India: 16 October 2003, Iran: 31 August 2004), all of which had been ratified, although only four were in force (United States of America: 9 November 2000, Canada: 3 April 2001, France 1 March 2004, People's Republic of China: 17 November 2004). Negotiations with five other states had been concluded, but the agreements had not been signed (Argentina, Brazil, Hong Kong, Namibia, Zambia). Negotiations with nine other states have been initiated (Australia, Chile, Cuba, India, Iran, Peru, Thailand, United Arab Emirates, Uruguay). A request that South Africa be allowed to accede to the European Convention on Mutual Legal Assistance has been made to the Council of Europe. One regional multilateral agreement has been signed and ratified, namely the Southern African Development Community on Mutual Legal Assistance [hereinafter referred to as the SADC Protocol on Mutual Legal Assistance in Criminal Matters]. It was signed at Luanda on 3 October 2002 by the heads of 12 of the 14 member states (excluding the Republics of Mozambique and Zambia). It was ratified by the South African Parliament on 16 June 2003 and will enter into force after ratification by two-thirds of the SADC member states. It is intended solely for mutual legal assistance between the state parties. South Africa is continuing with its treaty-making initiative as one of the ways in which it endeavours to position itself in the international mutual legal assistance playing field. The Treaty Section of the Office of the Chief State Law Advisor (IL), National Department of Foreign Affairs is the custodian of all conventions and treaties. Information on conventions and treaties may either be obtained directly from the Department of Foreign Affairs or through the International Section of the Department of Justice. The information on the conventions mentioned in this research was obtained in February 2006 from the Treaty Section of the Office of the Chief State Law Advisor (IL), National Department of Foreign Affairs (courtesy Ms R Louw). Slight differences, that are in no way critical to this research, were picked up between the information provided by the Treaty Section (cited above) and the references contained in D'Oliveira 2003 *SAJCJ* 349 and 368-9.

governing mutual legal assistance.[327] Some of the existing bilateral or multilateral treaties applicable to the South African mutual legal assistance context are referred to below, by means of examples.

The first significant multilateral mutual assistance instrument was the 1959 European Convention on Mutual Assistance in Criminal Matters,[328] developed by the Council of Europe and concluded in Strasbourg. It was an important achievement of its time in its recognition of the necessity for specific instruments for co-operation in evidence gathering. However, it did not address the most significant challenge to mutual assistance, namely bridging the differences between legal systems, as it was designed to operate amongst the civil law states of Europe.[329] If its request for accession to the 1959 European Convention on Mutual Assistance in Criminal Matters is accepted, South Africa will at one stroke become a convention partner with a large number of states. South Africa has also acceded to the 1957 European Convention on Extradition and its two Additional Protocols.[330]

The 1959 European Convention on Mutual Assistance in Criminal Matters has profoundly influenced the development of other instruments, notably the Commonwealth Scheme for Mutual Assistance in Criminal Matters.[331] A scheme represents an agreed set of recommendations for legislative implementation by each government. As such, it is not a binding instrument that creates binding international obligations and it is not registered under article 102 of the United Nations Charter.[332] Some countries might have real difficulties in implementing the whole scheme (albeit it for constitutional reasons or because of a paucity of resources), but there is nonetheless some value in all Commonwealth countries' participating in and using a device which permits of relatively easy amendment and development of procedures in the light of experience. A scheme serves as a template for and an exhortation to introduce domestic enabling legislation which makes it possible to render assistance to another state.

South Africa's return to the Commonwealth in 1994 *ipso facto* entitled it to participate in the Scheme arrangement.[333] The Harare Scheme was amended, for example, in 1999 to provide for the protection of third party interests in the restraint or confiscation of proceeds of crime

---

327 Examples of such provisions can be found in articles 13(9) and 18(6) of the 2000 United Nations Convention against Transnational Organised Crime and articles 5(4)(g) and 7(6) of the Vienna Convention. See D'Oliveira 2003 *SAJCJ* 361.

328 Two Additional Protocols, in 1978 and 2001 respectively, developed the European Convention on Mutual Assistance in Criminal Matters, which was further supplemented by the European Union's Convention on Mutual Assistance in Criminal Matters between States adopted in 2000 (together with its Protocol of 2001).

329 Proust 2003 *SACJ* 306.

330 South Africa acceded to the European Convention on Extradition and its two Additional Protocols on 12 February 2003 and it entered into force on 13 May 2003. Information courtesy of Ms R Louw of the Treaty Section of the Office of the Chief State Law Advisor (IL), as provided in February 2006.

331 Hereinafter referred to as the Harare Scheme, which was endorsed by the Commonwealth Law Ministers' meeting in Harare in July 1986. Amendments were agreed upon in 1990. See McClean *International Cooperation in Civil and Criminal Matters* 186.

332 McClean *International Cooperation in Civil and Criminal Matters* 197.

333 D'Oliveira 2003 *SAJCJ* 327.

arising from a request for assistance. At the 2002 meeting of the law ministers, a further amendment was adopted to clarify the protection against self-incrimination and the process for determining questions of legal privilege. By virtue of this amendment, material can be transmitted between member states without concern about a violation of the protection against self-incrimination. Further, it is possible for the authorities in a requested state to send material to a requesting state without determining questions of privilege. However, the condition of sending such material is that the authorities in the requesting state must consider the issue of privilege before allowing the material to be used. Law ministers have also called for further review and consideration of the Harare Scheme with reference to emerging trends and issues in mutual assistance practice. It is interesting to note that two of the key areas identified were the use of mutual assistance requests to obtain the preservation of computer data and the interception of communications.[334]

The United Nations contributed most significantly to the development of mutual legal assistance by the preparation and adoption of the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.[335] The 1969 Vienna Convention on the Law of Treaties[336] has also had a marked influence on the 2000 United Nations Convention against Transnational Organised Crime.[337] The United Nations Convention against Transnational Organised Crime, as well as the draft United Nations Convention against Corruption, which is currently being negotiated, and the Cybercrime Convention contain detailed mutual legal assistance, subject-specific provisions. This is also the position with the 1999 International Convention for the Suppression of Terrorist Financing[338] as well as the 2001 United Nations Security Council Resolution 1373.[339]

However, the 1997 International Convention for the Suppression of Terrorist Bombings,[340] together with the International Convention for the Suppression of Terrorist Financing and the United Nations Security Council Resolution 1373, as well as the Convention of the Organisation

---

334 Proust 2003 *SACJ* 308. She also points out other emerging issues in mutual assistance that may need to be considered under the Harare Scheme, including the use of video and satellite links to gather witness statements and testimony and the ability of the defence to access the mutual assistance process.

335 The enactment by South Africa of the International Cooperation in Criminal Matters Act and an Extradition Amendment Act 46 of 1987 was specifically to enable South Africa to accede to the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. It is further implemented by the Drugs and Drug Trafficking Act 140 of 1992 and the Prevention of Organised Crime Act 140 of 1998, which absorbed the Proceeds of Crime Act 76 of 1996. See D'Oliveira 2003 *SAJCJ* 328 and 368. See also Gilmore *Combating International Drugs Trafficking: The 1998 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* 3 and McClean *International Cooperation in Civil and Criminal Matters* 248-9.

336 Acceded to by South Africa on 14 December 1998.

337 Signed by South Africa on 14 December 2000 but not ratified as yet.

338 Signed by South Africa on 10 November 2001 and ratified on 1 May 2003.

339 The United Nations Security Council Resolution 1373 is automatically binding on all member states and does not require ratification as it is a Chapter VII Resolution.

340 Signed by South Africa on 23 December 1999 and ratified on 1 May 2003.

of African Unity for the Suppression and Combating of Terrorism,[341] state the obligation to afford assistance without going into detail. The 1970 Hague Convention on the Unlawful Seizure of Aircraft[342] and the 1971 Montreal Convention on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation[343] also merely state the obligation to afford assistance. The 1962 Tokyo Convention on Offences and Certain Other Acts committed on Board Aircraft does not refer to mutual legal assistance at all. The 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms on the Continental Shelf[344] also simply state the obligation to afford assistance, without going into detail.[345]

Obtaining and providing evidential material in connection with an extradition[346] where criminal proceedings are pending constitutes one of the roots of mutual legal assistance. In treaties with other states, South Africa has committed itself to the seizure and surrender of articles connected to the proof of the offence which is the subject of extradition. An example of such a provision includes article 19 of the Extradition Agreement between the Government of the Republic of South Africa and the Government of the United Kingdom of Swaziland.[347]

4.3.1.2 Foreign requests to South Africa, as the requested state[348]

Chapter 2 of the International Cooperation in Criminal Matters Act provides for the mutual provision of evidence[349] and information between states. A request from a foreign state for assistance in obtaining evidence in South Africa for use in such a foreign state must be submitted to the South African Director-General of Justice who must be satisfied

(a) that proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting state;[350] or

(b) that there are reasonable grounds for believing that an offence has been committed in the requesting state or that it is necessary to determine whether an offence has been so

---

341 Signed by South Africa on 14 July 1999 and ratified on 7 November 2002. All three of these instruments aimed at terrorism have been implemented by the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.

342 Ratified by South Africa on 30 May 1972.

343 Acceded to by South Africa on 21 September 1998.

344 Neither have yet been ratified or acceded to by South Africa.

345 D'Oliveira 2003 *SAJCJ* 368-9.

346 By February 2006, South Africa entered into extradition treaties with 54 states. Information courtesy of Ms R Louw of the Treaty Section of the Office of the Chief State Law Advisor (IL), as provided in February 2006.

347 Published on 4 October 1968 in Government Notice 292 of 1968 in Government Gazette 2179 (Regulation Gazette 1026). Article 19 of the said extradition agreement provides for the handing over of property, even if extradition (although granted) could not be carried out; for temporary retention or conditional handing over; and to preserve the rights of third parties.

348 Section 1 of the International Cooperation in Criminal Matters Act defines a requested state as any foreign state to which a request for assistance in respect of any criminal matter in the Republic of South Africa is directed.

349 Section 1 of the International Cooperation in Criminal Matters Act specifically provides that evidence includes "all books, documents, and objects produced by a witness".

350 Section 7(2)(a) of the International Cooperation in Criminal Matters Act.

committed and that an investigation in respect thereof is being conducted in the requesting state.[351]

If the Director-General is so satisfied, she must submit the request to the Minister of Justice and Constitutional Development for approval,[352] upon whose approval the Director-General is to forward the request to the magistrate within whose area of jurisdiction the witness resides.[353] The magistrate causes the witness to be subpoenaed and to give evidence under oath or affirmation or to produce any book, document or object. A request to the competent authority in South Africa that a subpoena or process be served on a person who is required to attend proceedings in the requesting state is usually acceded to. However, such person cannot be compelled to obey the summons.[354]

The International Cooperation in Criminal Matters Act also provides for the subpoena, including *duces tecum*, and examination of witnesses,[355] the rights and privileges[356] of and offences by witnesses, which is illustrative of the coercive element embedded in the provisions.[357] Once a witness is sworn in or affirms to tell the truth, the magistrate must take the evidence of such person upon interrogatories or otherwise as requested, as if the said person was a witness in a magistrate's court in proceedings similar to those in connection with which her evidence is required. The magistrate must certify the record as correct, whereupon the record, together with a statement of the expenses incurred in connection with the examination, must be transmitted to the Director-General. An interpreter's certificate must accompany the record where applicable. A witness subpoenaed in terms of a request has the privileges enjoyed by witnesses in South African law, including being entitled to payment of expenses and fees provided for by magistrate's courts. Should the witness claim any privilege according to the law of the requesting state, the magistrate must record the objection and may postpone the

---

351 Section 7(2)(b) of the International Cooperation in Criminal Matters Act. In terms of section 7(3), the Director-General may rely on a certificate to that effect, issued by a competent authority in the requesting state.

352 Section 7(4) of the International Cooperation in Criminal Matters Act.

353 Section 7(5) of the International Cooperation in Criminal Matters Act.

354 This is a rule of international practice, as is also illustrated by paragraph 23(4) of the Harare Scheme, which states that a person whose appearance as a witness is the subject of a request and who does not agree to appear shall not by reason thereof be liable to any penalty or measure of compulsion in either the requesting or requested country. Our law has, however, made an exception in the case of neighbouring states. Subpoenas emanating from states which have been designated in terms of section 11(1) read with Schedule 1 of the International Cooperation in Criminal Matters Act are endorsed for service by a magistrate upon service of the subpoena on the witness. Such a witness is tendered an amount sufficient to cover the reasonable expenses to attend proceedings in the requesting state. Failure without sufficient cause to attend at the time and place specified in the subpoena is an offence. As for mutual legal assistance to our neighbouring states, the Documentary Evidence from Countries in Africa Act 62 of 1993 was furthermore designed to assist in the admissibility of documentary evidence emanating from a country in Africa, designated by the Minister of Justice and Constitutional Development, who may also designate institutions, offices, qualifications, functions or activities in a designated country as equivalent to those in the Republic. It is provided that a document, widely defined, is admissible as evidence in civil and criminal proceedings if it emanates from a designated country and appears on the face of it to have been prepared, attested, certified, compiled or executed by a person holding an office, possessing a qualification, performing a function or engaged in an activity equivalent to a corresponding institution in South Africa. It is, however, not known whether any designations have been made. See D'Oliveira 2003 *SAJCJ* 334 and 356.

355 Section 8 of the International Cooperation in Criminal Matters Act.

356 Section 9 of the International Cooperation in Criminal Matters Act.

357 Section 10 of the International Cooperation in Criminal Matters Act. Examples of such offences include the failure to attend or to remain in attendance; the refusal to be sworn in or to make an affirmation and the failure to answer satisfactorily or to produce any document or article under her control. The giving of false evidence is an offence punishable as in the case of perjury.

proceedings in order to obtain from the competent authority in the requesting state an intimation as to whether or not the witness could be compelled to give the evidence in question in criminal proceedings in the requesting state. Where the competent authority intimates that the claim to privilege is not recognised in its state, the magistrate must reject the objection and proceed to take the evidence.

Where a request relates to a number of witnesses[358] in various magisterial districts, a literal interpretation could be that the request must be forwarded to a number of magistrates, which could be cumbersome, cause delays and pose problems of coordination. D'Oliveira suggests that an amendment to the International Cooperation in Criminal Matters Act, to the effect of providing for any one magistrate to be designated with concomitant trans-jurisdictional powers to deal with the whole request, be considered.

In further popularising mutual legal assistance practice, it has been suggested that the South African central authority should consider compiling and circulating guidelines[359] for the contents of both outgoing requests and incoming requests to all agencies and other role players. The compilation of a database of the relevant legislation and requirements for the requests of foreign states, including their contact particulars, would also be very useful.[360]

4.3.1.3 Requests from South Africa, as the requesting state[361]

The International Cooperation in Criminal Matters Act makes provision for requests to the authorities of a foreign state for obtaining not only evidence emanating from proceedings in a court[362] but also information from a foreign agency via a judge in chambers or a magistrate.[363]

The procedure in section 2(1) of the International Cooperation in Criminal Matters Act is intended for hearings in which it appears to the Court that the examination of a person in a foreign state is necessary in the interests of justice and that the attendance of such a person cannot be obtained without undue delay, expense or inconvenience. The Court may then issue a letter of request[364] for the evidence of the person for use in the proceedings.

---

358 Such as a number of banking institutions or Internet service providers.

359 An example of such guidelines is the United Kingdom Central Authority Guidelines for Judicial and Prosecuting Authorities.

360 In this regard, the central authority could liaise with, for example, the Commonwealth Secretariat in London. See D'Oliveira 2003 *SAJCJ* 376.

361 Section 1 of the International Cooperation in Criminal Matters Act defines a requesting state as any foreign state from which a request for assistance in respect of any criminal matter is received.

362 Section 2(1) of the International Cooperation in Criminal Matters Act.

363 Section 2(2) of the International Cooperation in Criminal Matters Act.

364 Section 1 of the International Cooperation in Criminal Matters Act defines a letter of request as a letter requesting assistance of the nature contemplated in sections 2 (the provision of evidence or information), 13 (assistance in recovering a fine or compensation), 19 (assistance in enforcing a confiscation order) and 23 (assistance in enforcing a restraint order).

Where a letter of request is issued, if it is permitted by the law of the requested state, any party may submit interrogatories for attachment to the letter or appear at the examination[365] abroad to examine, cross-examine and re-examine the witness. In issuing the letter of request, the Court must include a request that an accurate record of the proceedings be kept according to the procedure normally followed in the requested state. The letter of request must include a further request that an accurate record be made of a witness's refusal and reasons for any refusal to answer any question or to produce any book, document or object.[366] Another request which may be included is that a video recording which is to form part of the record be made of the proceedings at the examination of the witness. Video conferencing facilities, of course, enable the virtual appearance of a witness. Evidence obtained by a letter of request is deemed to be evidence under oath if it appears that the witness was, in terms of the law of the requested state, properly warned to tell the truth.[367] The evidence obtained together, with the record of examination of the witness, is open to inspection by the parties.[368]

Section 2(2) of the International Cooperation in Criminal Matters Act makes provision for obtaining information prior to instituting proceedings, for use in an investigation related to an alleged offence. Upon application, a judge in chambers or a magistrate may issue an *ex parte* letter of request seeking to obtain information. The judge must be satisfied

(a) that there are reasonable grounds for believing that an offence has been committed in the Republic or that it is necessary to determine whether an offence has been committed;

(b) that an investigation in respect thereof is conducted; and

(c) that for purposes of the investigation it is necessary in the interests of justice that information be obtained from a person or authority in a foreign state.

Provision is made for the person in charge of the investigation to submit interrogatories to be attached to the letter of request, provided that this is permitted by the law of the requested state and, under the same proviso, to appear at the examination and question the person concerned.[369] Normally, where pre-trial statements are obtained from abroad whether by formal

---

365 Section 3(1) of the International Cooperation in Criminal Matters Act. This can be done through a legal representative, in the case of an accused who is not in custody, or in the case of a private prosecutor, in person.

366 Section 4 of the International Cooperation in Criminal Matters Act. In accordance with international practice, there is also now explicit provision in section 12 of the said Act, for the temporary immunity of a person appearing in South African proceedings.

367 Section 5 of the International Cooperation in Criminal Matters Act.

368 Section 6 of the International Cooperation in Criminal Matters Act.

369 Section 3 of the International Cooperation in Criminal Matters Act. In practice, the prosecuting authority will have included in its application the following: the precise assistance requested; the interrogatories (if any) together with a request for leave to supplement them; a request that statements comply with certain formalities, where required for admissibility in our law; and a request that the investigating officer and/or the prosecutor be permitted to be present at any inquiries or interviews and, in the case of a formal examination, to participate in questioning, subject to the law of the requested state. If the prosecution has done its homework, it will already have liaised with its foreign counterpart to ensure that this detailed draft request complies

or informal assistance, the State would be required to arrange to have the witness in question testify at the trial. However, when evidence is obtained by letter of request in terms of section 2(2), it must be admitted and forms part of the record on one of two bases

(a) if the party against whom it is to be adduced agrees that it be admitted; or

(b) if the Court, taking into account certain factors,[370] is of the opinion that it should be admitted in the interests of justice.[371]

Letters of request issued in terms of sections 2(1) or 2(2) of the International Cooperation in Criminal Matters Act must be sent to the Director-General for transmission to the court or tribunal specified in the request, or to the appropriate government body in the requested state, as the case may be. However, in cases of urgency, section 2(4) allows for the letter of request to be sent directly to the appropriate addressee, but in such cases the Director-General must be notified and furnished with a copy of the letter of request. There is no requirement that the response to a letter of request has to be sent to or via the Director-General. It may be sent directly to the court which issued the letter or, in the case of investigations, to the relevant prosecuting or law enforcement agency.

4.3.1.4 24 Hours a day, 7 days a week network

The National Prosecuting Authority currently acts informally as the South African point of contact for the purposes of the G8 Network.[372] No formal decision has, however, been taken in respect of the designation of a future permanent point of contact in terms of article 35 of the Cybercrime Convention.

4.3.1.5 Search and seizure specific mutual assistance

The basis for search and seizure in current South African mutual legal assistance practice is unclear. Some practitioners rely on the provisions of chapter 2 of the Criminal Procedure Act, read with section 31 of the International Cooperation in Criminal Matters Act, to facilitate mutual searches and seizures. Other practitioners utilise the provisions of sections 2 and 7 of the International Cooperation in Criminal Matters Act to enable mutual searches and seizures.

---

with the particular requirements of the foreign law, before submitting it to a judicial officer in chambers. See D'Oliveira 2003 *SAJCJ* 352.

370 Such as the nature of the proceedings, the nature of the evidence, the purpose for which it is tendered, any prejudice to any party which the admission of such evidence might entail and any other factor which in the opinion of the Court should be taken into account.

371 Section 5(3) of the International Cooperation in Criminal Matters Act.

372 See also footnote 121 in paragraph 3.4.1.2.4 above.

D'Oliveira argues that the extant criminal procedural statutory arrangements for rendering search and seizure specific international assistance predates the International Cooperation in Criminal Matters Act. He contends that the said statute does not deal with search and seizure, but leaves the existing law in place. Furthermore, the provision of search and seizure and other assistance is expressly not limited, in that section 31 of the International Cooperation in Criminal Matters Act provides that nothing contained in the Act shall be construed so as to prevent or abrogate or derogate from any arrangement or practice for the provision or obtaining of international cooperation in criminal matters otherwise than in the manner provided for by the said Act.[373] He further advances that the failure to avert to the background and precise contents of the International Cooperation in Criminal Matters Act have led to misunderstandings in case law.[374] D'Oliveira postulates that section 2 of the International Cooperation in Criminal Matters Act specifically provides for evidence or information only and that there are no prescriptions for a request for search and seizure which perforce rests on section 31. A request for search and seizure cannot be forced into section 2 any more than it can be processed through sections 13, 19 or 23 of the International Cooperation in Criminal Matters Act. He submits that the Criminal Procedure Act confers wide powers to search where the object of the search is to seize an article which falls into any one of three categories.[375] Two of these categories are relevant in the mutual assistance context in that it empowers law enforcement to seize anything

(a) which is concerned in or is on reasonable grounds believed to be concerned in,[376] or

(b) which may afford evidence of[377] the commission or suspected commission of, an offence, whether within the Republic or elsewhere.

Sections 20(a) and 20(b) of the Criminal Procedure Act were ahead of their time in that they did not require proceedings to be pending in a foreign state.[378] D'Oliveira opines that the Criminal Procedure Act does not prescribe how the request by a foreign jurisdiction must be channelled to the South African authorities. Presumably the known extradition route would be followed, namely through the diplomatic channel to the Justice Ministry.[379] Ultimately, as a general rule, a judicial officer would have to be satisfied that the conditions for the issue of a search warrant

---

373 There is a similar non-restriction provision in section 35 of the Implementation of the Rome Statute of the International Criminal Court 27 of 2002.

374 *Reuters Group PLC v Viljoen NNO* 2001 (12) BCLR 1265 (C) 1728 and 1729. The fact and import of the amendments explicitly effected by the International Cooperation in Criminal Matters Act were overlooked in this case (see D'Oliveira 2003 *SAJCJ* 324, 337 and 369). In *S v S E Mbongwa* Unreported Case No 1/2001 delivered on 28 June 2001 (OPD), the Court overlooked the amendment to section 171 of the Criminal Procedure Act. In granting an application in terms of section 2 of the International Cooperation in Criminal Matters Act for a request to the Republic of Poland, the Court erroneously issued a commission to itself. See D'Oliveira 2003 *SAJCJ* 353.

375 See the discussion in paragraph 4.2.2.1 above.

376 Section 20(a) of the Criminal Procedure Act.

377 Section 20(b) of the Criminal Procedure Act.

378 D'Oliveira 2003 *SAJCJ* 329.

379 D'Oliveira 2003 *SAJCJ* 329.

have been met. Alternatively, the requirements for acting without a search and seizure warrant ought to have been met.[380]

D'Oliveira's approach was rejected in the case of *Beheersmaatschappij Helling I NV v Magistrate, Cape Town.*[381] The Court held that where a foreign request for assistance entails intrusive, legally compulsive or coercive measures, such as arrest, subpoena or search and seizure, legal mechanisms must be found in the domestic law of South Africa which authorises such measures.[382] The Court argued that the respondents' reliance on section 31 of the International Cooperation in Criminal Matters Act as justification for the application for and issue of search warrants was misplaced. The reasons advanced by the Court were, firstly, that section 31 of the International Cooperation in Criminal Matters Act does not in itself confer any power on the State. Section 31 simply preserves any pre-existing power which there might be, and which must be derived from a legal source. Neither the State nor the prosecuting authority enjoys any residual power in this regard which is to be found in any other source.[383] Secondly, the Court stated that there is no evidence of the existence of any "arrangement or practice" of the kind referred to in section 31 of the International Cooperation in Criminal Matters Act. It does not necessarily follow from the fact that the International Cooperation in Criminal Matters Act is silent on the subject of searches and seizures that the legislature did not intend the Act also to apply to evidence obtained by those means. The Court found no incompatibility between sections 20 and 21 of the Criminal Procedure Act and section 7 of the International Cooperation in Criminal Matters Act. The contention that, when it comes to foreign requests for searches and seizures, law enforcement agents may simply apply to a magistrate for a search warrant under section 21 of the Criminal Procedure Act, without the necessity for any preliminary steps at all, cannot prevail in the Court's view. The Court ultimately held the following:

> Every consideration therefore points to the desirability of assistance in the form of search and seizure being subject to the same limitations and safeguards, in the form of ministerial approval, as assistance by way of obtaining *viva voce* evidence or depositions. The alternative would entail the possibility of search and seizure operations being launched at the instance of foreign authorities simply at 'police-to-police' level. In my view that cannot have been the intention of the Legislature when it enacted the Co-operation Act. For these reasons I am unable to agree with d'Oliveira, *op cit*, when he says at 330, *á propos* section 20 of the Criminal Procedure Act: 'The above statutory arrangement rendering international assistance predates the International Co-operation in Criminal Matters Act and is not affected by it' (underlining supplied), if by that he means that, after the commencement of the Co-operation Act, it

380 See the discussion in paragraph 4.2.2.3 above.
381 [2005] JOL 13758 (C).
382 See *Coetzee v Attorney-General, KwaZulu-Natal* 1997 (1) SACR 546 (D) 560a-c and *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C) 16-17.
383 See also *Reuters Group PLC v Viljoen NNO* 2001 (12) BCLR 1265 (C) 1276C-1278H.

> was still unnecessary to comply with section 7 of the latter Act before applying for a search warrant under section 20 of the Criminal Procedure Act. It seems to me that the interpretation of the Co-operation Act contended by the fifth, sixth, and seventh respondents would result in a *casus omissus* as regards searches and seizures. For this reason too it must be rejected, and the applicant's interpretation must be preferred. In this regard Devenish *Interpretation of Statutes* says at 212: 'Where a statute has two possible interpretations, one of which leads to a *casus omissus*, the other one should be applied.'[384]

The delivery or disposal of a seized article in connection with which an offence was committed or is on reasonable grounds suspected to have been committed in a country outside South Africa is furthermore provided for by section 36(1) of the Criminal Procedure Act. It must be ascertained whether reasonable grounds exist for believing that the seized article will afford evidence as to the commission (in a country outside South Africa) of any offence, or that it was used for the purpose of or in connection with such a commission of any offence. A magistrate within whose area of jurisdiction such an article was seized may, on application, order such article to be delivered to a member of a law enforcement agency established in such a country and the member of this agency may thereupon remove it from South Africa. The magistrate must, however, be satisfied that such an offence is punishable in such a country by death,[385] or by imprisonment for a period of twelve months or more, or by a fine of five hundred rand or more. Section 36(2) provides that whenever the article so removed from South Africa is returned to the magistrate, or whenever the magistrate refuses to order that the article be delivered as aforesaid, the article must be returned to the person from whose possession it was taken, unless the magistrate is authorised or required by law to dispose of it in some other manner.

4.3.2 Scope

4.3.2.1 Widest extent possible

Although this is not explicitly stated in the International Cooperation in Criminal Matters Act, the Act does not limit other forms of assistance.[386] The implied stance is that the widest measure of assistance is to be given.[387] South Africa has aligned itself with the injunction to afford other

---

384 *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C) 25-26 (Court's emphasis).

385 The death penalty has, however, been abolished in South Africa as a result of the judgment of the Constitutional Court in *S v Makwanyane* 1995 (6) BCLR 665 (CC).

386 Section 31 of the International Cooperation in Criminal Matters Act.

387 This also appears explicitly in two other instruments. Section 31 appears in a slightly different form in section 35 of the Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002. Article 1 of the SADC Protocol provides that, in accordance with its provisions, the parties must provide each other with the widest possible measure of mutual legal assistance in criminal matters. See D'Oliveira 2003 *SAJCJ* 365.

jurisdictions the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to criminal offences.[388]

4.3.2.2 Categories of crime

All categories of crime, unless specifically excluded in a relevant treaty, can be the subject of an evidence collection intervention. The definitions of "requested State" and "requesting State" in section 1 of the International Cooperation in Criminal Matters Act underscores the possibility of a mutual legal assistance request in respect of "any criminal matter".

4.3.2.3 Jurisdiction

Under chapter 2 of the Criminal Procedure Act a search warrant may be issued by a magistrate if the sought after article(s) reside within her jurisdiction. Section 7 of the International Cooperation in Criminal Matters Act states that foreign requests for assistance in obtaining evidence must be forwarded to the magistrate within whose area of jurisdiction the relevant witness from whom the evidence is to be sourced resides.[389] Both these sections could require multiple warrants if the relevant witnesses reside in different jurisdictions.

Section 36 of the Criminal Procedure Act provides that a magistrate within whose area of jurisdiction an article was seized may, on application, order such an article to be delivered to a member of a law enforcement agency established in a country outside South Africa, who may thereupon remove it from South Africa.

4.3.3 Conditions and safeguards

South Africa is a party to a number of international instruments that seek, *inter alia*, to ensure the adequate protection of human rights and liberties.[390]

4.3.3.1 Dual criminality

Section 16 of the International Cooperation in Criminal Matters Act provides for the express introduction of the dual criminality rule of extradition law into the South African mutual

---

388 This is also in line with, *inter alia*, article 1(1) of the 1959 European Convention on Mutual Assistance in Criminal Matters; article 18(2) of the 2000 United Nations Convention against Transnational Organised Crime; paragraph 1(1) of the Harare Scheme and articles 23 and 25(1) of the Cybercrime Convention. See also D'Oliveira 2003 *SAJCJ* 361.

389 See paragraph 4.3.1.2 above where it is recommended that provision be made for the designation of a single magistrate with concomitant trans-jurisdictional powers to deal with the whole request under section 7 of the International Cooperation in Criminal Matters Act in cases where witnesses reside in multiple jurisdictions.

390 Of those pertinently mentioned in the Cybercrime Convention, South Africa is a party to the 1996 International Covenant on Civil and Political Rights, the 1981 African Charter on Human Rights and People's Rights and the 1989 United Nations Convention on the Rights of the Child (a list of all the basic human rights instruments to which South Africa is a signatory party can be found on the Internet http://www.doj.gov.za/2004dojsite/docs/hrmtreaties.htm (the website of the Department of Justice) or, alternatively, it can be sourced from the Department of Foreign Affairs or through the International Section of the Department of Justice). See also footnote 326 in paragraph 4.3.1.1 above.

assistance law, by way of prominent exception.[391] It is the first and, thus far, only explicit introduction of dual criminality into the South African mutual assistance regime. Section 16 relates to the mutual execution of sentences and compulsory orders, with South Africa as requested state. The Minister of Justice and Constitutional Development may refuse a request from a foreign state for assistance in recovering a fine to which a person has been sentenced in criminal proceedings, or an order for the payment of compensation for damages. In order to refuse such a mutual legal assistance request, the Minister must be satisfied that the surrender of the person upon whom the sentence was imposed or against whom the order was made, would not have been ordered under any South African law relating to extradition, if the extradition of such person had been requested. South Africa should not assist in enforcing penal provisions which are patent violations of fundamental rights.

It might be argued that, in considering the interests of justice as made provision for, *inter alia*, in sections 18, 20(1)[392] and 26(1) of the International Cooperation in Criminal Matters Act, the issue of double criminality might receive secondary consideration. The enforcement of a sentence, confiscation and restraint orders may not be contrary to the interests of justice.

4.3.3.2 Grounds for refusing a mutual legal assistance request

Barring one exception in a specific category of assistance, namely section 16, which enables the Minister of Justice and Constitutional Development to apply the dual criminality requirement, there is no statement of grounds for refusal in the International Cooperation in Criminal Matters Act. Although section 16 commences with the words "without limiting the Minister's discretion in any manner", there is nowhere a legislated indication of the components of such discretion.[393] South Africa's mutual assistance treaties generally do contain a suitable statement,[394] but this does not remedy the *lacuna* in the domestic legislation.

As the International Cooperation in Criminal Matters Act is silent on the aspects of confidentiality and use limitations, these are also areas in which South African treaty-making is ahead of the Act. The legislature could consider the formulations contained in our treaties in remedying the *lacuna*, particularly because investigations might require confidentiality prior to disclosure for trial purposes.[395]

---

391 D'Oliveira 2003 *SAJCJ* 358.

392 D'Oliveira, however, specifically observes that there is no provision in section 20 of the International Cooperation in Criminal Matters Act, as is the case in respect of section 16 of the International Cooperation in Criminal Matters Act, expanding the Minister's discretion or taking into account double criminality, *per se*. D'Oliveira 2003 *SAJCJ* 367.

393 D'Oliveira 2003 *SAJCJ* 367.

394 See, for example, article 6 of the SADC Protocol and section 11 of the Extradition Act 67 of 1962, where provisions are made for the Minister's discretion in extradition matters.

395 Examples where provision have been made for confidentiality and use limitations include article 8 of the Treaty between the Government of the Republic of South Africa and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters and article 11 of the SADC Protocol. D'Oliveira 2003 *SAJCJ* 367.

4.3.3.3 Costs

In international practice, the general rule is that the normal costs are for the account of the requested state. Only certain specified costs and extraordinary expenses are for the account of the requesting state. The responsibility for costs is normally included in treaties which also make provision for consultation between the countries concerned.[396] Alternatively, *ad hoc* interstate arrangements are often the means to settle what could be a complicated issue.[397]

Section 3(3) of the International Cooperation in Criminal Matters Act provides that where the prosecution has applied for the letter of request the Court may order that the costs of legal representation for the accused be paid by the State. If, subsequently, the accused unreasonably and unjustifiably refuses to admit the evidence obtained by the letter, the Court may make an appropriate order of costs against the accused.

Section 8(3) of the International Cooperation in Criminal Matters Act is aimed at foreign requests to South Africa and provides that, upon completion of the examination of a witness, the magistrate taking the evidence must transmit to the Director-General: Justice the record of the evidence certified by her to be correct. A certificate showing the amount of expenses and costs incurred in connection with the examination of the witness must be attached to the record of the evidence.

In terms of section 9(4) any person required to give evidence at an examination under section 8 of the International Cooperation in Criminal Matters Act is entitled to payment of such expenses and fees as are payable to witnesses in a magistrate's court.[398]

4.3.3.4 Admissibility and authentication

The purpose of obtaining legal assistance from abroad is to secure evidential material that will be legally admissible in South African court proceedings. Similarly, to enable South Africa to render assistance, documentation from a requesting state needs to be acceptable to the judicial authority. As South African courts have to be satisfied that foreign documentation is genuine, such documentation, whether the original or a certified copy thereof, must be authenticated. This is understood to mean the verification of any signature thereon.

---

396 Examples of such provisions include paragraph 12 of the Harare Scheme and article 10 of the SADC Protocol. See also D'Oliveira 2003 *SAJCJ* 367.

397 Such *ad hoc* interstate arrangements could be particularly helpful where the request entails engaging senior counsel for interlocutory matters or in major fraud investigations, requiring the production of voluminous documentation. D'Oliveira, however, proposes that consideration should be given to including at least general provisions to costs in either the statute or in the regulations, as the subject is, according to him, only obliquely mentioned in the International Cooperation in Criminal Matters Act. This would seem advisable for the guidance of officials and practitioners and for serving as rules to be applied where the requesting state is not a treaty partner. D'Oliveira 2003 *SAJCJ* 367-368.

398 In proceedings similar to those in connection with which the evidence given by the person is required.

Section 30 of the International Cooperation in Criminal Matters Act provides that any deposition, affidavit, record of any conviction or any document evidencing an order of court, issued in a foreign state,[399] may be received in evidence at any proceedings in terms of a provision of this Act if

(a) it is authenticated in the manner in which foreign documents are authenticated; or

(b) authenticated in the manner provided for in any agreement with the foreign state concerned.

4.4 Domestic production orders in computing environments

4.4.1 Background

Production orders under the Cybercrime Convention[400] are directed at two categories of information, namely specified, stored computer data and subscriber information. The procedural mechanisms in South African law that can be aimed at the production of, *inter alia*, these types of data are, first, section 205 of the Criminal Procedure Act, second, section 19 of the RICPCIA[401] and, third, sections 39(3) and 40(3) of the RICPCIA.[402] These production devices are considered below, with specific reference to their requirements, scope and conditions and safeguards.

It needs to be mentioned that data protection legislation for South Africa has been in the pipeline for a couple of years. Privacy has become an important trade issue as information privacy concerns can create a barrier to international trade. South Africa cannot afford to be denied general access to personal information from its major trading partner countries, most of which have already implemented proper information protection legislation. The protection of personal information is, to some extent, addressed in chapter VIII of the Electronic Communications and Transactions Act. These provisions, however, introduced only a voluntary data protection regime. The South African Law Reform Commission's *Discussion Paper 109 on Privacy and Data Protection*[403] was released in October 2005. The preliminary recommendations are set out in a draft Protection of Personal Information Bill. When it comes into force, the new Protection of Personal Information Act will provide for comprehensive regulation of all aspects of the collection, use, disclosure, storage of and access to personal

---

399 Or any copy or sworn translation thereof.

400 See paragraph 3.5 above.

401 Section 19 of the RICPCIA provides for the application for, and issuing of an archived communication-related information direction. See paragraph 4.4.2.2 below.

402 Sections 39(3) and 40(3) of the RICPCIA provide for the provision of information obtained and kept by certain telecommunications service providers and information kept in respect of cellular phones and SIM-cards respectively. See paragraph 4.4.2.3 below.

403 The closing date for comments was 28 February 2006. A copy can be found at http://www.doj.gov.za/salrc/dpapers.htm.

information. The general principles[404] espoused in the new legislation will, in due course, be supplemented by industry-specific codes of conduct which will provide more detailed, practical guidance. Provision has also been made for the establishment of a statutory regulatory agency, called the Independent Information Protection Commission, which will be responsible for the implementation of both the proposed Protection of Personal Information Act and the Promotion of Access to Information Act.[405] The South African Law Reform Commission furthermore explicitly endeavoured to ensure that the new legislation provides an adequate level of information protection as embodied in the terms of the European Union Data Protection Directive.[406] These developments will impact on, *inter alia*, the availability and production of information required for law enforcement purposes.

4.4.2 Requirements

4.4.2.1 Section 205 of the Criminal Procedure Act

Section 205(1) of the Criminal Procedure Act provides that a judge of the High Court or a magistrate of the Lower Court may,[407] upon the request of a Director of Public Prosecutions, or a public prosecutor authorised thereto in writing by the Director of Public Prosecutions, require the attendance[408] before her or any other judge or magistrate, for examination by the prosecutor, of any person who is likely to give material or relevant information[409] as to any alleged offence, whether or not it is known by whom the offence was committed. However, if such a person furnishes that information to the satisfaction of the prosecutor concerned prior to the date on which she is required to appear before a judge or magistrate, she shall be under no further obligation to appear before such a judicial officer. Nowadays, section 205 is frequently

---

404 The proposed Protection of Personal Information Bill gives effect to eight core information protection principles, namely: processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability. See the South African Law Reform Commission's *Discussion Paper 109 on Privacy and Data Protection* 6-7.

405 2 of 2000.

406 See the EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data found on the Internet http://www.cdt.org/privacy/eudirective/EU-Directive .html.

407 In *S v Cornelissen; Cornelissen v Zeelie NO* 1994 (2) SACR 41 (W), the Court took the view that the word "may" in section 205 was to be read as investing in the judicial officer issuing the subpoena an independent discretion. The Court found nothing in the section to indicate that the judicial officer should be relegated to being a mere functionary of the public prosecutor. As such, the judicial officer is entitled to require the submission of further evidence in exercising this discretion (*Haysom v Additional Magistrate, Cape Town, S v Haysom* 1979 (3) SA 155 (C) 158F-G; *Matisonn v Additional Magistrate, Cape Town* 1980 (2) SA 619 (C) 625 and *S v Matison* 1981 (3) SA 302 (A) 311). The function of the issuing judicial officer involves the exercise of a judgment as to whether the circumstances placed before her warrant the issue of a subpoena upon the person named by the prosecutor. Recently, indications are that the issuing magistrate must exercise an independent judgment not only as to the existence, in law, of the alleged offence, but also as to the likelihood that the prospective witness will be able to provide material evidence regarding the offence. See Du Toit *et al Commentary on the Criminal Procedure Act* 23-52B.

408 Although section 205 does not require the formal issuing of a subpoena, this is the method invariably employed to procure attendance. See *S v Matison* 1981 (3) SA 302 (A) 310F.

409 Under the old section 83 of the Criminal Procedure Act 56 of 1955 (the predecessor to section 205 of the Criminal Procedure Act) it was required that the person examined should be one likely to give "material evidence" as to the alleged offence. In *S v Russell* 1977 (4) SA 291 (C) it was held that a failure by a witness to furnish the names of his informers did not afford the magistrate jurisdiction to impose a sentence in terms of section 212 of the Criminal Procedure Act 56 of 1955 (now section 189 of the Criminal Procedure Act). Although the identity of these informers constituted, at most, information as to the alleged offence, it was not evidence which could properly be adduced in a court of law (294-5). It was pointed out, however, that the words "material or relevant information" in the new section 205(1) appear to have a wider connotation, and it seems probable that the facts in *Russell* case would have yielded a different conclusion under this section. See Du Toit *et al Commentary on the Criminal Procedure Act* 23-52B.

utilised as a sort of a legal disclaimer that service providers rely on when making available confidential information of their customers, such as bank statements, detailed cellular phone billings and Internet logs.

The section 205 examination may be conducted in private at any place designated by the judicial officer concerned.[410] The judicial officer must be of the opinion that the information required from a person examined in terms of section 205(1) who refuses or fails to give such information must be furnished for the administration of justice or the maintenance of law and order before a sentence to imprisonment as contemplated in section 189 may be ordered.[411]

Section 205(2) stipulates that the provisions of section 162-165,[412] 179-181,[413] 187-189,[414] 191[415] and 204[416] applies, *mutatis mutandis*, with reference to the proceedings under section 205(1).

---

410 Section 205(3) of the Criminal Procedure Act.

411 Section 205(4) of the Criminal Procedure Act.

412 As section 162 of the Criminal Procedure Act, which requires witnesses to be examined under oath, is peremptory, the evidence will be disregarded if witnesses (including any expert witnesses and interpreters involved) are not properly sworn. A witness subpoenaed merely to produce documents need not be sworn (*Waterhouse v Shields* 1924 CPD 155). If a witness objects to taking the oath, she may opt to make an affirmation in terms of section 163. Section 164 allows the presiding judicial officer to admonish any person who, from ignorance arising from youth, defective education or other cause, is found not to understand the nature and import of the oath or the affirmation to speak the truth. Such persons may be admitted to give evidence in criminal proceedings without taking the oath or making an affirmation. In terms of section 165, an oath, affirmation or admonition may be administered by or through an interpreter or intermediary in the presence or under the eyes of the presiding judicial officer. In addition to being competent, the interpreter must also take an oath or make an affirmation that she will interpret truly and correctly. An unsworn interpreter may not administer the oath to a witness, as any "evidence" thus given would be considered unsworn. Du Toit *et al Commentary on the Criminal Procedure Act* 22-20A.

413 Section 179 of the Criminal Procedure Act details the process for securing the attendance of witnesses. Section 180 provides for the service of a subpoena, with reference also to Supreme Court Rules 54(5) 54(8), Rule 55(1)-(3) and Rule 56, as well as Rule 64 of the Magistrates' Courts Rules that provide for the manner of issuing and serving a subpoena. Section 328 provides that any process of court is of force throughout the Republic. Section 329 provides that, subject to the rules of court, any law enforcement officer may serve or execute court process. Section 330 allows for the transmission of court process by telegraph or similar communication. In respect of the attendance of witnesses in foreign courts, section 7 of the Foreign Courts Evidence Act 80 of 1962, as amended by the International Cooperation in Criminal Matters Act applies in respect of the Kingdoms of Lesotho and Swaziland and the Republics of Botswana, Malawi, Namibia and Zimbabwe. See also Du Toit *et al Commentary on the Criminal Procedure Act* 23-2 and paragraph 4.3.1.2 above in respect of mutual legal assistance. Section 181 provides for the pre-payment of witness expenses (i.e. travelling and overnight expenses). Other payments in terms of section 191 will be considered after the witnesses have attended in obedience to the subpoena.

414 Section 187 of the Criminal Procedure Act requires a witness to attend proceedings and to remain in attendance, failure of which, in terms of section 188, is an offence, subject to the same sentence as provided for in section 170(2) (i.e. a fine not exceeding R300 or imprisonment for a period not exceeding 3 months). Section 189 of the Criminal Procedure Act deals with the powers of the Court with regard to recalcitrant witnesses. It provides that if any person present at criminal proceedings is required to give evidence at such proceedings and refuses to be sworn or to make affirmation as a witness, or having been sworn or having made an affirmation as a witness, refuses to answer any question put to her or refuses or fails to produce any book, paper or document required to be produced by her, the Court may in a summary manner enquire into such refusal or failure and, unless the person so refusing or failing has a just excuse for her refusal or failure, sentence her to imprisonment for a period not exceeding two years or, where the criminal proceedings in question relate to an offence referred to in Part III of Schedule 2 to imprisonment for a period not exceeding five years. After the expiration of any sentence imposed under section 189(1), the person concerned may from time to time again be dealt with under section 189(1) with regard to any further refusal or failure (section 189(2)). A court may at any time on good cause shown remit any punishment or part thereof imposed by it under section 189(1) (section 189(3)). Any sentence imposed by any court under section 189(1) shall be executed and be subject to appeal in the same manner as a sentence imposed in any criminal case by such court, and shall be served before any other sentence of imprisonment imposed on the person concerned (section 189(4)). The Court may, notwithstanding any action taken under section 189, at any time conclude the criminal proceedings referred to in section 189(1) (section 189(5)). No person shall be bound to produce any book, paper or document not specified in a subpoena served upon her, unless she has such book, paper or document in court (section 189(6)). Any Lower Court shall have jurisdiction to sentence any person to the maximum period of imprisonment prescribed by this section (section 189(7)). Section 11 of the Constitutional Court Complementary Act 13 of 1995 allows for the detention of a recalcitrant witness for a period of 8 days at a time it the witness without any just excuse refuses to be sworn, refuses to answer questions or refuses or fails to produce a document which she is required to produce.

415 Section 191 of the Criminal Procedure Act provides for the payment of the expenses of witnesses.

416 Section 204 of the Criminal Procedure Act addresses the provision of incriminating evidence by a witness for the prosecution.

Section 15(2) of the RICPCIA safeguards the availability of section 205 of the Criminal Procedure Act and other alternative procedures in respect of the provision of real-time or archived communication-related information, provided that such communication-related information is not obtained in terms of other such acts on an ongoing basis.[417] The measures provided for in sections 17 and 19 of the RICPCIA[418] do not preclude obtaining such information in respect of any person in accordance with alternative procedures prescribed in any other act.

4.4.2.2 Archived communication-related directions

Telecommunications service providers must not only provide a telecommunications service which has the capability to be intercepted, but are also under a general obligation to store communication-related information.[419]

As a general rule, telecommunications service providers and their employees are prohibited from intentionally providing or attempting to provide any real-time or archived communication-related information to any person other than the customer of the telecommunications service provider concerned to whom such real-time or archived communication-related information relates.[420] However, any telecommunications service provider to whom an archived communication-related direction is addressed may provide any archived communication-related information to which that archived communication-related direction relates.[421] Any telecommunications service provider may also, upon the written authorisation given by a customer on each occasion, and subject to the conditions determined by the customer concerned, provide to any person specified by that customer archived communication-related information which relates to the customer concerned.[422]

Section 19 of the RICPCIA allows for the application for and issuing of an archived communication-related direction. If only archived communication-related information is required, an application may be made to a judge of a High Court or a magistrate of the Lower Court to issue an archived communication-related direction,[423] whereupon an archived

---

417 Section 59 of the RICPCIA amended section 205 of the Criminal Procedure Act to also subject it to section 15 of the RIPCIA.

418 Sections 17 and 19 of RICPCIA provide for the application for, and issuing of, real-time communication-related and archived communication-related directions respectively.

419 Section 30(1) of RICPCIA. See paragraph 2.4.4 above in respect of data retention. The directives in respect of different categories of telecommunications service providers (i.e. fixed line operators, mobile cellular operators and Internet Service Providers) made in terms of the RICPCIA has been published in the Government Gazette 28 November 2005 No 28271 3 by General Notice 1325 of 2005. Copies are also available on the Internet http://www.info.gov.za/gazette/notices/2005/28271.pdf. These directives provide that communication-related information must be kept for a period of three years with regard to the fixed line and mobile cellular operators (see section 17 of Schedule A and section 17 of Schedule B). No reference to a period of retention is mentioned in respect of the Internet Service Providers. These directives also provide technical content to, *inter alia*, the term "archived communication-related information".

420 Section 12 of the RICPCIA.

421 Section 13 of the RICPCIA.

422 Section 14 of the RICPCIA.

423 Section 19(1) of the RICPCIA.

communication-related direction may be issued.[424] An archived communication-related direction may only be issued if it appears to the judge of a High Court or a magistrate of the Lower Court concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that the provision of archived communication-related information is necessary for the purposes of investigating or gathering information in respect of the following offences:[425]

(a) a serious offence[426] has been or is being or will probably be committed;[427]

(b) it is necessary to gather information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic;[428]

(c) it is necessary to gather information concerning a potential threat to the public health or safety or national security of the Republic;[429]

(d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or

---

424 Section 19(3) of the RICPCIA.

425 Section 19(4) of the RICPCIA.

426 A serious offence is defined in section 1 of the RICPCIA to mean any offence mentioned in the Schedule to the RICPCIA, namely: high treason; any offence referred to in paragraph (a) of the definition of "specified offence" of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004; sedition; any offence which could result in the loss of a person's life or serious risk of loss of a person's life; any offence referred to in Schedule 1 to the Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002; any specified offence as defined in section 1 of the National Prosecuting Authority Act 32 of 1998; any offence referred to in chapters 2, 3 and 4 of the Prevention of Organised Crime Act 121 of 1998; any offence referred to in section 13(f) of the Drugs and Drug Trafficking Act 140 of 1992; any offence relating to the dealing in or smuggling of ammunition, firearms, explosives or armament and the unlawful possession of such firearms, explosives or armament; any offence under any law relating to the illicit dealing in or possession of precious metals or precious stones; any offence contemplated in part 1 to 4, or section 17, 20 or 21 (in so far as it relates to the aforementioned offences) of chapter 2 of the Prevention and Combating of Corrupt Activities Act 12 of 2004; dealing in, being in possession of or conveying endangered, scarce and protected game or plants or parts or remains thereof in contravention of any legislation; any offence wherefore the punishment may be imprisonment for life or a period of imprisonment prescribed by section 51 of the Criminal Law Amendment Act 105 of 1997, or a period of imprisonment exceeding five years without the option of a fine. A serious offence also includes an offence that is allegedly being or has allegedly been or will probably be committed by a person, group of persons or syndicate acting in an organised fashion. "Organised fashion" includes the planned, ongoing, continuous or repeated participation, involvement or engagement in at least two incidents of criminal or unlawful conduct that have the same or similar intents, results, accomplices, victims or methods of commission, or otherwise are related by distinguishing characteristics. Acting in the execution or furtherance of a common purpose or conspiracy or which could result in substantial financial gain for the person, group of persons or syndicate committing the offence also qualifies as a serious offence. Any conspiracy, incitement or attempts to commit any of the above-mentioned offences are also considered to be serious offences in terms of section 1 of the RICPCIA.

427 An application on this ground must be made, as *per* the definition of "applicant" in section 1, read with sections 19(6) and 16(3) of the RICPCIA, by the following persons: An officer referred to in section 33 of the South African Police Services Act 68 of 1995, if the officer concerned obtained in writing the approval in advance of another officer in the SAPS with at least the rank of assistant-commissioner and who has been authorised in writing by the National Commissioner to grant such approval; the head of the Directorate of Special Operations referred to in section 1 of the National Prosecuting Authority Act 32 of 1998 (hereinafter referred to as the DSO) or an Investigating Director authorised thereto in writing by the head of the DSO; and a member of the Independent Complaints Directorate, if the member concerned obtained in writing the approval in advance of the Executive Director. The latter application may only be made on this ground if the offence has allegedly been or is being or will be committed by a member of the SAPS, or in respect of a death in police custody or as a result of police action.

428 An application on this ground must be made, as *per* the definition of "applicant" in section 1, read with sections 19(6) and 16(3) of the RICPCIA, by the following persons: an officer as defined in section 1 of the Defence Act 44 of 1957, if the officer concerned obtained in writing the approval in advance of another officer in the Defence Force with at least the rank of major-general and who has been authorised in writing by the Chief of the Defence Force to grant such approval; and a member as defined in section 1 of the Intelligence Services Act 38 of 1994, if the member concerned obtained in writing the approval of another member of the Agency or the Service, as respectively defined in section 1 of the Intelligence Services Act, as the case may be, holding a post of at least general manager.

429 The position is the same as set out in footnote 428.

terrorism, is in accordance with an international mutual assistance agreement; or in the interests of the Republic's international relations or obligations;[430] or

(e) it is necessary to gather information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities.[431]

An application for an archived communication-related direction must be in writing and must comply with any supplementary directives relating to applications for archived communication-related directions.[432] The application must contain, with the necessary changes, the information required for the purposes of an application for a real-time communication-related direction.[433] This includes an indication of the identities of the applicant and, if known, the customer in respect of whom the communication-related information is required. The telecommunications service provider to whom the archived communication-related direction must be addressed must also be identified. The application must contain full particulars of all the facts and circumstances alleged by the applicant in support of her application, including the specific grounds[434] on which the application is made. A description of the type of archived communication-related information that is required must be provided. The basis for believing that evidence relating to the grounds on which the application is made will be obtained through the provision of the communication-related information must also be provided. The logistics pertaining to whether the archived communication-related information must be routed to a designated interception centre specified in the application or provided to the law enforcement agency concerned must be elaborated upon. The period for which and the manner in which the archived communication-related information is required to be provided must be detailed. It must also be stated whether any previous application has been made for the issuing of an archived communication-related direction in respect of the same customer or archived communication-related information specified in the application. Furthermore, if such a previous application exists, the application must indicate the current status of that application.

---

430 An application on these grounds must, in the case of the investigation of a serious offence, be made by an applicant, as qualified above in footnote 427 from the ranks of the SAPS or the DSO and in the case of the gathering of information, be made by an applicant, as qualified above in footnote 428 from the ranks of the Intelligence Services. See the definition of "applicant" in section 1, read with sections 19(6) and 16(3) of the RICPCIA.

431 An application on this ground must be made, as *per* the definition of "applicant" in section 1, read with sections 19(6) and 16(3) of the RICPCIA, by a member of any component of the prosecuting authority, designated by the National Director of Public Prosecutions, contemplated in section 179(1)(a) of the Constitution to specialise in the application of Chapter 6 of the Prevention of Organised Crime Act 121 of 1998, authorised thereto in writing by the National Director of Public Prosecutions.

432 Section 19(2) of the RICPCIA. Section 58 provides that a designated judge or, if there is more than one designated judge, all of the designated judges jointly, may, after consultation with the respective Judges-President of the High Courts, issue directives to supplement the procedure for making application for the issuing of directions or entry warrants in terms of the RICPCIA. Such a directive must be submitted to Parliament and may at any time in like manner be amended or withdrawn.

433 Section 19(2)(a) with reference to section 17(2) of the RICPCIA.

434 These grounds are set out in section 19(4) of the RICPCIA.

An archived communication-related direction must be in writing and must specify the following information:

(a) the identity of the customer, if known, in respect of whom the archived communication-related information is required, and the telecommunications service provider to whom the archived communication-related direction must be addressed;

(b) a description of the archived communication-related information that is required;

(c) whether the archived communication-related information must be routed to a designated interception centre specified in the application, or provided to the law enforcement agency concerned; and

(d) the period within which the archived communication-related information must be routed or provided.

The archived communication-related information may also specify conditions or restrictions relating to the provision of archived communication-related information authorised therein.[435]

An application must be considered and an interception direction must be issued without any notice to the person or customer to whom the application applies and without hearing such a person or customer. A designated judge considering an application may require the applicant to furnish whatever further information she deems necessary.[436]

If a judge of a High Court or a magistrate of a Lower Court issues an archived communication-related direction, she must, as soon as is practicable thereafter, submit a copy of the application and archived communication-related direction concerned to a designated judge.[437] A designated judge must keep all copies of such applications and archived communication-related directions submitted to her, or cause them to be kept, for a period of at least five years.[438]

Section 18 of the RICPCIA also provides for the combined application for, and the simultaneous issuing by a designated judge[439] of

---

435 Section 19(5) of the RICPCIA.
436 Section 19(6), read with section 16(7) of the RICPCIA.
437 Section 19(7) of the RICPCIA.
438 Section 19(8) of the RICPCIA.
439 Section 18(4) of the RICPCIA provides that, notwithstanding sections 19(1), (3) and (4), such a combined application in terms of section 18(1) for the issuing of an archived communication-related direction under section 18(3)(a) may only be made to and issued by a designated judge.

(a) any combination of interception directions in respect of an indirect communication, real-time communication-related directions and/or archived communication-related directions,[440] or

(b) an interception direction supplemented by a real-time communication-related direction.[441]

If an authorised person who executes or assists with the execution of an archived communication-related direction hands such a direction or a copy thereof to the telecommunications service provider to whom such a direction is addressed, the telecommunications service provider concerned must assist in the execution of the direction.[442] The required information must be routed to the designated interception centre concerned or must be provided to the law enforcement agency concerned, in the form specified in the relevant archived communication-related direction.[443]

4.4.2.3 Sections 39(3) and 40(3) of the RICPCIA

For the purposes of applying for a direction to be issued, a written request may be made to a telecommunications service provider, including a telecommunications service provider who provides a mobile cellular telecommunication service,[444]

(a) to confirm that the person specified in the request is a customer of that telecommunications service provider concerned;

(b) to provide the applicant with the telephone number or any other number allocated to that person by that telecommunications service provider; and

(c) to furnish the applicant with a photocopy of the identification document of that person, which is then retained by that telecommunications service provider.[445]

A telecommunications service provider must immediately comply with such a request if the person specified in the request is a customer of the telecommunications service provider concerned.[446]

---

440 Section 18(1) of the RICPCIA.

441 Section 18(2) of the RICPCIA. Section 18(3) contains the proviso that such a real-time communication-related direction expires when the period or extended period for which the interception direction concerned has been issued lapses.

442 Section 28(2) of the RICPCIA.

443 In the case of real-time communication-related information, this must be done immediately, whilst archived communication-related information must be routed or provided within the period stated in the archived communication-related direction concerned.

444 As per section 40(3) of the RICPCIA that makes section 39(3) and (4), with the necessary changes, applicable in respect of any person who has sold, or in any other manner provided, a cellular phone or SIM-card to any other person.

445 Section 39(3) of the RICPCIA.

446 Section 39(4) of the RICPCIA.

4.4.3 Scope

4.4.3.1 Specific criminal investigations or proceedings

Uncertainty about the nature of the offence alleged does not constitute a bar to the issuing of a subpoena in terms of section 205 of the Criminal Procedure Act, nor to the duty of the witness to obey it.[447] A section 205 subpoena does not need to specify the alleged offence with the degree of particularity of a criminal charge. It suffices that the witness is apprised of an alleged offence about which information is sought. The enquiry is not restricted to the offences specified in the subpoena, but may be pursued also with regard to additional offences, the possible commission of which may emerge from the evidence.[448]

The cumulative effect of the requirements of sections 19(2)(a), 19(4) and 19(5) of the RICPCIA[449] is that archived communication-related directions are aimed at specific criminal investigations or proceedings.

Sections 39(3) and 40(3) of the RICPCIA are meant to facilitate making applications for directions in terms of the RICPCIA. As such, these sections are also aimed at specific criminal investigations or proceedings in individual cases.

4.4.3.2 Categories of crimes

Section 205(1) of the Criminal Procedure Act provides for the attendance of any person who is likely to give material or relevant information about any alleged offence.
Archived communication-related directions may only be issued in respect of a limited category of offences, as set out in section 19(4) of the RICPCIA.[450]

Bearing in mind that sections 39(3) and 40(3) of the RICPCIA are meant to facilitate the making of applications for directions in terms of the RICPCIA, they are directed at the limited category of offences covered by the particular direction concerned.

---

447 *Haysom v Additional Magistrate, Cape Town, S v Haysom* 1979 (3) SA 155 (C) 158H.

448 In *Davis v Additional Magistrate, Johannesburg* 1989 (4) SA 299 (W) it was held that the person subpoenaed under section 205 of the Criminal Procedure Act may not ignore the subpoena on the ground of vagueness (at 305). Such a person may raise the problem after having been sworn in and it is then up to the public prosecutor to furnish particulars. To require such particulars before the attendance at the inquiry the potential witness would, it was found, frustrate the very purpose of section 205. Also, where a witness attends the enquiry, complaints relating to technical or formal defects in the wording of the subpoena will not be entertained. Du Toit *et al Commentary on the Criminal Procedure Act* 23-52D discusses these more technical aspects of the section 205 subpoena, as considered in *Matisonn v Additional Magistrate, Cape Town,* 1980 (2) SA 619 (C) 625.

449 Incorporated in paragraph 4.4.2.2 above.

450 See paragraph 4.4.2.2 above.

4.4.3.3 Stored computer data

Section 205 of the Criminal Procedure Act can be used to induce the production of material or relevant information regarding any alleged offence. This section is aimed at both archived and real-time communication-related information, provided that it is not used to obtain such data on an ongoing basis.

There seems to be no prohibition against using section 205 of the Criminal Procedure Act to obtain access to encrypted information.[451] A cryptography[452] provider may not provide cryptographic services or products in South Africa unless the provider is registered with the Department of Communications.[453] A register of cryptography providers must be established and maintained.[454] Disclosure of the information contained in this cryptography register is restricted to, *inter alia*, a relevant authority investigating a criminal offence for the purposes of any criminal proceedings, government agencies responsible for safety and security in South Africa or a cyber inspector.

Under a decryption direction issued in terms of section 21(3) of the RICPCIA, a decryption key holder[455] is directed to disclose a decryption key;[456] or provide decryption assistance[457] in respect of encrypted information, and includes an oral decryption direction issued under section 23(7) of the RICPCIA. These decryption directions, however, must coincide with an application for the interception of communications, in terms of section 16(1) of the RICPCIA. The decryption directions cannot be utilised to facilitate the decryption of data obtained by other legislative mechanisms, such as a search and seizure or production.

Archived communication-related directions are aimed at archived communication-related information.

---

451 Section 1 of the RICPCIA defines "encrypted information" as any electronic data which, without the decryption key to that data, cannot, or cannot readily, be accessed; or cannot, or cannot readily, be put into an intelligible form. "Intelligible form" is defined as the form in which electronic data was before an encryption or similar process was applied to it.

452 See paragraph 2.3.1.3.2 above for a reference to the meaning of cryptography and paragraph 1.1.2 above for a reference to the issue of decryption assistance in the South African legislative framework. See also Lawack-Davids 2001 *Obiter* 1-30 for an overview of possible approaches to formulating policy on cryptography in South Africa (prior to the promulgation of the Electronic Communcations and Transactions Act).

453 Section 30(1) of the Electronic Communications and Transactions Act.

454 Section 29 of the Electronic Communications and Transactions Act.

455 "Decryption key holder" in terms of section 1 of the RICPCIA means any person who is in possession of a decryption key for the purposes of subsequent decryption of encrypted information relating to indirect communications.

456 "Decryption key" under section 1 of the RICPCIA means any key, mathematical formula, code, password, algorithm or any other data which is used to allow access to encrypted information or facilitate putting encrypted information into an intelligible form.

457 "Decryption assistance" in terms of section 1 of the RICPCIA means to allow access, to the extent possible, to encrypted information or to facilitate putting encrypted information into an intelligible form.

Sections 39(3) and 40(3) of the RICPCIA are directed at the identity of a customer and her telephone, cellular phone or any other number(s) allocated by the person by the telecommunications service provider.

4.4.3.4 Jurisdiction

An application for a subpoena in terms of section 205 of the Criminal Procedure Act may be made to any judge or magistrate. The subpoena may be directed to any person[458] and the examination may be conducted at any place designated by the judge or magistrate. Applications for archived communication-related directions may be made to a judge of the High Court or a magistrate of the Lower Court.

4.4.4 Conditions and safeguards

Some of the fundamental rights that might come into play when performing searches and seizures need to be considered in the context of production orders.[459] The following conditions and safeguards are considered here: supervision by competent authorities, the proportionality requirement, the protection of privileged data, the safeguarding of the rights of third parties, the consequences of unlawful actions by law enforcement officers and confidentiality.

4.4.4.1 Supervision by competent authorities

Section 205(1) of the Criminal Procedure Act provides that a judge or a magistrate may issue a subpoena to any person upon the request of a Director of Public Prosecutions, or a public prosecutor authorised thereto in writing by the Director of Public Prosecutions.

The position of a section 205-examinee or a recalcitrant witness is not similar to that of an accused person, as required for the protection afforded by the right to a fair trial.[460] The examinee cannot be convicted of any offence and the imprisonment of an examinee is not regarded as a criminal sentence or treated as such. The examinee is entitled to procedural fairness, but not to the protection of a right to a fair trial *per se.* This requires, in most cases, no more than the interposition of an impartial, independent entity to act as arbiter between the individual and the State.[461] However, a witness facing an inquiry under section 205 of the Criminal Procedure Act has a right to legal representation.[462]

---

458 Section 205(1) of the Criminal Procedure Act.

459 See paragraph 4.2.4 above, where the constitutional rights relevant in a search and seizure context were referred to.

460 *Nel v Le Roux NO* 1996 (1) SACR 572 (CC) 580c-g.

461 See *Nel v Le Roux NO* 1996 (1) SACR 572 (CC) 583g-h and Du Toit *et al Commentary on the Criminal Procedure Act* 23-52.

462 In *S v Nkosi* 1990 (1) SACR 509 (N), it was held that there was no reason in logic or fairness for depriving a witness facing an inquiry under section 189 of the Criminal Procedure Act of the right to legal representation afforded to an accused in terms of section 73 and the same reasoning should apply in the context of section 205. In *S v Bekisi* 1992 (1) SACR 39 (C), it was held that proceedings held under section 189 of the Criminal Procedure Act require an adherence to the rules of natural justice and that a witness is entitled both to legal representation and to a reasonable opportunity to prepare for the proceedings. A failure to explain to the witness her rights in this regard constitutes an irregularity which vitiates the

Once the judicial officer is satisfied that the person in question is likely to give the material information sought, it is her duty to authorise the subpoena. Thereupon it can be assumed, in the absence of evidence to the contrary, that the judicial officer issuing the subpoena exercised a proper discretion. It is then for the person subpoenaed to produce countervailing evidence which would require the judicial officer conducting the enquiry to decide whether the subpoena was validly authorised. The subpoena may be held void if it does not comply with the provisions of section 205. However, this may only be done on objectively determined grounds which do not depend on a value judgment.[463] If the judicial officer conducting the inquiry concludes that any of these jurisdictional facts were not present at the time of the issuing of the subpoena, such an order will be regarded as void *ab initio*.[464] Any attack on the validity of the subpoena that does not relate to these objective requirements would necessarily raise the issue of whether the judicial officer issuing the subpoena has exercised a proper judgement. This involves a review of the judgment of the functionary who issued the subpoena. This power can only be exercised by the High Court by virtue of its inherent powers.[465]

Section 19 of the RICPCIA provides that a judge or magistrate may issue an archived communication-related direction. Section 19(4) of the RICPCIA directs that a copy of both the application for, as well as the archived communication-related direction itself must be submitted to a designated judge.[466] If the archived communication-related direction constitutes part of a combined application in terms of section 18 of the RICPCIA, such a combined application must be considered by the designated judge.

Sections 39(3) and 40(3) of the RICPCIA do not require supervision by competent authorities. It is limited to the extent that a written application in terms of these sections may only be made for

---

proceedings. An unrepresented witness should furthermore be given an explanation of the import of the phrase "just excuse", as well as an opportunity to make a statement or adduce evidence on the basis of that explanation. See also Du Toit *et al Commentary on the Criminal Procedure Act* 23-53.

463 Examples of grounds which can be objectively determined include, the fact that the person who issued the subpoena was not a magistrate, regional court magistrate or a judge; the topic on which the witness is to be examined does not concern an offence known to the law; the subpoena was not issued at the request of a Director of Public Prosecutions; if the subpoena was issued upon the request of a public prosecutor, that prosecutor was not authorised to do so in writing by the Director of Public Prosecutions; or the judicial officer issuing the subpoena did not consider the application in that she signed the necessary authority for the subpoena while she was not *compos mentis* or in the mistaken belief that she was authorising some other kind of process. See *S v Matison* 1981 (3) SA 302 (A) 311 and 312H; *Haysom v Additional Magistrate, Cape Town, S v Haysom* 1979 (3) SA 155 (C) 159B-D and Du Toit *et al Commentary on the Criminal Procedure Act* 23-52C.

464 *S v Cornelissen; Cornelissen v Zeelie* NO 1994 (2) SACR 41 (W) 72-4.

465 The High Court's powers to set aside proceedings that amount to an abuse of process will only be exercised in exceptional cases, where it appears as a matter of certainty, and not only on a preponderance of probability, that the proceeding is obviously unsustainable (*Matisonn v Additional Magistrate, Cape Town* 1980 (2) SA 619 (C) 313G). Before a person can be convicted under section 189 for failing to give evidence in an enquiry under section 205 of the Criminal Procedure Act, the subpoena to attend must be issued for a motive authorised by section 205 and not for an ulterior motive which is not so authorised. If a prosecutor was granted a subpoena and thereafter sought to enforce it for a reason other than that sanctioned by section 205, then the subpoena itself would be invalid and its purported enforcement *ultra vires*. Examples of reviewable decisions include where the alleged motive of the judicial officer in issuing the subpoena did not relate to the investigation of an offence, but was simply part of an information gathering process on the part of law enforcement and where the principal purpose behind the enforcement of the subpoena had been the tracing of the victim, instead of the institution of a prosecution. See *Laurence v Verhoef NNO* 1993 (1) SACR 552 (W) and Du Toit *et al Commentary on the Criminal Procedure Act* 23-52C; 23-52D and 23-16B.

466 The Minister responsible for the administration of justice must designate a judge to perform the functions of a designated judge for the purposes of the RICPCIA (section 1 of the RICPCIA).

the purposes of making an application for the issuing of a direction. A telecommunications service provider must immediately comply with such a request, independent of further judicial supervision at this stage.

The National Director of Public Prosecutions[467] must authorise in writing the use of any information obtained under the provisions of the RICPCIA,[468] or any other similar Act in another country, as evidence in criminal or civil proceedings as contemplated in chapter 5 or 6 of the Prevention of Organised Crime Act.[469]

4.4.4.2 Proportionality

Sections 189[470] and 205 of the Criminal Procedure Act must be construed in such a way that their application does not unjustifiably infringe or threaten to infringe any of the examinee's fundamental rights.[471] If the answer to any question put to an examinee at an examination under section 205 would infringe or threaten to infringe any of the examinee's fundamental rights, this would constitute a just excuse for the purposes of section 189(1) unless the limitations clause applies.[472] In applying the limitations clause, regard must be had to both the rights asserted by the examinee and the State's interest in securing information necessary for the prosecution of crimes.[473] The provisions of section 205 were held to be as narrowly tailored as possible to meet the legitimate State interest of investigating and prosecuting crime.[474]

It would serve no purpose to try to define the circumstances which would amount to a just excuse, as each case has to be decided on its own merits, taking into account general principles.[475] A just excuse would arise if a witness were to find herself in a situation in which it

---

467 Or any member of the prosecuting authority authorised thereto in writing by the National Director of Public Prosecutions.

468 I.e. information obtained by means of any interception or the provision of any real-time or archived communication-related information.

469 Act 121 of 1998. See section 47(2) of the RICPCIA. Section 47(1) provides for the admissibility of information regarding the commission of any criminal offence, obtained by means of the provision of, *inter alia*, any archived communication-related information under the RICPCIA, or any similar Act in another country. Such archived communication-related information may be used in criminal or civil proceedings contemplated in chapter 5 or 6 of the Prevention of Organised Crime Act 121 of 1998. In terms of section 48 of the RICPCIA, a certificate signed by a designated judge, a judge of a High Court, a regional magistrate or a magistrate is, upon its mere production at criminal or civil proceedings, in terms of chapters 5 or 6 of the Prevention of Organised Crime Act *prima facie* proof that the judicial officer concerned received and considered such an application, issued such a direction and was familiar with the contents thereof.

470 Section 205(a) makes section 189 of the Criminal Procedure Act applicable to section 205 enquiries.

471 See *Nel v Le Roux NO* 1996 (1) SACR 572 (CC) 579f-g. In this case it was contended for various reasons that section 205 violated the rights to equality, privacy, freedom of speech and expression, the right of an accused person to a fair trial, to be presumed innocent, to remain silent, not to be detained without trial and the right against self-incrimination. In addition, Du Toit remarks that section 205 would seem, *prima facie,* to infringe on the right to administrative justice. Du Toit advances that decisions made by the judicial officer issuing the subpoena, without at least a proper judgment of the merits, are unacceptable (Du Toit *et al Commentary on the Criminal Procedure Act* 23-52C). In *S v Mahlangu* 2000 (1) SACR 565 (W), the Court dismissed an application by a prospective examinee for an order requiring the State to inform the applicant, prior to the section 205 proceedings, what information the State required from the applicant and also to furnish the applicant with information in the possession of the State.

472 *Nel v Le Roux NO* 1996 (1) SACR 572 (CC) 578-9.

473 Du Toit *et al Commentary on the Criminal Procedure Act* 23-52.

474 *Nel v Le Roux NO* 1996 (1) SACR 572 (CC).

475 *Attorney-General, Transvaal v Kader* 1991 (4) SA 727 (A). See also Skeen 1992 *SALJ* 587.

would be humanly intolerable to testify.[476] There may, however, be circumstances in which a just excuse may exist if it was not humanly intolerable to give evidence. In striking a balance between the public interest in receiving relevant testimony against the disadvantages which the witness was likely to suffer if she was to testify, the public interest should be afforded much more weight than the individual.[477] The mere fact that a person acts on legal advice and refuses to take the oath does not constitute a just excuse in terms of section 189(1).[478] The fear of incriminating a friend,[479] the fear of being regarded as a traitor,[480] the fear that the life of a witness will be in danger,[481] sympathy with the political ideas of an accused,[482] the loss of faith in one's ability to give evidence[483] and the claim of a privilege by a minister of the church[484] have so far been held not to constitute just excuses. A person who has been subjected to unlawful interrogation could not claim a just excuse, as equated with a legal excuse, for a failure to give evidence.[485] The onus on a preponderance of probabilities is on the witness claiming a just excuse where this is in dispute.[486] A witness must be called upon to furnish her reasons for refusal.[487] Section 189 is contravened if the witness refuses to testify even where no specific question has been put.[488] The fact that a just excuse did not exist when the witness first refused to testify does not mean that the witness is not entitled to rely on it later on.[489]

Before a witness is sentenced for a contravention of section 189, such a witness must be given a full and fair opportunity of being heard on the question of sentence.[490] Although proceedings under section 189 are not trials as such, the rules of natural justice must be complied with, otherwise the proceedings may be vitiated.[491] The witness must be afforded a reasonable opportunity to prepare for the proceedings and is entitled to legal representation. If the witness is unrepresented, the Court should explain the phrase "just excuse" to her. Section 189 does not prescribe the procedure to be followed. It is open to the witness to explain her attitude *viva voce* or by submitting a statement or by retaining a legal representative to apprise the Court of the reason for refusal. As the onus rests on the witness to establish a just excuse, she should be afforded some latitude and assistance by the Court in explaining herself. The Court enjoys a

---

476 See also the *dictum* in *S v Weinberg* 1966 (4) SA 660 (A) 665H-666A.
477 *R v Parker* 1966 (2) SA 56 (RA).
478 *Haysom v Additional Magistrate, Cape Town* 1979 (3) SA 155 (C).
479 *S v Carneson* 1962 (3) SA 437 (T); *Natal Law Society v N* 1985 (4) SA 115 (N).
480 *S v Govender* 1967 (2) SA 121 (N).
481 *S v Maduna* 1978 (2) SA 777 (D) and *S v Sithole* 1991 (4) SA 94 (W). Whilst remote possibilities of future reprisals do not amount to a just excuse for not giving evidence, a genuine fear of giving evidence because of the consequences may be relevant to sentence. The interests of society and justice require that a witness should give evidence even when afraid (*S v Moloto* 1991 (1) SACR 617 (T)).
482 *S v Molobi* 1976 (2) SA 301 (W).
483 *S v Maduna* 1978 (2) SA 777 (D).
484 *Smit v Van Niekerk NO* 1976 (4) SA 293 (A).
485 *S v Weinberg* 1966 (4) SA 660 (A).
486 *S v Leepile* 1990 (3) SA 988 (W).
487 *S v Seals* 1990 (1) SACR 38 (C).
488 *S v Mthenjane* 1979 (2) SA 105 (A).
489 *S v Leepile*1986 (2) SA 352 (W).
490 *S v Maluleke* 1993 (1) SACR 649 (T).
491 *S v Bekesi* 1992 (1) SACR 39 (C).

wide discretion in determining the procedure to be followed. Whatever procedure is followed, real justice must be done.[492] If, after imprisonment, the examinee becomes willing to testify, this would entitle her to instant release.

Archived communication-related information can only be obtained in respect of a very limited category of offences.[493] Although section 205 may be used to obtain the same information in respect of any offence, this may not be done on an ongoing basis.[494] A request for archived communication-related information, when combined with applications for other directions, must be authorised by the designated judge, as a combined application is considered a graver infringement than an application for archived communication-related information. Information may only be requested under sections 39(3) and 40(3) of the RICPCIA for the purposes of making applications for directions.

4.4.4.3 Third parties

There is no obligation to serve notice upon third parties in respect of information provided under section 205 of the Criminal Procedure Act. The section 205 examination may, in fact, be conducted in private at any place designated by the judicial officer concerned.[495]

Notwithstanding any other law, agreement or license, a telecommunications service provider must, at own cost, acquire, whether by purchasing or leasing, the facilities and devices determined in a directive referred to in section 30(2)(a) of the RICPCIA.[496] Any costs incurred by a telecommunications service provider under the RICPCIA in enabling a telecommunications service to be intercepted; and communication-related information to be stored, including the investment, technical, maintenance and operating costs and complying with section 28(1)(b)(i) and (2)(a), must be borne by that telecommunications service provider.[497]

Section 31 of the RICPCIA provides for compensation payable to a postal service provider, telecommunications service provider and decryption key holder. The Minister of Justice and Constitutional Development[498] must by notice[499] in the *Gazette* prescribe

---

492 *S v Diale* 1994 (1) SACR 221 (BG).
493 Section 19(4) of the RICPCIA. See paragraph 4.4.2.2 above for reference to these offences.
494 Section 15(2) of the RICPCIA.
495 Section 205(3) of the Criminal Procedure Act.
496 Section 30(4) which is subject to section 46(1)(a) of the RICPCIA.
497 Section 30(5) of the RICPCIA.
498 After consultation with the Cabinet members responsible for communications and national financial matters and the postal service providers or telecommunications service providers concerned, as the case may be.
499 In terms of section 31(4) of the RICPCIA, any such notice must be submitted to Parliament before publication thereof in the *Gazette*. In terms of section 31(1)(c), such a notice may at any time, in like manner, be amended or withdrawn. Section 31(1)(d) provides that the first such notice to be issued must be published in the *Gazette* within three months after the date of commencement of the RICPCIA.

(a) the forms of assistance in the execution of a direction for which a postal service provider, telecommunications service provider or decryption key holder must be compensated; and

(b) reasonable tariffs of compensation payable to a postal service provider, telecommunications service provider or decryption key holder for providing such prescribed forms of assistance.[500]

These tariffs may differ in respect of different categories of postal service providers, telecommunications service providers or decryption key holders. They must be uniform in respect of each postal service provider, telecommunications service provider or decryption key holder falling within the same category.[501] The compensation payable to a postal service provider, telecommunications service provider or decryption key holder in terms of this section is only for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance, as set out in section 31(1)(a)(ii) of the RICPCIA.[502]

The Minister of Justice and Constitutional Development may, upon application and in consultation with the relevant Ministers, exempt any Internet service provider from complying with section 30(4) of the RICPCIA in respect of the facilities and devices referred to in section 30(2)(a)(ii), for such a period and on such conditions as she determines.[503] Such conditions may include that an Internet service provider to whom an exemption has been granted must pay as an annual contribution to the Internet Service Providers Assistance Fund[504] an amount that the Minister determines in each case.[505] The Minister may grant such an exemption if she is satisfied that the Internet service provider concerned carries on such a small business that it cannot comply with section 30(4), that such an exemption is in the public interest; or that special circumstances exist which justify such exemption.[506] In addition, the Minister may also exempt telecommunications service providers, law enforcement agencies or any other person from the prohibition on the manufacture, possession and advertising of listed equipment to the extent that the purpose for which such listed equipment will be manufactured, assembled, possessed, sold, purchased or advertised is reasonably necessary.[507] Exemptions under section 46(1)(a) must be granted by issuing to the Internet service provider, telecommunications service provider

---

500 Section 31(1)(a) of the RICPCIA. The forms of assistance, in terms of section 31(2) of the RICPCIA, must include, in the case of a telecommunications service provider, making available a facility, device or telecommunication system; and/or decryption holder, the disclosure of a decryption key; and provision of decryption assistance.
501 Section 31(1)(b) of the RICPCIA.
502 Section 31(3) of the RICPCIA.
503 Section 46(1)(a) of the RICPCIA.
504 Established by section 38(1) of the RICPCIA.
505 Section 46(1)(b) of the RICPCIA.
506 Section 46(2) of the RICPCIA.
507 Section 46(2)(b), read with section 46(1)(a), of the RICPCIA.

or other person or law enforcement agency concerned, a certificate of exemption[508] in which her or its name and the scope, period and conditions of the exemption are specified.[509] If an exemption has been granted to an Internet service provider, that Internet service provider is subject to all the other applicable provisions of the RICPCIA. The law enforcement agency which made the application for the issuing of the direction addressed to such an Internet service provider must make available the necessary facilities and devices to execute that direction.[510]

4.4.4.4 Privileged categories of information

A witness must obey the subpoena issued under section 205 of the Criminal Procedure Act, take the oath when called upon and wait until a particular question is asked before claiming privilege.[511] A subpoena *duces tecum* may be issued by the defence in respect of a state witness who either has some degree of custody or control of the document to be produced.[512] However, where the document belongs to a third party, the witness cannot claim privilege.[513] The concept of a "just excuse" not to disclose information is not confined to lawful excuses, arising from the rules of privilege, compellability of witnesses or the admissibility of evidence.[514]

Section 205 of the Criminal Procedure Act is generally used to compel a person who refuses to make a statement to the law enforcement officer to furnish the required information under oath, unless she has a just excuse, permitted by law,[515] for her refusal.[516] A refusal to give evidence does not only arise from silence, but also from evidence or improper answers to questions.[517] What constitutes a "just excuse" must be interpreted subject to the provisions of the Constitution. A just excuse would include the privilege against self-incrimination.[518] However,

---

508 In terms of section 46(3)(b) of the RICPCIA, such a certificate of exemption must be published in the *Gazette* and becomes valid upon the date of such publication. Before she publishes such a certificate of exemption, the Minister of Justice and Constitutional Development must table the certificate in the National Assembly for approval. The National Assembly may reject a certificate within two months after it has been tabled, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within 14 days after the commencement of its next ensuing ordinary session. If the National Assembly rejects such a certificate, the Minister may table an amended certificate in the National Assembly. If the Minister tables an amended certificate and the National Assembly approves the amended certificate, the Minister must publish that certificate within one month of the National Assembly's approval; or reject the amended certificate within two months after it has been tabled, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within 14 days after the commencement of its next ensuing ordinary session, sections 46(4)(c) and (d) apply). If the National Assembly does not reject a certificate as contemplated in section 46(4)(b) or (d)(ii), such a certificate will be deemed to have been approved by the National Assembly; and the Minister must publish that certificate within one month thereafter. See sections 46(4)(a)-(e) and 46(5). A certificate of exemption may at any time in like manner be amended or withdrawn by the Minister (section 46(5)). An exemption lapses upon termination of the period for which it was granted; or withdrawal of the relevant certificate (section 46(6)).

509 Section 46(3)(a) of the RICPCIA.

510 Section 46(7) of the RICPCIA.

511 *R v Heard* 1937 CPD 401.

512 *R v Mkwayi* 1956 (3) SA 406 (E).

513 *Cave v Johannes NO* 1949 (1) SA 72 (T).

514 In *Attorney-General, Transvaal v Kader* 1991 (4) SA 727 (A) the Appellate Division held that the term "just excuse" even goes beyond matters of privilege, compellability and admissibility.

515 *S v Waite* 1978 (3) SA 896 (O) 898E-F.

516 Du Toit *et al Commentary on the Criminal Procedure Act* 23-51.

517 *R v Nani* 1930 EDL 12 and Du Toit *et al* Commentary on the Criminal Procedure Act 23-51.

518 Despite section 203 of the Criminal Procedure Act not being specifically included in the provisions listed as *per* section 205(2). The listing of section 204, however, would be meaningless without the inclusion of section 203. Du Toit *et al Commentary on the Criminal Procedure Act* 23-51. An accused who refuses to give evidence in other matters connected with a pending criminal case against her can probably raise a lawful excuse for not testifying (*S v Lunngile* 1999 (2) SACR 597 (SCA).

the circumstances of the case and the nature of the evidence that the witness is called to give will determine whether there are reasonable grounds underlying a witness's fear of self-incrimination.[519] The answers need not be directly incriminating.[520] The witness must be sworn in and can only claim the privilege in respect of individual questions.[521] Whether the witness has reasonable fears with regard to self-incrimination is a matter for the discretion of the Court.

Section 204 allows for immunity from prosecution if a witness answers frankly and honestly all questions put to her, including self-incriminating questions. The prosecutor must specify a particular offence in respect of which the indemnity is offered.[522] If this is done, the witness has no "just excuse" for a failure to answer.
Section 189 applies to all compellable witnesses and it appears that the only clearly demarcated privilege is that all witnesses are excused from answering self-incriminating questions in terms of section 203.[523]

The effect of section 204 is that persons criminally associated with the accused are compellable witnesses and that such witnesses are deprived of the privilege against self-incrimination in exchange for another valuable privilege in the form of a discharge from prosecution in respect of certain specified offences,[524] provided that she answers all questions frankly and honestly in the opinion of the Court. With regard to the limitations clause, it has been remarked that section 204 afforded a person under suspicion "a very fair and reasonable bargain".[525] A prosecutor, by specifying an offence with the intention of applying section 204, offers that a witness will be discharged from prosecution, but only under the circumstances and to the extent set out in section 204(2).[526] The prosecution has an unfettered discretion to specify offences in criminal proceedings and at enquiries conducted in terms of section 205.[527] Referring to an offence in a subpoena issued in terms of section 205 is merely to identify the topic on which information is sought,[528] but a prosecutor may, without the authority of the Director of Public Prosecutions,

---

519 *R v Boyes* (1861) 121 ER 730 738.
520 *S v Heyman* 1966 (4) SA 598 (A); *Rademeyer v Attorney-General* 1955 (1) SA 444 (T).
521 *Waddell v Eyles NO and Welsh NO* 1939 TPD 198.
522 *S v Waite* 1978 (3) SA 896 (O).
523 Du Toit *et al Commentary on the Criminal Procedure Act* 23-15.
524 Including offences in respect of which a verdict of guilty would be competent upon a charge relating to the specified offences (*S v Waite* 1978 (3) SA 896 (O) 898-9 and *S v Bosman* 1978 (3) SA 903 (O) 905B-C). If an offence is specified, the privilege may be invoked only in respect of another offence, not being a competent offence (*S v Waite* 899A-B). A charge may, in certain circumstances, also said to have been specified by implication (*S v Maunye* 2002 (1) SACR 266 (T) 273-4 and 175g-h). The prosecutor, however, need not always specify an offence *before* calling a witness, but she may also do so during the course of the giving of evidence by the witness, if it appears that the witness may incriminate herself. The prosecutor may then, on the strength of what the witness has told the Court, specify an offence in terms of section 204 (*S v Bosman, S v Kleinschmidt* 1980 (1) SA 852 (A) 856C-D).
525 *S v Maunye* 2002 (1) SACR 266 (T) 272-3.
526 *S v Waite* 1978 (3) SA 896 (O) 899D-E.
527 *S v Bosman, S v Kleinschmidt* 1979 (1) SA 277 (O) 280E-F.
528 *S v Waite* 1978 (3) SA 896 (O) 899H.

specify an offence other than one mentioned in the subpoena. It also does not, therefore, restrict the power of the prosecutor to specify an offence in terms of section 204(1).[529]

Before a person can be dealt with under section 204, the Court must be satisfied that she is a competent witness for the prosecution.[530] It is the duty of the Court to see to it that the offence specified by the prosecutor is duly placed on the record of the case.[531] Once the prosecutor has specified an offence, it is the duty of the Court to inform the witness of the four points set out in section 204(1)(a).[532] In *S v Maunye*,[533] the need for a proper explanation[534] of the position to an unrepresented accused and to an unrepresented witness who was a suspect was emphasised. The witness must be enabled to elect without misunderstanding whether to give evidence or not and must be put on her guard against possibly losing her immunity by giving unsatisfactory evidence.

The discharge is of no legal force or effect if it is given at preparatory examination proceedings and the witness concerned does not at any trial arising out of such preparatory examination, answer, in the opinion of the Court, frankly and honestly all questions put to her at such a trial by the prosecution, the accused or the Court.[535]

If the Court decides that the witness should be discharged, such a discharge should be given only after all the witnesses have testified and argument has been heard.[536] An earlier decision on this issue would constitute an irregularity. Whether such an irregularity constitutes a failure of justice depends on the facts of each case.[537] If the witness answers frankly and honestly all questions put to her, she acquires a right, or at least a legitimate expectation to be discharged, since the language in section 204(2)(a) is peremptory.[538] The witness is thus also entitled, in

---

529 *S v Matison* 1981 (3) SA 302 (A).

530 *S v Hendrix* 1979 (3) SA 816 (D) 818.

531 *S v Maunye* 2002 (1) SACR 266 (T) 274-5.

532 I.e. that she is obliged to give evidence at the proceedings in question; that questions may be put to her which may incriminate her with regard to the offence specified by the prosecutor; that she will be obliged to answer any question put to her, whether by the prosecution, the accused or the Court, notwithstanding that the answer may incriminate her with regard to the offence so specified or with regard to any offence in respect of which a verdict of guilty would be competent upon a charge relating to the offence so specified; that if she answers frankly and honestly all questions put to her, she shall be discharged from prosecution with regard to the offence so specified and with regard to any offence in respect of which a verdict of guilty would be competent upon a charge relating to the offence so specified.

533 2002 (1) SACR 266 (T) 279-80. On the facts of the case, it was held that the magistrate's failure to give any explanation of the effect of section 204 to the accused and to make a note of it on the record was an irregularity.

534 It constitutes an irregularity to warn the witness that she is required to answer all the questions put to her to the satisfaction of the Court, as such a warning may induce in the witness a belief that the Court will not be satisfied unless she implicates the accused (*S v Ncube* 1976 (1) SA 798 (RA)). She should be informed that she need only answer all questions frankly and honestly in order that she may be indemnified in terms of section 204(2)(a). A warning that the evidence to be given should be favourable to the State was also held to constitute an irregularity which was highly prejudicial to the interests of the unrepresented accused (*S v Mokoena* 2003 (1) SACR 74 (T)). A warning that the Court will have to be satisfied that the witness is reliable or credible is also not entirely satisfactory, for it fails to specify the criteria by which that standard is gauged (*S v Dlamini* 1978 (4) SA 917 (N) 919H).

535 Section 204(3) of the Criminal Procedure Act.

536 *S v Mnyamana* 1990 (1) SACR 137 (A), *S v Dlamini* 1978 (4) SA 917 (N) and *S v Mokoena* 2003 (1) SACR 74 (T) 78 para [10])).

537 *S v Lubbe* 1981 (2) SA 854 (C) and *R v McMillan* 1958 (4) SA 461 (A).

538 *Mahomed v Attorney-General of Natal* 998 (1) SACR 73 (N) 82h-i.

terms of the *audi alteram partem* principle, to a hearing before a decision may be made not to discharge her from prosecution.[539] The presiding officer can only make the decision whether or not to discharge a witness after giving judgment in the case in which the witness testified, although the witness's representations ought to be heard prior to judgment.[540] If the Court decides that the witness should not be discharged, her evidence cannot then be used against her in any subsequent proceedings.[541]

The Court in *Mahomed v Attorney-General of Natal (2)*[542] found, as to the nature of scope of the hearing to which the witness is entitled, that there was nothing unduly inequitable or unconstitutional about the concept of a limited right to a hearing in this context, since the accomplice stood to gain the substantial indulgence of a discharge from prosecution by merely performing the duties to be expected of an ordinary citizen.[543] It was also held that as to the nature of the decision-making process of the presiding officer in determining whether or not to grant the witness a discharge it was inappropriate to speak about an *onus* or particular degrees of proof. The words "in the opinion of the Court" indicated that the investigation was a subjective one and that a higher forum could not interfere with the presiding officer's decision on the basis of its own views. The fact that the presiding officer held a *bona fide* opinion which was not the result of any gross irregularity in the proceedings culminating in the formation of that opinion was all that was necessary for the purposes of section 204(2).[544]

4.4.4.5 Confidentiality

The section 205-examination may be conducted in private at any place designated by the judicial officer concerned.[545] The position of an examinee is also not the same as that of a witness in a trial, as the section 205-proceedings constitutes a preliminary stage in the proceedings, prior to the examinee possibly becoming a witness in the discretion of the State. An examinee has no right not to provide information. She has no basis for seeking any information from the State prior to the commencement of the inquiry. It is normally in the interests of the State to withhold secret information until it becomes necessary to disclose it. Section 32 of the Constitution is aimed at the protection of the rights of a party seeking

---

539 In *Mahomed v Attorney-General of Natal* 1998 (1) SACR 73 (N), the failure to give a witness a hearing was held to be a gross irregularity.

540 In *S v Kheswa* 1997 (2) SACR 638 (D), it was held that to only permit the witness to make representations after judgment would largely stultify the witness's right to be heard.

541 Section 204(4)(a) of the Criminal Procedure Act. Exceptions are provided for in, for example, prosecutions for perjury arising from the giving of that evidence.

542 1998 (1) SACR 73 (N).

543 *Mahomed v Attorney-General of Natal* 1998 (1) SACR 73 (N) 81.

544 *Mahomed v Attorney-General of Natal* 1998 (1) SACR 73 (N) 75, 82.

545 Section 205(3) of the Criminal Procedure Act.

information from the State, whilst an examinee is the one who is obliged to give evidence in terms of section 205.[546]

No person may disclose any information which she obtained in exercising her powers or performing her duties in terms of the RICPCIA, except

(a) to any other person who of necessity requires it for the performance of her functions in terms of the RICPCIA;

(b) if she is a person who of necessity supplies it in the performance of her functions in terms of the RICPCIA;

(c) if the information is required in terms of any law or as evidence in any court of law; or

(d) to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.[547]

This prohibition against the disclosure of confidential information under the RICPCIA includes information relating to the fact that

(a) a direction has been issued under the RICPCIA;

(b) a communication is being or has been or will probably be intercepted;

(c) real-time or archived communication-related information is being or has been or will probably be provided;

(d) a decryption key is being or has been or will probably be disclosed or that decryption assistance is being or has been or will probably be provided; and

(e) an interception device is being or has been or will probably be installed.[548]

No postal service provider, telecommunications service provider or decryption key holder may disclose any information that was obtained in exercising the powers or in performing her duties in terms of the RICPCIA. An employee of a postal service provider, telecommunications service provider or decryption key holder may not disclose any information that was obtained in the course of her employment and which is connected with exercising any power or performing any

---

546 Du Toit *et al Commentary on the Criminal Procedure Act* 23-52A. In *S v Mahlangu* 2000 (1) SACR 565 (W), the applicant had not even mentioned what specific rights he sought to protect, with reference to section 32 of the Constitution, and since he had been offered immunity in terms of sections 203 and 204 of the Criminal Procedure Act, he was only at risk under section 205 itself, should he refuse to disclose the relevant information asked of him without a just cause.

547 Section 42 of the RICPCIA.

548 Section 42(3) of the RICPCIA.

duty in terms of the RICPCIA.[549] The only exceptions to this general rule are those provided for in section 42(1).[550]

Any authorised person who executes a direction or assists with the execution thereof and who has obtained information in respect of such a direction[551] may, however, disclose such information to another law enforcement officer. The disclosure of such information is only allowed to the extent necessary for the proper performance of the official duties of the authorised person making or the law enforcement officer receiving the disclosure. The information may be used only to the extent that such use is necessary for the proper performance of official duties.[552]

4.4.4.6 Discretionary conditions

In terms of section 19(5)(d) of the RICPCIA, an archived communication-related direction may also specify conditions or restrictions relating to the provision of archived communication-related information authorised therein.

4.4.4.7 Consequences of unlawful action taken

Section 51 of the RICPCIA creates a number of offences with regard to exercising the powers relevant to the provision, *inter alia*, of communication-related information under the RICPCIA. These offences include

(a) contravening or failing to comply with sections 29(8), 40(1)-(3), 42(1) or 45(1) of the RICPCIA;

(b) furnishing information or making a statement in any application made in terms of the RICPCIA, knowing such information or statement to be false, incorrect or misleading or not believing it to be correct;

(c) acting in a manner that is contrary to the authority of any direction issued under the RICPCIA or proceeding to act under any such direction knowing that it has expired;

(d) forging or, with the intent to deceive, altering or tampering with any direction or entry warrant issued under the RICPCIA;

---

549 Whether that employee is involved in exercising that power or performing that duty or not.
550 Section 42(2) of the RICPCIA.
551 Including the contents of any communications intercepted under that direction, or evidence derived therefrom or real-time or archived communication-related information provided under that direction.
552 Section 43 of the RICPCIA.

(e) furnishing particulars or information in any affidavit or report referred to in the RICPCIA, knowing such particulars or information to be false, incorrect or misleading or not believing it to be correct; and

(f) obstructing, hindering or interfering with an authorised person who executes any direction or entry warrant issued under the RICPCIA or assists with the execution thereof.

These offences are sanctioned by a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.[553] Section 54 criminalises certain unlawful acts in respect of telecommunications and other equipment and carries the same sentence.[554]

Any telecommunications service provider or employee of a telecommunications service provider who intentionally provides or attempts to provide any real-time or archived communication-related information to any person other than the customer of the telecommunications service provider concerned to whom such real-time or archived communication-related information relates is guilty of an offence.[555] Any telecommunications service provider or employee of a telecommunications service provider who contravenes or fails to comply with section 28(2), 30(1), 39(4); contravenes or fails to comply with section 30(4); 39(1) or (2) or 42(2); or performs an act contemplated in section 51(1)(a)(iii) or (vii) of the RICPCIA is guilty of an offence. Any telecommunications service provider or employee of a telecommunications service provider who is convicted of any of these offences is liable to

(a) a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years, in the case of a telecommunications service provider who is a natural person; or

(b) a fine not exceeding R5 000 000 in the case of a juristic person; or

(c) a fine not exceeding R2 000 000 or imprisonment not exceeding 10 years in the case of an employee.

Section 50(1), which criminalizes the unlawful provision of real-time or archived communication-related information, carries the same sentences.[556]

---

553 Section 51(1)(a) of the RICPCIA.

554 Section 54(1) of the RICPCIA. Any person who, intentionally and unlawfully, in any manner modifies, tampers with, alters, reconfigures or interferes with, any telecommunication equipment, including a cellular phone and a SIM-card, or any part thereof; reverse engineers, decompiles, disassembles or interferes with the software installed on any telecommunication equipment, including a cellular phone and a SIM-card, by the manufacturer thereof; or allows any other person to perform any of the said acts, is guilty of an offence (section 54(2)). Any person who, intentionally and unlawfully, in any manner modifies, tampers with or interferes with, any interception or monitoring equipment, device or apparatus installed or utilised in terms of the RICPCIA; or allows any other person to perform any of the said acts, is guilty of an offence.

555 Section 50(1) of the RICPCIA. This, of course, does not apply to the provision of real-time or archived communication-related information as contemplated in sections 13, 14 and 15 (section 50(2)).

556 Section 51(3) of the RICPCIA.

A conviction of an offence referred to in section 51(3)(a)(i) or (ii) does not relieve any telecommunications service provider or any employee of such a telecommunications service provider of the obligation to comply with section 28(2), 30(1) or (4) or 39(4).[557]

Notwithstanding anything to the contrary in any other law contained, a magistrate's Court may impose any penalty provided for in the RICPCIA.[558] However, no person who in good faith assists an authorised person with the execution of a direction and believes on reasonable grounds that such authorised person is acting in accordance with such a direction, is liable to prosecution for a contravention of the RICPCIA.[559]

4.5 Transborder production orders in computing environments

The transborder production of information is to be facilitated within the general framework of South African mutual legal assistance, as provided for in, *inter alia*, the International Cooperation in Criminal Matters Act.[560] Foreign requests to South Africa, as the requested state, for the production of information are generally provided for in section 7 of the International Cooperation in Criminal Matters Act. Similarly, foreign requests from South Africa, as the requesting state, are provided for in section 2 of the International Cooperation in Criminal Matters Act.

Section 19(4)(d) of the RICPCIA[561] pertinently provides that an application for an archived communication-related direction may be made, *inter alia*, on the grounds that

> the making [of] a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in
>
> (i)
>
> accordance with an international mutual assistance agreement, or
>
> (ii)
>
> the interests of the Republic's international relations or obligations; ...

---

557 Section 51(5) of the RICPCIA.
558 Section 51(6) of the RICPCIA.
559 Section 51(7) of the RICPCIA.
560 See generally paragraph 4.3 above for a discussion of the transborder search and seizure in the South African mutual legal assistance framework. These provisions (excluding paragraph 4.3.1.5 that deals with search and seizure specific mutual legal assistance) are *ipso facto* applicable to the facilitation of the transborder production of required information.
561 Section 17(4)(d) contains a similarly worded provision in respect of the application for and issuing of real-time communication-related directions.

To the extent that an argument is made that section 19(4)(d) of the RICPCIA could be relied upon to facilitate direct[562] cooperation between countries, the dualism regarding the facilitation of mutual searches and seizures[563] also applies to the provision of archived communication-related information. Section 205 of the Criminal Procedure Act, however, does not make provision for international requests and section 7 of the International Cooperation in Criminal Matters is accordingly the only appropriate mutual assistance vehicle.

4.6 *Domestic preservation and partial disclosure provisional measures in computing environments*

No specific provision for the expedited preservation of stored computer data exists in the current South African criminal[564] procedural legislative framework. Preservation of stored computer data must accordingly be accomplished by means of the traditional search and seizure and production mechanisms.[565]

The position regarding the expedited preservation of traffic data must be considered in the context of section 30 of the RICPCIA that provides for the obligatory storing of communication-related information for a period not less than three years and not more than five years.[566] The default effect of this provision is that certain specified categories of communication-related information are available for the specified period. Although this study is concerned with stored, as opposed to real-time, data, section 1 of the RICPCIA provides that real-time communication-related information means communication-related information which is immediately available to a telecommunications service provider before, during or for a period of 90 days after the transmission of an indirect communication. This 90-day period, to some extent, obscures the

---

562 As opposed to making use of section 7 of the International Cooperation in Criminal Matters Act.

563 See paragraph 4.3.1.5 above.

564 Preservation may, however, be accomplished by an Anton Pillar order. This may become relevant in a law enforcement context, for example, when a private investigation has been conducted with regard to the alleged offences. The need to attach and preserve evidence for trial purposes has grown to such an extent that Anton Pillar orders are used, not only in the various branches of intellectual property law, but in general. An Anton Pillar order consists of a type of "search warrant" applied for *ex parte* and usually *in camera*. It is often used in computer-related cases where the electronically stored evidence might "disappear" at the slightest hint of trouble. Thus, instead of founding jurisdiction, an Anton Pillar order actually founds the proof of a case (see *Shoba v Officer Commanding, Temporary Police Camp, Wagendrift Dam; Maphanga v Officer Commanding, South African Police Murder & Robbery Unit Pietermaritzburg* 1995 (4) SA 1 (A)). The Appellate Division now seems to have settled that this type of order does have a place in the South African legal system and can be used to preserve fragile evidence, as would typically be the case with computer data. To obtain an Anton Pillar order, an applicant must *prima facie* establish, firstly, that the applicant has a cause of action against the respondent which she intends to pursue. Secondly, that the respondent has in her possession specific (and specified) documents or things which constitute vital evidence in substantiation of the applicant's cause of action (but in respect of which the applicant cannot claim a real or personal right). There must, lastly, be a real and well-founded apprehension that this evidence may be hidden or destroyed or in some manner be spirited away before discovery or by the time the case comes to trial. The Court has a discretion whether or not to grant an Anton Pillar order and, if it does, on what terms. In exercising its discretion, the Court will take into account the cogency of the case made out by the applicant and, with reference to the requisites for the order, must weigh the potential harm that will be suffered by the respondent if the order is granted against the potential harm to the applicant if the relief is withheld. The order granted should not be more onerous than is necessary to protect the applicant's interests. Courts should be careful to ensure that the Anton Pillar procedure is not used indiscriminately or as an instrument to harass defendants. To prevent abuse, the Court should insist on safeguards. See Van der Merwe *Computers and the Law* (2nd ed) 262.

565 See paragraphs 4.2 and 4.4 above.

566 The directives in respect of different categories of telecommunications service providers (i.e. fixed line operators, mobile cellular operators and Internet Service Providers) made in terms of the RICPCIA has been published in the Government Gazette 28 November 2005 No 28271 3 by General Notice 1325 of 2005. Copies are also available on the Internet http://www.info.gov.za/gazette/notices/2005/28271.pdf. See also footnote 419 in paragraph 4.4.2.2 above.

meaning of stored computer data as *per* the Cybercrime Convention.[567] Section 17 and 23 of the RICPCIA could therefore also be used to facilitate the expedited partial disclosure of traffic data.

The measures provided for in sections 17 and 19 of the RICPCIA[568] do not preclude obtaining such information in respect of any person in accordance with alternative procedures prescribed in any other act. Any real-time or archived communication-related information which is obtained in terms of such other acts may, however, not be obtained on an ongoing basis.[569] Section 205 of the Criminal Procedure Act can facilitate access to communication-related information relevant to all categories of offences, while the provisions of the RICPCIA are limited to a small number of serious offences.

4.7 Transborder preservation and partial disclosure provisional measures in computing environments

The position is similar to that of the transborder production of information.[570]

4.8 Brouter[571] to chapter 5

In this chapter, an exposition of the current South African domestic and international search and seizure, production and preservation procedural mechanisms was provided. This was done to facilitate a comparative analysis between the catalogue of criminal procedural search and seizure, production and preservation devices proposed by the Cybercrime Convention compared to those devices available within the current South African legislative framework. It is not considered necessary to summarise the South African *status quo*, as set out in this chapter, as an objective in itself. The main objective of this study is to consider whether the South African search and seizure, production and preservation mechanisms, when directed at electronic evidence, need to be augmented and/or aligned in accordance with those set out in the Cybercrime Convention. The findings and recommendations relevant to this main objective are listed in chapter 7.

In considering any alignments and/or augmentations required in respect of the South African search and seizure, production and preservation mechanisms, the application of the equivalent domestic search and seizure, production and preservation mechanisms directed at electronic

---

567 See paragraph 2.4.1 above with regard to the definition of real-time communication-related information that, to some extent, obscures the meaning of stored (as opposed to real-time) computer data given in the Cybercrime Convention. See also paragraph 2.4.4. above in respect of data preservation and the extent to which data retention in terms of section 30 of the RICPCIA addresses this requirement.

568 Sections 17 and 19 of RICPCIA provides for the application for, and issuing of, real-time communication-related and archived communication-related directions, respectively.

569 Section 15(2) of the RICPCIA.

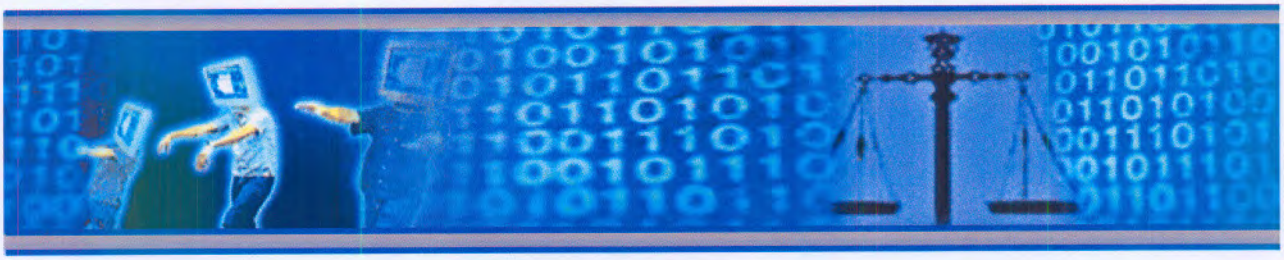
570 See paragraph 4.5 above in respect of the transborder production of information.

571 See chapter 7 for a list of the findings extracted from the contents of chapter 4.

evidence used in the United States and England are now considered in chapters 5 and 6 respectively.[572] This is of particular importance in view of the fact that so far there has been only one South African case[573] where the actual procedure employed to collect electronic evidence has been challenged. Precedents regarding the practical deployment and application not only of search and seizure, but also of production and preservation measures may prove useful to South African law enforcement and legal practitioners.

572 The rationale for choosing these two legal systems is set out in paragraph 1.3 above.
573 *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C).

CHAPTER 5:
A SNAPSHOT OF TROUBLESHOOTING @ THE UNITED STATES



5.1 BIOS BITS AND BYTES 243

5.2 DOMESTIC SEARCH AND SEIZURE OF E-EVIDENCE 246

5.2.1 Root domain 246
5.2.2 Right to privacy 247
5.2.3 Search and seizure of e-evidence with a warrant 251
5.2.3.1 Particularity and specificity 251
5.2.3.2 Judicial supervision 256
5.2.3.3 Probable cause requirement 257
5.2.3.4 The quest for an *e*-evidence search strategy 259
5.2.4 Search and seizure of e-evidence without a warrant 271
5.2.4.1 Warrantless search and seizure doctrines 272

5.3 DOMESTIC PRODUCTION DEVICES 290

5.3.1 Backgound 290
5.3.2 Categories of service providers 293
5.3.2.1 Electronic communication service 293
5.3.2.2 Electronic storage 294
5.3.2.3 Remote computing service 295
5.3.3 Information categories 296
5.3.3.1 Basic subscriber information 296
5.3.3.2 Records or other information pertaining to a customer or subscriber to such a service 297
5.3.3.3 Contents 297
5.3.4 Different production devices 298
5.3.4.1 Compelled disclosure 299
5.3.4.2 Voluntary disclosure 305

5.4 DOMESTIC PRESERVATION DEVICES 306

5.4.1 Background 306
5.4.1.1 Section 2703(f) preservation orders 307
5.4.1.2 Section 2705(b) order not to disclose the existence of a warrant, subpoena or court order 308

5.5 BROUTER TO CHAPTER 6 308

5.1 BIOS bits and bytes[1]

The main objective of this research is to consider whether the South African search and seizure, production and preservation measures in respect of electronic evidence need to be augmented and/or aligned in accordance with the measures set out in the Cybercrime Convention. The technicalities and terminology underpinning these collection devices were explained in chapter 2 to prepare the reader for a comparatve analysis of these devices.[2] Next, an exposition of the domestic and transborder search and seizure, production and preservation mechanisms proposed in the Cybercrime Convention was given as a benchmark against which to compare the South African, United States and English measures.[3] An exposition of the South African search and seizure, production and preservation devices was then given.[4] The findings and recommendations extracted from the comparative analysis between the existing South African search and seizure, production and preservation mechanisms compared to those proposed in the Cybercrime Convention are listed in chapter 7. In considering any alignments and/or augmentations required in respect of the South African search and seizure, production and preservation mechanisms, the application of the equivalent domestic[5] search and seizure, production and preservation mechanisms directed at electronic evidence used in the United States and England[6] are now considered in chapters 5 and 6 respectively.

This chapter is aimed at providing a snapshot of the domestic search and seizure, production and preservation mechanisms available in the legal framework of the United States. The primary reason for benchmarking South African mechanisms against the procedural mechanisms available in the legal framework of the Unites States is to illustrate the ways in which these mechanisms are applied to electronic evidence. Such foreign mechanisms must, however, be considered in the context of the broader legislative frameworks from which they emanate. This chapter is accordingly aimed at enabling a contextually comparative troubleshooting utility[7] in respect of the application of these procedural mechanisms to electronic evidence in South Africa. This is of particular importance in view of the fact that so

---

1 In this heading, BIOS means some introductory bits and pieces with which to contextualise the primary sources of preservation, production and search and seizure mechanisms in the law of the United States. It also broadly contextualises the relevance of this chapter within the overarching framework of this thesis. See footnote 1 of paragraph 3.1 above for a technical definition of the term "BIOS".

2 See chapter 2 of this thesis.

3 See chapter 3 of this thesis.

4 See chapter 4 of this thesis.

5 Although both the domestic and transborder procedural mechanisms available in the South African legal framework and those proposed in the Cybercrime Convention were investigated in chapters 3 and 4 respectively, only the domestic procedural mechanisms available in the United States and England are considered in chapters 5 and 6 respectively. An attempt also to incorporate the transborder mechanisms, from a comparative perspective, would have rendered the scope of this thesis too extensive. See footnote 109 in paragraph 1.2 above.

6 The rationale for choosing the legal systems of the United States and England for comparative purposes is set out in paragraph 1.3 above.

7 See footnote 125 in paragraph 1.3 above for a definition of the term "utility" and "troubleshooting". In this context, a troubleshooting utility involves the comparative consideration of the application of search and seizure, production and preservation devices in the United States to electronic evidence in order to consider its equivalent application to the South African legislative context.

far there has been only one South African case[8] where the actual procedure employed to collect electronic evidence has been challenged. Precedents regarding the practical deployment and application, not only of search and seizure, but also of production and preservation measures, may prove useful to South African law enforcement agents and legal practitioners.

The law governing the preservation, production and search and seizure of electronic evidence[9] in the United States evolved from two primary sources. The first of these is the Fourth Amendment to the United States Constitution,[10] which states the following:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Rule 41 of the Federal Rules of Criminal Procedure, in conjunction with sections 3101 to 3118 of Title 18 of the United States Code Collection,[11] addresses criminal procedural search and seizure interventions generally applicable throughout the United States, without modifying any statute regulating search, seizure or the issuance and execution of a search warrant in special circumstances.[12] A look-and-feel[13] of search and seizures under authority of a search warrant[14] and a drilldown[15] of the warrantless search and seizure exceptions[16] are provided below.

---

8 *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C).

9 Although the interception and monitoring of electronic evidence does not resort within the research parameters, it is useful to note that, in the United States, interception and monitoring is governed by the Pen Register and Trap and Trace Devices Statute codified in chapter 206, sections 3121-3127 of Title 18 of the United States Code Collection and the Electronic Communications Privacy Act of 1986 codified in chapter 119, sections 2510-2522 of Title 18 of the United States Code Collection (commonly referred to as "Title III" in recognition of its original name, i.e. "Title III of the Omnibus Crime Control and Safe Streets Act of 1968"). The Electronic Communications and Privacy Act has two parts: Title I is an amendment to the wiretap provisions and deals with the interception of transmission and Title II deals with access to stored electronic communications. See also USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 5.

10 The United States Constitution became the cornerstone of the United States legal system on 4 March 1789. It includes a preamble, a main body of text and 26 amendments. The first 10 amendments to the United States Constitution are collectively called the Bill of Rights and were added in 1791 in order to address individual rights and liberties. The United States Constitution is the oldest written constitution still in use in the world and has only been added to and/or changed 26 times in 200 years. See Cullop *The Constitution of the United States* vi. In article 1, section 8, the United States Constitution grants the House and Senate the power to make any laws necessary and proper for seeing that the powers given to Congress, to the United States government, and to any department or officer of the United States government are carried out. The United States Constitution lays out what powers are given to state and local law governments and what powers fall under federal jurisdiction. State constitutions give the same power to state legislatures. However, federal laws always have precedence over state laws as a result of the supremacy clause in article VI of the United States Constitution.

11 Hereinafter referred to as 18 USC.

12 Rule 41(a)(1) of the Federal Rules of Criminal Procedure.

13 The "look-and-feel" of a product refers to the general appearance and operation of the junction between a user and a computer program, called the user interface. This is an unresolved and hotly debated legal issue because some software companies claim that competitors who copy the look-and-feel of their products are infringing on their copyright protection. See Webopedia "Look-and-feel" found on the Internet http://www.webopedia.com/TERM/l/look_and_deel.html 1 and Webopedia "User Interface" found on the Internet http://www.webopedia.com/TERM/U/user_interface.html 1. In this context, it is meant to indicate that the reader is provided with a broad overview of the warrant-based search and seizure enabling legislative provisions.

14 See paragraph 5.2.3 below with regard to search and seizure under the authority of a search warrant.

15 A "drilldown" as currently used in information technology is the act of focusing in on something, such as warrantless searches and seizures within the United States legislative framework in this context. The term is sometimes used when referring to moving down a hierarchy of folders and files in a file system like Windows. It may also mean clicking through a series of dropdown menus in a graphical user interface (GIU). See SearchSQLServer.com "Drilldown" found on the Internet http://searchsqlserver.techtaget.com/sDefinition/0,290660,sid87_gci212001,00.html 1.

16 See paragraph 5.2.4 below in respect of the warrantless search and seizure doctrines.

The second primary source of production, preservation and search and seizure law is the statutory privacy laws codified in sections 2701 to 2712 of 18 USC, which governs how stored account records, subscriber information and contents can be obtained from network service providers, including Internet service providers, telephone companies, cellular phone providers and satellite services.[17] These statutory protections exist to protect the general privacy of electronic communications stored remotely with service providers and to protect the privacy of Internet users when the Fourth Amendment may not. The Electronic Communications Privacy Act[18] permits law enforcement to obtain and/or to preserve certain categories of information with less process than a traditional search warrant,[19] examples of which include an articulable facts court order that provides access to transactional records and a subpoena that is aimed at basic subscriber information. A special type of search warrant served on service providers is also provided for.[20] Subject to certain restrictions, the Electronic Communications Privacy Act now allows providers of services that are not available to the public freely to disclose both contents and other records relating to stored communications.

---

17 Commonly referred to as the stored communications portion of the Electronic Communications Privacy Act of 1986. The USA PATRIOT Act of 2001 clarified and updated these statutory privacy laws in light of modern technologies and in several respects eased restrictions on law enforcement access to stored communications. President Bush has signed legislation to renew the USA PATRIOT Act making permanent several sunsetting provisions, extending sections 206 and 215 of the USA PATRIOT Act until 2009 and incorporating a number of new rights protections (specifically in respect of National Security Letters). Two separate, but related bills were approved, namely the USA PATRIOT Improvement and Reauthorisation Act of 2005 and the USA PATRIOT Act Additional Reauthorising Amendments Act of 2006. See Shawl "Breaking News – Bush Signs Partriot Act Renewal" found on the Internet http://www.jurist.law.pitt.edu/paperchase/2006/03/breking-news-bush-signs-patriot-act.php 1. URLs to copies of the two related Acts can also be found on this website. See also paragraph 1.1 above for a general reference to the anti-terrorism drives in the United States, England and South Africa. In the aftermath of 9/11, a series of laws was passed in the United States designed to assist law enforcement agencies to combat terrorism by expanding the government's access to electronic data in Cyberspace. The United States Congress introduced several provisions in the USA PATRIOT Act, which, for example, expands the list of identifying records that law enforcement may obtain with a subpoena (section 210 of the USA PATRIOT ACT), and permits an Internet Service Provider to give "voluntary consent" to disclosing its customers' communication records during an emergency (section 212 of the USA PATRIOT Act provides an exemption from civil liability to service providers that make "voluntary disclosures" of content and non-content communication records in emergencies). See Aldesco "Notes and Comments – The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime" found on the Internet http://elr.lls.edu/issues/v23-issue1/aldesco.pdf 87. While these measures differ from the Cybercrime Convention's broader provisions concerning the expedited preservation of data, they represent a similar legislative push to track communication data and Internet use for policing purposes. See Scheeres "EU Law Turns ISPs Into Spies?" found on the Internet http://www.wired.com/news/politics/0,1283,52829,00.html 2. Ironically, the lives of ordinary Americans who are not suspected of having ties to terrorism will be affected by the government's expanded definition of "cyberterrorism" (section 814 of the USA PATRIOT Act). Kerr, however, argues that "the common wisdom on the USA PATRIOT Act is incorrect and that it did not expand law enforcement powers dramatically, as its critics have alleged. He submits that the USA PATRIOT Act made "mostly minor amendments" and many of the amendments merely codified pre-existing law. He argues that several of the most controversial amendments may actually increase privacy protections, rather than decrease them. See Kerr 2003 *Northwestern University Law Review* 608. Lyon contends that surveillance "before and after 9/11" has manifestly not changed. He opines that today's surveillance is increasingly computer-assisted and technology-dependant, meaning that the reinforcement and reproduction of social inequalities are being automated. In the current climate in the United States, he argues that "it is hard to see how calls for democratic accountability and ethical scrutiny of surveillance systems will be heard as anything but liberal whining". Lyon *Surveillance after September 11* 39.

18 Of 1986 (hereinafter referred to as the Electronic Communications Privacy Act) and codified at sections 2701 – 2712 of 18 USC.

19 See generally paragraph 5.3 below for a reference to these devices provided for in the Electronic Communications and Privacy Act.

20 Although the mechanism created under section 2703(a) of 18 UCS is termed a (full) search warrant (see the USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 68-69) the terminology may be open to some debate, as this mechanism is not deemed to be a traditional search warrant under Rule 41 of the Federal Rules of Criminal Procedure. Although the term search warrant will be retained, this production device is discussed in paragraph 5.3.4 below.

5.2 Domestic search and seizure of e-evidence

5.2.1 Root domain[21]

The warrant was always a contentious instrument in the North American colonies, and its oppressive historical reputation led to constitutional conflict in pre-1870 America during the seventeenth and eighteenth centuries. The constitution of the newly independent American state was formed in the context of revolt against executive powers contained in general "writs of assistance". These "writs of assistance" had no real judicial origin but allowed the Act of Frauds of 1662 to be enforced by conferring virtually unfettered powers of search on customs officials. Resistance to the writ and to the customs regime that it supported was a vital part in the sequence of events that culminated in the 1688 Revolution. It has also been pointed out that, even after 1688, when a judge issued a warrant, it was greeted with foreboding.[22] It is not surprising then that express restrictions on the issue of warrants and upon powers of search appear in the Constitution of the United States. The fundamental requirements of reasonableness, particularity, probable cause and judicial control are seen as safeguarding a citizen's interests.[23]

The arguments surrounding the legitimacy of the warrant procedure have significantly shaped the constitutional history of the United States. The eventual outcome of these conflicts was that strict constraints were imposed upon the circumstances in which a warrant might be issued, and the issuance itself is required to be a judicial act.[24] Because of the fetters placed upon the granting of warrants, the warrant procedure became a due process safeguard rather than a coercive means of obtaining incriminating evidence through an exceptional intrusion into a person's privacy.[25] This theory is most evident in the rhetoric of the United States Supreme Court in *Coolidge v New Hampshire*[26] where it was stated that, as a general proposition, warrantless searches were unreasonable, subject to a few specifically established and well delineated exceptions. There has been an entrenched protection against unreasonable searches in the United States for two centuries. The United States Supreme Court has also recognised for over 40 years that the protection against unreasonable searches and seizures is not limited to tangible things, but extends to intangibles such as spoken words.[27]

---

21 The root domain is the starting point of the top level domain structure on the Internet. It is the root, or entry point, to the .com, .org, .net and other domains. See footnote 447 in paragraph 2.6.3 above in respect of domain names. In this context "root domain" is meant to refer to the historical origins of the power of search and seizure in the United States.

22 Sharpe *Search and Surveillance* 3.

23 Sharpe *Search and Surveillance* 4.

24 Sharpe *Search and Surveillance* 48.

25 As opposed to the theory traditionally subscribed to by English judges that warrants are coercive instruments and that they must therefore be limited to those situations that have been expressly set out in a statute, as a result of democratic process. See paragraph 6.2.1 below for a discussion of the historical origins of search warrants in England.

26 403 US 443 (1970).

27 See *US v On Lee* 343 US 757 (1952) and Sharpe *Search and Surveillance* 6. A considerable jurisprudence has developed with regard to the reconciliation of what has been referred to as "electronic searches" with the Fourth Amendment. The fact that something happens to be stored in digital form does not make it any less subject to the Fourth Amendment protection

5.2.2 Right to privacy

Privacy is undoubtedly a broad and nebulous concept and the meanings accrued to it vary in different contexts and between jurisdictions. In the United States, the concept of privacy has been built on the broad assertion of "a right to be let alone".[28] Despite the fact that the United States Bill of Rights at no point mentions a constitutional "right to privacy", a substantial jurisprudence recognising the concept has developed.[29] The right to privacy is also considered an implicit part of several of the provisions of the Bill of Rights, including the First,[30] Fourth[31] and Ninth[32] Amendments, supported by the due process provisions of the Fifth[33] and Fourteenth[34] Amendments.[35]

In the United States, the single most significant decision is the case of *Katz v United States*,[36] which firmly overturned earlier authority[37] by viewing the protection from unreasonable search

---

against unreasonable searches and seizures. In fact, searches involving computers exacerbate the invasion of the privacy of innocent documents inherent in most document searches. See Adair and David 2001 *Federal Probation* 66.

28 Stone *The Law of Entry, Search, and Seizure* 4.

29 Some of these cases are referred to in this paragraph.

30 The First Amendment to the United States Constitution reads: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of people peaceably to assemble, and to petition the Government for a redress of grievances".

31 The Fourth Amendment is specifically concerned with prohibiting unreasonable searches. See a quotation of the text of the Fourth Amendment in paragraph 5.1 above. Evidence seized in violation of Fourth Amendment cannot be used against the defendant in a criminal prosecution. This doctrine is known as the "exclusionary rule" and such evidence is referred to as the "fruits of a poisonous tree". It requires suppression of evidence obtained from constitutional violations. See Freeman 2003 *Information Systems Security* 6 and Haberle 1996 *Seton Hall Law Review* 866-896. Because computers have the capacity to store massive amounts of information, there is a very real danger that information obtained from an unconstitutional seizure of a computer will lead law enforcement agencies to evidence that would have remained undiscovered but for the search of the computer. If, therefore, a Fourth Amendment violation can be proved, some or all subsequently obtained evidence may accordingly be excluded as "fruits of the poisonous tree". See Rhoden 2002 *American Journal of Criminal Law* 128. In the United States, suppression of evidence is achieved by an automatic exclusionary rule. However, this rule is subject to judicial determination as to its applicability to the facts of any particular case, and, in respect of search, to common law and statutory exceptions in respect of the warrant requirement (see Sharpe *Search and Surveillance* 56). The current exceptions to the exclusionary rule include the following: the impeachment exception, the independent source exception, the inevitable discovery exception, the good faith exception, the harmless error exception and the rule of attenuation. For a discussion of these exceptions see Jackson 1996 *The Journal of Criminal Law & Criminology* 1201-1227.

32 The Ninth Amendment to the United States Constitution reads: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people".

33 The Fifth Amendment of the United States Constitution reads: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

34 The Fourteenth Amendment consists of 5 sections. It was primarily concerned with the details of reintegrating the southern states after the 1861 Civil War and defining some of the rights of recently freed slaves. The first section of the amendment, however, was aimed at revolutionising federalism. It states that no state could "deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws". Gradually, the United States Supreme Court interpreted the amendment to mean that the guarantees of the Bill of Rights apply to the states as well as the national government. The Fourteenth Amendment has the effect of subjecting all state organs to the Fourth Amendment. See *Mapp v Ohio* 367 US 643 (1961).

35 Stone *The Law of Entry, Search, and Seizure* 4.

36 389 US 347 (1967). It has been argued that the application of *Katz v United States* to new technology is simultaneously normative and descriptive. In determining reasonable expectations of privacy, the level of privacy that the Constitution protects cannot be divorced from a judgment about how much privacy society ought to protect. The Fourth Amendment needs to balance the individual's claim to privacy against the societal demands for effective law enforcement (see 1997 *Harvard Law Review* 1607). Reetz opines that an analysis of the Fourth Amendment expectation of privacy is difficult, as society has not yet had time to assess the reasonableness of expectations of privacy in computerized information. He advances that sound results will generally be reached by remembering that the Fourth Amendment protects people; only individuals, and not machines, can "disclose" information or "consent" to searches. Only by according due weight to the privacy expectations of computer users and the reasonable methods of protecting those expectations will an appropriate balance be struck between the individual's need for privacy and the government's need for access to information. See Reetz 1987 *Boston University Law Review* 211-212. Johnson gives an extensive overview of pre- and post-*Katz* case law that makes for informative reading in Johnson 2005 *Seattle University Law Review* 467-503.

as an aspect of privacy rights rather than as a safeguard from trespassory interference. The Court affirmed that the Fourth Amendment protects the person and is not focused upon whether there has been a physical intrusion into the person's constitutionally protected area, such as the person's private home, offices or hotel room. The reasonableness of a search does not depend on whether there has been any interference with property rights, but on whether a justifiable expectation of privacy existed and whether this right has been overridden.[38]

A search is constitutional if it does not violate a person's reasonable or legitimate expectation of privacy. This inquiry embraces two questions: first, whether the individual's conduct reflects an actual, subjective expectation of privacy and, second, whether the individual's subjective expectation of privacy is one that society is prepared to recognise as reasonable.[39] What constitutes a constitutionally reasonable expectation of privacy is subject to interpretation.[40]

The United States Supreme Court has generally held that a person has a reasonable expectation of privacy regarding items in closed containers.[41] It is generally accepted that technological storage media should be considered equivalent to a special filing cabinet or a briefcase.[42] Although courts have generally agreed that electronic storage devices can be compared to closed containers, they have reached different conclusions regarding whether

---

37 See, for example, *Olmstead v US* 277 US 438 (1928) and *Silverman v US* 365 US 505 (1961).

38 Sharpe *Search and Surveillance* 9.

39 *Katz v United States* 389 US 347, 361, 362 (1967). This test was incorporated into the South African constitutional framework in *Bernstein v Bester NO* 1996 (4) BCLR 449 (CC). This approach was accepted as sensible because it confines any claim to privacy only to aspects in respect of which a legitimate expectation of privacy can be harboured. See paragraph 4.2.4.1 above for a reference to the right to privacy in the South African legislative framework.

40 See *O'Connor v Ortega* 480 US 709, 715 (1986). In *Payton v New York* 445 US 573, 589-90 (1980), the Supreme Court held that a person has a reasonable expectation of privacy in property located inside a person's home; in *Kyllo v United States* 533 US 27 (2000), the relative heat of various rooms in the home, revealed through the use of a thermal imager, was protected; in *United States v Ross* 456 US 798, 822-23 (1982), the contents of opaque containers were protected, as were conversations taking place in an enclosed phone booth in *Katz v United States* 389 US 347, 362 (1967). By contrast, in *Oliver v United States* 466 US 170, 177 (1984), it was held that a person does not have a reasonable expectation of privacy in activities conducted in open fields; in *California v Greenwood* 486 US 35, 40-41 (1988), garbage deposited at the outskirts of real property was considered unprotected and, in *Rakas v Illinois* 439 US 128, 143 (1978), no reasonable expectation of privacy was upheld in a stranger's house entered by the defendant without the owner's consent in order to commit a theft.

41 In *United States v Blas* 1990 US Dist LEXIS 1996 (ED Wis 1990), a law enforcement officer asked to examine a suspect's pager as the suspect exited a vehicle. The officer then searched through the device and wrote down several numbers that the officer later used to make further arrests. The Court found that the permission to examine the pager did not include consent to examine the contents of the pager. As such, the evidence obtained from the illegal search was barred from admission at trial. The Court noted that an individual has the same expectation of privacy in a pager, computer or other electronic data storage and retrieval device as in a closed container. The Court also found a reasonable expectation of privacy in data stored in a pager in *United States v Reyes* 922 F Supp 818, 832-833 (SDNY 1996), *United States v Lynch* 908 F Supp 284, 287 (DVI 1995) and *United States v Chan* 830 F Supp 531, 535 (ND Cal 1993). However, in *United States v Ross* 456 US 798 (1982), law enforcement officers working on information obtained from a confidential informant stopped a vehicle and arrested the occupants after a brown paper bag in the trunk was determined to be narcotics. The vehicle was taken to law enforcement headquarters and searched again, at which time a zippered pouch was opened. The defendant claimed that the evidence was seized illegally, because there was no search warrant for opening closed containers. The Supreme Court ruled that after a vehicle is stopped, if officers have probable cause to believe there is contraband, then a search might be as thorough as a magistrate could authorise. This includes searches of containers. Resseguie argues that it could be dangerous to compare computers to closed containers. If a computer is viewed as a closed container, a warrant authorising a search of computer memory provides a virtually unlimited right to law enforcement officers to review the contents of any files without any sorting as to relevance. Once an officer has the right to open a closed container, that means that she may look at anything contained therein. He concludes that the analogy is too simplistic and allows for the search and seizure of a computer to proceed in a very intrusive manner. He advises that the file cabinet analogy is much more appropriate to a search of computer files than the closed container analogy that has been predominantly followed. See Resseguie 2000 *Cleveland State Law Review* 213.

42 See Moore *Search and Seizure of Digital Evidence* 99. In *United States v Barth* 26 F Supp 2d 929 (WD Tex 1998), the defendant was arrested for possession of child pornography after the computer repairman noticed images during a repair and notified law enforcement officers. It was the opinion of the Court that the repairman was not a state actor when the initial images were discovered. Subsequent images that were discovered after law enforcement was notified were not admissible, because, at that point, the repairman became an actor under state law.

each individual file stored on a computer or disk should be treated as a separate closed container.[43]

There are times when a closed container can be opened without a warrant, as the individual has lost her right to privacy, even if she maintained a reasonable expectation of privacy. Should the information contained in the computer, briefcase or filing cabinet be viewable by the public,[44] then the owner of the information has waived her right to privacy.[45] Nor do individuals generally enjoy a reasonable expectation of privacy in the contents of computers they have stolen.[46] An individual may also maintain a reasonable expectation of privacy at one point in time and then lose that right over a period of time.[47]

When a person leaves a package with a third party for temporary safekeeping, she usually retains control of the package and thus retains a reasonable expectation of privacy in its

---

43 A computer disk containing multiple files was considered a single container for Fourth Amendment purposes in *United States v Runyan* 275 F3d 449, 464-65 (5th Cir 2001) and in *United States v Slanina* 283 F3d 670, 680 (5th Cir 2002). In the latter case, the Court held that when a warrantless search of a portion of a computer and zip disk had been justified, the defendant no longer retained any reasonable expectation of privacy in the remaining contents of the computer and disk, and thus a comprehensive search by law enforcement officers did not violate the Fourth Amendment. In *United States v Runyan* 275 F3d 449, 464-65 (5th Cir 2001), private parties had searched certain files and found child pornography. It was ruled that law enforcement officers did not exceed the scope of the private search when they examined additional files on any disk that had been, in part, privately searched. Comparing a disk to a closed container, the Court explained that law enforcement officers do not exceed the private search when they examine more items within a closed container than did the private searchers. However, in *United States v Carey* 172 F3d 1268, 1273-75 (10th Cir 1999), it was ruled that a law enforcement officer had exceeded the scope of a warrant to search for evidence of drug sales when the officer abandoned that search and instead spent the next five hours searching for evidence of child pornography. In *United States v Walser* 275 F3d 981, 986 (10th Cir 2001), the Court cautioned that there is a greater potential for the intermingling of documents and a consequent invasion of privacy when law enforcement executes a search for evidence on a computer due to the fact that computers can hold so much information touching on many different areas of a person's life.

44 In *Katz v United States* 389 US 347, 351 (1967), the Court noted that what a person knowingly exposes to the public, even in the person's own home or office, is not subject to Fourth Amendment protection. A related issue, which is yet to be fully addressed by the courts, is whether the Internet is public or private. The Internet and chat rooms, in particular, can be viewed from the privacy of one's home where a reasonable expectation of privacy does exist, but the information is also viewable by anyone else who is connected to the Internet. See paragraph 2.6.3 above for a reference to the chat room service offered on the Internet.

45 In *United States v David* 756 F Supp 1385, 1389 (D Nev 1991), law enforcement officers seized a data book and obtained information from the device after law enforcement officers feared the suspect was deleting information. The password to the device was obtained when an officer looked over the shoulder of the suspect as he typed. The Court found that the password was not illegally obtained, as the officer was where he was allowed to be and the suspect brought forth the information for all to see. The Court found no Fourth Amendment violation in obtaining the password, because the defendant did not enjoy a reasonable expectation of privacy in the display that appeared on the screen. The seizure of the data book was held to be acceptable because of the exigency in protecting the data. The search, however, was found to be invalid because the exigency ended upon seizure of the device. In *United States v Gorshkov* 2001 WL 1024026 at *2 (WD Wash May 23 2001), it was held that the defendant did not have a reasonable expectation of privacy in the use of a private computer network when undercover federal officers looked over his shoulder, when he did not own the computer he used and when he knew that the system administrator could monitor his activities.

46 In *United States v Lyons* 992 F2d 1029 (10th Cir 1993), the defendant was arrested and charged with the theft of computer-related equipment. Upon his arrest, the computer parts were seized and searched. The defendant argued that his Fourth Amendment privacy rights had been violated, but the Court disagreed and found that there is no expectation of privacy in stolen goods.

47 Kevin Poulsen was a hacker who has gained notoriety for his combination of hacking and phreaking abilities. While exploiting several phone companies, he collected numerous pieces of phone company equipment and computers. Along with several other pieces of evidence, Poulsen kept the computers stored in a rented locker facility. When Poulsen failed to pay the rent on the facility, the owner of the storage facility entered the storage locker with the intent of removing the belongings. When the manager entered the locker, he immediately noticed an abundance of computer equipment. Because of this discovery, the manager elected to notify both local law enforcement and the phone company whose brand name was on the phone equipment. At his trial, Poulsen attempted to have the evidence seized from several of the computer tapes removed on the basis that the evidence had been illegally seized. The Court, however, rejected Poulsen's argument based on the belief that Poulsen's privacy expectation disappeared along with his right to access the facility when he failed to make payment. See *United States v Poulsen* 41 F3d 1330 (9th Cir 1994). In *United States v Rahme* 813 F2d 31 (2nd Cir 1987), the Court ruled that even the expectation to privacy in items like briefcases and luggage does not exist once the allotted time has expired and the owner of the hotel room has regained control of the hotel room in which the item was found.

contents.[48] However, when an individual turns over the control of an item to a third party and she cannot reasonably expect to retain control over the item in the third party's possession, the sender no longer retains a reasonable expectation of privacy in its contents.[49]

An example of how this can be applied to technology would be a known drug dealer who ships a laptop, believed to contain buyer information, to an associate operating under a known alias. The fact that the individual is operating under an assumed name could potentially allow law enforcement to seize the evidence or conduct a search.[50] An individual generally cannot reasonably expect to retain control over mere information revealed to a third party, even when she has a subjective expectation that the third party will keep the information confidential.[51]

Because computer data is information, individuals who send data over communications networks may lose Fourth Amendment protection regarding the data once it reaches the intended recipient.[52] An individual's loss of control over information can become especially important when one is dealing with issues such as the posting of information in chat rooms. Since the courts have long held that information conveyed to undercover law enforcement officers does not maintain any right of privacy, it is argued that there could be no way that an individual who posts information in a chat room could discover whether the individuals who

---

48 In *United States v Most* 876 F2d 191, 197-98 (DC Cir 1989), a reasonable expectation of privacy in the contents of a plastic bag left with a grocery store clerk was upheld; in *United States v Barry* 853 F2d 1479, 1481-83 (8th Cir 1988), a reasonable expectation of privacy was upheld in a locked suitcase stored at an airport baggage counter; in *United States v Presler* 610 F2d 1206, 1213-14 (4th Cir 1979), a reasonable expectation of privacy in locked briefcases stored with the defendant's friend for safekeeping was protected; and in *United States v Barth* 26 F Supp 2d 929, 936-37 (WD Tex 1998), the Court held that the defendant retained a reasonable expectation of privacy in computer files contained in a hard drive left with a computer technician for the limited purpose of repairing the computer.

49 For example, in *United States v Horowitz* 806 F2d 1222, 1225-1226 (4th Cir 1986), the defendant emailed confidential pricing information relating to his employer to his employer's competitor. After the FBI searched the competitor's computers and found the pricing information, the defendant claimed that the search violated his Fourth Amendment rights. The Court disagreed, holding that the defendant had relinquished his interest in and control over the information by sending it to the competitor for the competitor's future use. See also *United States v Charbonneau* 979 F Supp 1177, 1184 (SD Ohio 1997), where the Court held that the defendant did not retain a reasonable expectation of privacy in the contents of an email message sent to the America Online chat room after the message had been received by chat room participants. It could, however, be argued that if the email message was encrypted, the sender had made a concerted effort to retain her reasonable expectation to privacy.

50 Moore *Search and Seizure of Digital Evidence* 100.

51 In *United States v Miller* 425 US 435, 443 (1976), the Court held that the Fourth Amendment does not protect bank account information that account holders divulge to their banks. By placing information under the control of a third party, an account holder assumes the risk that the information could be conveyed to the government. The Fourth Amendment does not prohibit obtaining information revealed to a third party and conveyed by such third party to government authorities even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. In *Smith v Maryland* 442 US 735, 743-744 (1979), it was found that no reasonable expectation of privacy exists in the phone numbers dialled by the owner of a telephone, because the act of dialling the number effectively tells the phone company the number. In *Couch v United States* 409 US 322, 335 (1972), it was held that law enforcement may subpoena an accountant for client information given to the accountant by a client, because the client retains no reasonable expectation of privacy in information given to an accountant. In *United States v Fregoso* 60 F3d 1314, 1321 (8th Cir 1995), it was held that a telephone company customer has no reasonable expectation of privacy in account information disclosed to the telephone company. In *In Re Grand Jury Proceedings: Subpoena Duces Tecum; Larry Danbom and Western Union v United States* 827 F2d 301, 302-03 (8th Cir 1987), it was held that customer account records maintained and held by Western Union are not protected by the Fourth Amendment.

52 Courts are not willing to be as generous in finding a right to privacy when data is stored in some third party computer system (see Loundy *Computer Crime, Information Warfare, and Economic Espionage* 197). Customers of Internet service providers do not have a reasonable expectation of privacy in customer account records maintained by and for the service provider's business. The Court found no Fourth Amendment protection for a network account holder's basic subscriber information obtained from the Internet service provider in *United States v Kennedy* 81 F Supp 2d 1103, 1110 (D Kan 2000). Intrusion and examination of the contents, however, ordinarily violates the reasonable expectation of privacy of both the sender and receiver (*United States v Villarreal* 963 F2d 770, 774 (5th Cir 1992). But in *United States v Walker* 20 F Supp 2d 971, 973-74 (SDW Va 1998), the Court concluded that packages sent to an alias in furtherance of a criminal scheme do not support a reasonable expectation of privacy.

receive the postings are undercover officers.[53] The absence of constitutional protections, however, does not necessarily mean that law enforcement officers can access the data without a warrant or court order, as statutory protections exist that generally protect the privacy of electronic communications.

5.2.3 Search and seizure of e-evidence with a warrant

The legal framework for searching for and seizing electronic evidence in a computing context largely mirrors the legal framework regulating other traditional searches and seizures. The eighteenth century declaration of the rights of persons encapsulated in the Fourth Amendment remains immutable; and it constitutes the standard by which courts in the United States evaluate the constitutionality of twenty-first century *e*-evidence. Despite this common legal framework, searching for and seizing *e*-evidence with a warrant tends to be more complicated and has been described as "as much an art as a science".[54]

In general, three steps are involved in drafting the search warrant and its accompanying affidavit, which explains the basis for the affiant's belief that the search is justified by probable cause. Firstly, the warrant and/or its attachments must accurately and particularly describe the property to be seized. Secondly, the affidavit must establish probable cause. Thirdly, the affidavit should include an explanation of the search strategy.[55] These three steps are discussed below.[56] In addition, the requirement of judicial supervision, *inter alia*, in respect of these steps is considered.[57]

5.2.3.1 Particularity and specificity

Securing a properly drafted search warrant is the best way to ensure that a search and seizure is not deemed unreasonable.[58] Executing a general warrant that permits an exploratory rummaging through a person's belongings in search of evidence is prohibited.[59] In interpreting the Fourth Amendment in the physical realm, it has been held that a search warrant must be particular with regard to the items that are to be seized, and specific with regard to where the

---

53 In the case of *United States v Charbonneau* 979 F Supp 1177 (SD Ohio 1997), the Court reasoned that a defendant did not retain a reasonable expectation of privacy in information posted to an America Online chat room. It was the Court's belief that information posted in chat rooms cannot be considered private because there is no way for the individual to verify who is at the other end of the computers receiving the postings. The issue in this case, however, was focused on postings to chat rooms and not on the issue of email messages. Emails are still regulated by the Electronic Communications Privacy Act of 1986, which controls who may obtain electronic communications and the legal process required for such an action. Therefore, in order to obtain an unread email, an investigator will usually have to obtain a search warrant. See paragraph 5.3 below in this respect.

54 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 30. See also paragraph 1.1 above that highlights some of these complexities.

55 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 43.

56 Paragraph 5.2.3.1 addresses the particularity and specificity requirements, paragraph 5.2.3.3 deals with the probable cause requirement and paragraph 5.2.3.4 gives pointers to the development of a search strategy.

57 In paragraph 5.2.3.2. below.

58 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 30.

59 *Coolidge v New Hampshire* 403 US 443, 467 (1970).

search and seizure will take place.[60] This doctrine of particularity and specificity becomes quite complex when one examines the issuance of a search warrant involving *e*-evidence. Regrettably, there is little final authority on the subject, because the United States Supreme Court has not yet ruled on either of the issues, which means that the sometimes conflicting opinions of the High Court and various circuit courts apply.[61]

Moore[62] asserts that the requirement of specificity is a less contentious aspect of search warrants involving electronic evidence than the requirement of particularity, as it is generally possible to provide the magistrate who is to issue the warrant with specific information as to where the computer or other evidence is located. Although this rings true as a launch pad for the execution of a search and seizure mechanism, the accurate identification of a location where *e*-evidence is kept can be very complex.[63] Law enforcement officers must understand the technical limits of different search techniques, plan the search carefully and then draft the warrant in a manner that authorises law enforcement officers to take the necessary steps to obtain the *e*-evidence they need.[64]

The requirement of particularity in a computing context is more problematic than its specificity counterpart, primarily due to the fact that technological advances in recent years have enabled media capable of massive data storage on physically smaller disks.[65] The most important decision law enforcement agencies must make when describing the property in the warrant is

---

60 Moore *Search and Seizure of Digital Evidence* 135.

61 Some of these conflicting opinions are referred to in the rest of paragraph 5.2.3.1. See also Moore *Search and Seizure of Digital Evidence* 74. There are more than 50 judicial systems in the United States. Each state and the District of Columbia have individual court systems, as do the territories of Puerto Rico, the United States Virgin Islands and Guam. There is also the federal court system, which is made up of district courts, appellate courts and the United States Supreme Court. The federal set-up is very similar to court systems at the state level. The hierarchy and the roles of the different courts are established by the United States Constitution and the various state constitutions. Trial courts exist at both the state and federal level. At the federal level, a district court can be thought of as a federal trial court. There is at least one United States District Court in each state, United States territory and the District of Columbia. Larger states may have several district courts. Appeals courts are called appellate courts and, at the federal level, circuit courts. There are 13 circuit courts. The first 11 circuits cover the 50 states and Unites States territories (indicated next to the circuit in brackets): First Circuit (Maine, Massachusetts, New Hampshire, Puerto Rico, Rhode Island), Second Circuit (Connecticut, New York, Vermont), Third Circuit (Delaware, New Jersey, Pennsylvania, Virgin Islands), Fourth Circuit (Maryland, North Carolina, South Carolina, Virginia, West Virginia), Fifth Circuit (Louisiana, Mississippi, Texas), Sixth Circuit (Kentucky, Michigan, Ohio, Tennessee), Seventh Circuit (Illinois, Indiana, Wisconsin), Eight Circuit (Arkansas, Iowa, Minnesota, Missouri, Nebraska, North Dakota, South Dakota), Ninth Circuit (Alaska, Arizona, California, Guam, Hawaii, Idaho, Montana, Nevada, Northern Mariana Islands, Oregon, Washington), Tenth Circuit (Colorado, Kansas, New Mexico, Utah, Oklahoma, Wyoming), Eleventh Circuit (Alabama, Florida, Georgia). The 12th and 13th Circuits are not known by numbers. The "12th" is the United States Court of Appeals for the District of Columbia (or the DC Court of Appeals). Congress created a "13th Circuit" in 1982, which became the Court of Appeals for the Federal Circuit. The United States Supreme Court is the highest court in the United States. It is the oldest federal court established by the Constitution in 1789. It is the United States Supreme Court that makes the final determination about whether a law violates the United States Constitution. However, lower courts may also make determinations about the constitutionality of laws. The United States Supreme Court rules on any conflicts that arise between state constitutions and the United States Constitution. All 50 states have constitutions and they operate on the same basic principle as the federal constitution. No state law can stand if it violates that state's constitution and state supreme courts ultimately determine whether a law is unconstitutional for that state. The court systems of the 50 states are, often, similar to the federal system. The trial courts can be at the county or state level. Most states also have one or two levels of appeals courts. Each state also has its own highest court or "supreme court". These state supreme courts have the final say unless the United States Supreme Court accepts an appeal of one of their rulings or overturns it. However, the state supreme court has the ultimate power to interpret that state's constitution. See Sadler *Electronic Media Law* 5-9.

62 Moore *Search and Seizure of Digital Evidence* 136.

63 See paragraph 1.1 above for a reference to some of these complexities.

64 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 30.

65 Moore *Search and Seizure of Digital Evidence* 136. See paragraph 2.5.1.1 above with regard to the storage capabilities of different storage media.

whether the seizable property[66] is the computer hardware itself, or merely the information that the hardware contains. If computer hardware is contraband, evidence, fruits, or instrumentalities of crime, the warrant should describe the hardware itself.[67] If the probable cause relates only to information, the warrant should describe the information, rather than the physical storage devices which happen to contain it.[68]

Two challenges to the scope of warrants arise particularly often in the context of warrants to seize hardware, compared to warrants to seize information.[69] Firstly, defendants may claim that a warrant is insufficiently particular when the warrant authorises the seizure of hardware but the affidavit only establishes probable cause to seize information.[70] Secondly, defendants may claim that law enforcement officers exceeded the scope of the warrant by seizing computer equipment if the warrant failed to state explicitly that the information to be seized might be in an electronic form. The former challenge argues that the description of the property to be seized is too broad, and the latter argues that the description is not broad enough.[71]

Search warrants sometimes fail to mention that the information described in the warrant may be in an electronic form. The courts have generally permitted law enforcement officers to seize computer equipment when law enforcement officers reasonably believe that the content described in the warrant may be stored in the equipment, regardless of whether the warrant states expressly that the information may be stored in electronic form.[72] What matters is the substance of the evidence, not its form, and the courts tend to defer to an executing law enforcement officer's reasonable construction of what property must be seized to obtain the evidence described in the warrant.[73]

On the other hand, computer search warrants sometimes authorise the seizure of hardware when the probable cause in the affidavit relates solely to the computer files the hardware

---

66 Rule 41(a)(2)(A) of the Federal Rules of Criminal Procedure defines property to include tangible objects such as documents, books, papers, as well as information. See *United States v New York Tel Co* 434 US 159, 170 (1977).

67 In *Davis v Gracey* 111 F3d 1472, 1480 (10th Cir 1997), it was held that the seizure of computer equipment used to store obscene pornography was proper because the equipment was an instrumentality.

68 In *United States v Gawrysiak* 972 F Supp 853, 860 (DNJ 1997), the seizure of records which included information and/or data stored in the form of magnetic or electronic coding on computer media that constituted evidence of certain specified federal crimes was upheld.

69 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 46-47.

70 Although the legal standards vary widely among the different circuit courts, most circuits permit the warrant to be construed with reference to the affidavit for the purposes of satisfying the particularity requirement in certain circumstances. Several circuits have held that courts can redact overbroad language and admit evidence from overbroad seizures if the evidence admitted was seized pursuant to sufficiently particular language. See *United States v Christine* 687 F2d 749, 759 (3rd Cir 1982) and *United States v Gomez-Soto* 723 F2d 649, 654 (9th Cir 1984).

71 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 46.

72 See *United States v Musson* 650 F Supp 525, 532 (D Colo 1986). In *United States v Reyes* 798 F2d 380, 383 (10th Cir 1986), it was found that in the age of modern technology and commercial availability of various forms of items, the warrant cannot be expected to describe with exactitude the precise form the records would take.

73 See *United States v Hill* 19 F3d 984, 987-89 (5th Cir 1994); *Hessel v O'Hearn* 977 F2d 299 (7th Cir 1992) and *United States v Word* 806 F2d 658, 661 (6th Cir 1986). In *United States v Gomez-Soto* 723 F2d 649, 655 (9th Cir 1984), the failure of the warrant to anticipate the precise container in which the material sought might be found has been found not fatal. In *United States v Abbell* 963 F Supp 1178 1997 (SD Fla 1997), it was noted that law enforcement agents may legitimately seize a document which is implicitly within the scope of the warrant, even if it is not specifically identified.

contains. Such a seizure might be challenged on the basis that the equipment itself is not evidence of a crime, an instrumentality or contraband that may be seized according to Rule 41(a) of the Federal Rules of Criminal Procedure.[74] Computer files, however, do not exist separately from some storage medium. Law enforcement officers may need to seize the equipment in order to obtain the files it contains. It must be borne in mind that the physical equipment merely stores the information that law enforcement officers have probable cause to seize. Focusing on the hardware, rather than on the information it contains, may also result in a warrant that is too narrow, in that law enforcement officers may lack the authority to seize information on other media, such as paper or photographs. To date, the courts have generally held that descriptions of hardware can satisfy the particularity requirement, as long as the subsequent searches of the seized computer hardware appear reasonably likely to yield evidence of crime.[75] It has been recommended that if the property to be seized is information, the warrant should describe the information to be seized, rather than its container. The container itself may, of course, be independently seized as an instrumentality when the information to be seized is contraband. When conducting a search for information, law enforcement officers need to consider carefully exactly what information they need, and each warrant should be tailored to the needs of each search. The warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored, whether electronic or not.[76]

Law enforcement officers should also be particularly careful when they seek authority to seize a broad class of information, especially from businesses.[77] A request for permission to seize "all records" from an operating business, unless officers have probable cause to believe that the criminal activity under investigation pervades the entire business, will not be granted.[78] Instead, the description of the files to be seized should include limiting phrases that can modify and limit the "all records" search as necessary and where appropriate. The crime under investigation, the target of the investigation if known and the time frame of the records involved may, for example, be specified in narrowing an "all records" search.[79] When law enforcement officers

---

74 In *In re Grand Jury Subpoena Duces Tecum* 846 F Supp 11, 13 (SDNY 1994), it was held that a subpoena demanding production of computer hardware, instead of the information it contained, was unreasonably broad.

75 In *United States v Hay* 231 F3d 630, 634 (9th Cir 2000), the seizure of "computer hardware" in a search for materials containing child pornography was upheld. In *United States v Campos* 221 F3d 1143, 1147 (10th Cir 2000), the seizure of "computer equipment which may be, or is used to visually depict child pornography" was upheld and the Court noted that the affidavit accompanying the warrant explained why it would be necessary to seize the hardware and search it off-site for the images it contained. In *United States v Upham* 168 F3d 532, 535 (1st Cir 1999), the seizure of "any and all computer software and hardware ... computer disks, disk drives" in a child pornography case was upheld because "as a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the [sought after] images". However, in *United States v Lacy* 119 F3d 742, 746 (9th Cir 1997), a warrant permitting the "blanket seizure" of computer equipment from the defendant's apartment was found to be insufficiently particular.

76 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 44.

77 *United States v Leary* 846 F2d 592, 600-604 (10th Cir 1988).

78 *United States v Ford* 184 F3d 566, 576 (6th Cir 1999) and *In re Grand Jury Investigation Concerning Solid State Devices v United States* 130 F3d 853, 857 (9th Cir 1997).

79 In *United States v Kow* 58 F3d 423, 427 (9th Cir 1995), a warrant was invalidated for failure to name the crime or to limit the seizure to documents authored during the time frame under investigation. In *United States v Ford* 184 F 3d 566, 576 (6th Cir

cannot reasonably know the precise form that records will take before the search occurs, a generic description must suffice.[80] Even an "all records" search may be appropriate in certain circumstances.[81]

In particularising the hardware that is to be seized, it has been suggested that investigators request a warrant for "all digital media, including, but not limited to ...".[82] At least one court, however, struck down a search warrant containing this statement as overly broad.[83] This phrase has traditionally been included on search warrants for *e*-evidence because of the need to ensure that all forms of storage media are covered by the search warrant. A search warrant calling for the seizure of computers, storage devices and software has also been held to be a catch-all warrant that failed to meet the particularity requirement.[84] To counter the argument that law enforcement is on an evidential "fishing expedition", it is imperative that the magistrate issuing the warrant be made to understand the following issues:

(a) the importance of the *e*-evidence to the successful prosecution of the state's case and the volatility of such evidence;
(b) the need to examine all the various storage media; and
(c) the fact that items seized that do not contain evidence of the crime for which the search warrant was issued will not be examined and will be released back to the owner.

1999), it was held that the failure to limit broad descriptive terms by relevant dates, when such dates are available to law enforcement, will render a warrant overbroad. In *In the Matter of the Application of Lafayette Academy Inc. v United States* 610 F2d 1, 3-4, 4 (1st Cir 1979) and *United States v Hunter* 13 F Supp 2d 574, 584 (D Vt 1998), the Court concluded that a warrant to seize "all computers" was not sufficiently particular where the description did not indicate the specific crimes for which the equipment was sought.

80 In *Davis v Gracey* 111 F3d 1472, 1478 (10th Cir 1997), it was found that even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit. In *United States v Lacy* 119 F3d 742, 746-47 (9th Cir 1997), it was held that general description of computer equipment to be seized was sufficient, as there was no way to specify what hardware and software had to be seized to retrieve the images accurately. In *United States v London* 66 F3d 1227, 1238 (1st Cir 1995), it was noted that where the defendant operated a complex criminal enterprise where he mingled innocent documents with apparently innocent documents which, in fact, memorialised illegal transactions, it would have been difficult for the magistrate to be more limiting in phrasing the warrant's language, and for the executing officers to have been more discerning in determining what to seize.

81 *See United States v Hargus* 128 F3d 1358, 1362-63 (10th Cir 1997), where the seizure of "any and all records relating to the business" under investigation for mail fraud and money laundering was upheld. In cases involving complex financial transactions and widespread allegations of various types of fraud, a reading of the warrant with "practical flexibility entails an awareness of the difficulty of piecing together the paper puzzle". The rationale behind such a flexible reading of the particularity requirement is that, in investigations of ongoing fraudulent practices, all the records are likely to be relevant to show the existence of a fraudulent scheme. See Bohn and Muster 2003 *Suffolk Journal of Trial & Appellate Advocacy* 68.

82 Moore *Search and Seizure of Digital Evidence* 136.

83 In *In the Matter of Search Warrant for K-Sports Imports Inc* 163 FRD 594 (CD Cal 1995), K-Sports was under investigation for smuggling and selling machine guns. Officers executed a search warrant on the premises that resulted in the seizure of all computer records. The Court found the wording "including, but not limited to ..." to provide too little guidance with regard to what evidence could be seized. The wording made the warrant too vague to satisfy the particularity requirement. Conversely, other courts have held that the particularity requirement of the Fourth Amendment is not violated when law enforcement officers make requests to search for all computer devices and computer-related storage devices. For example, in the case of *United States v Upham* 168 F3d 532 (1st Cir 1999), the Court found that a search for all computer-related storage devices was not overly broad because the officers had to search everything to ensure they found the pertinent evidence for which they were searching. The Court also refused to remove the images that were recovered using the "undelete" utilities. In the opinion of the Court, the recovery of deleted computer evidence is equivalent to the reassembly of a ransom note and, as such, is permissible by law.

84 In *United States v Hunter* 13F Supp 2d 574 (D Vt 1998), the Court upheld the defendant's argument that the search warrant was overly broad and in violation of the Fourth Amendment. The evidence was nevertheless accepted on the basis that law enforcement officers did not move through records outside the intent of the search warrant.

It has accordingly been recommended that the inclusion of every item that could potentially contain evidence be required on all search warrants, even warrants issued in circuits that have allowed the use of the phrase "including but not limited to ...".[85] If, during the search, additional storage media are discovered, then a new search warrant may be obtained and the evidence can be protected until the warrant arrives.

In addition to listing every item that could potentially contain *e*-evidence, all searches should preferably be conducted on site, without any seizure of computer hardware. Searches conducted on site could potentially solve a portion of the problem, but this solution creates an even larger problem, as the storage capacity of today's computer storage media would often make a search on site an almost impossible task. An examination like this would place an undue burden on both law enforcement officers and the owner of the computer system. Law enforcement officers should attempt to explain to the magistrate issuing a warrant the need to examine the evidence off-site.[86] If a magistrate determines that the seizure of an entire computer could present a problem, then investigators could settle for making an image of the suspect's hard drive.[87] This situation could potentially arise in cases involving the search of business computers, where seizure would result in financial damages to the suspect's entire office. Unless a magistrate believes that the entire company is involved in the criminal activity under investigation, the magistrate could consider seizure of all computers excessive.[88]

The requirement of facial validity does not mean that every officer authorised to execute the search must be individually named, or that every single detail concerning the object of the search must be particularised.[89] The knowledge of the law enforcement officer carrying out the search may, on occasion, supplement the description of items contained in the warrant.[90] Where a warrant is issued to search for a large amount of, for example, published material, a higher standard of particularity is required because the right to free speech and freedom of the press conjoins with the right to privacy.[91]

5.2.3.2 Judicial supervision

Judicial review of search warrants requires common sense. The review must focus on practicalities, rather than be overly technical.[92] Law enforcement officers, or a forensic expert instructed by them, must explain the complexities involved in the investigation of high technology crimes to magistrates who need to issue warrants. Such an explanation will provide

---

85 Moore *Search and Seizure of Digital Evidence* 140.
86 Moore *Search and Seizure of Digital Evidence* 76.
87 See generally paragraph 2.3 above for a reference to, *inter alia*, computer forensics that involves the imaging of a computer hard drive.
88 Moore *Search and Seizure of Digital Evidence* 77.
89 Sharpe *Search and Surveillance* 57.
90 *Massachusetts v Sheppard* 468 US 981 (1984).
91 See *Stanford v Texas* 379 US 476 (1965) and *Zurcher v Stanford Daily* 436 US 547(1978).
92 *United States v Ventresca* 380 US 102, 108 (1965).

the magistrate with reasons why computer disks may have to be seized and the explanation could also be used to counter an argument that law enforcement officers are fishing for evidence.[93]

It is also extremely important that law enforcement officers who request a warrant ensure that the judge understands what precisely it is they will be searching for and what types of information may be discovered. There are few areas of search and seizure where this is more important than in cases involving high technology crimes and/or *e*-evidence. Law enforcement officers who do not take this advice risk having their evidence excluded, notwithstanding the good faith clause.[94] This concern is due in part to the fact that there are continually new advances and that new terminology is used in the field of computer technology every day. To combat these types of circumstances, it has even been recommended that all law enforcement officers requesting a search warrant involving computers or other high technology devices carry a pocket dictionary of computer terms and definitions.[95]

Judicial supervision must be done by a neutral and detached magistrate who must exercise sufficient care in ensuring that a warrant is justified.[96] The requirement that the issuer of the warrant be "neutral and detached" does not necessarily mean that she has to be legally qualified.[97]

5.2.3.3 Probable cause requirement

The second step in preparing a warrant to search and seize a computer is to produce a sworn affidavit establishing probable cause to believe that contraband, evidence, fruits or instrumentalities of crime exist in the location to be searched.[98] A warrant must not be so lacking in *indicia* of probable cause as to render official belief in its existence entirely

---

93 Moore *Search and Seizure of Digital Evidence* 78.

94 The good faith clause provides that evidence seized outside a search warrant may still be entered into evidence if law enforcement officers are acting under what they reasonably and objectively believe to be a valid search warrant. See generally *United States v Leon* 468 US 897, 922 (1984) and *Massachusetts v Sheppard* 468 US 981, 990-991 (1984). If the good faith exception applies, the Court will not order the evidence to be suppressed. In *United States v Hunter* 13 F Supp 2d 574, 584-85 (D Vt 1998), the Court held that the good faith exception applied even though the computer search warrant was insufficiently particular.

95 Moore *Search and Seizure of Digital Evidence* 78.

96 In *Coolidge v New Hampshire* 403 US 443 (1970), warrants relating to a murder investigation were issued by the State Attorney General, acting as a justice of the peace. Prior to issuing the warrants, the Attorney General had personally taken charge of all police activities relating to the investigation. He later served as a chief prosecutor at the trial. The Supreme Court held that the search resulting from these warrants breached the Fourth Amendment. In *Connally v Georgia* 429 US 245 (1977) the justice had a direct, personal, substantial, pecuniary interest in making a determination, as he was paid a prescribed fee for the issuance of every warrant, whilst no fee was payable where a warrant was denied. Sharpe argues that if magistrates are not regarded by those at risk as sufficiently impartial to deliver a fair trial, it must be questioned whether they are always sufficiently impartial to act neutrally in a search warrant procedure that does not allow for defence representation. She contends that an unquestioning trust in the veracity of law enforcement is not conducive to creating the impartiality required from presiding officers. Such a trust in police veracity can arise not only through previous employment connections, but simply through the day-to-day contact that arises between magistrates and law enforcement officers and the creation of a collaborative culture. See Sharpe *Search and Surveillance* 52.

97 In *Shadwick v City of Tampa* 407 US 443 (1971), it was stated that there was nothing in the Fourth Amendment to require that all warrant authority must reside exclusively in a lawyer or judge. The Supreme Court's approval of lay justices was reiterated in *North v Russell* 427 US 328 (1976).

98 See the Fourth Amendment to the United States Constitution: "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation" and the Federal Rules of Criminal Procedure 41(b)(c).

unreasonable. This requirement is the crux of reasonableness determinations. If there is apparent insufficiency of probable cause, then the search is an unreasonable one. If an individual has given reasonable grounds to the law enforcement officers to search for evidence of crime, then she cannot complain of a privacy violation, since there is no right to secrete evidence of offending. This principle is implicit in the Constitution of the United States.[99]

The Supreme Court requires an affidavit to establish a fair probability that contraband or evidence of a crime will be found in a particular place.[100] A bare suspicion that criminal evidence will be found in the place searched will naturally not suffice.[101] A practical, common sense determination of the probabilities, based on the totality of the circumstances, is called for. The magistrate's determination that probable cause exists will be upheld only as long as there is a substantial basis for concluding that probable cause exists.[102]

The probable cause requirement does not require agents to acquire an accurate knowledge regarding the precise forms of evidence or contraband that will exist in the location that is to be searched, prior to the search and seizure intervention. Law enforcement officers accordingly do not need probable cause to believe that the evidence sought will be found in computerised, as opposed to paper, form.[103] Similarly, officers do not need to know exactly what statutory violation the evidence will help reveal.[104] They also do not need to know who owns the property that is to be searched and seized.[105] The probable cause standard simply requires law enforcement officers to establish a fair probability that contraband or evidence of a crime will be found in the particular place that is to be searched.[106] If the law enforcement officers do, however, have particular knowledge as to the form of evidence or contraband that exists at the place to be searched, they should articulate that knowledge fully in the affidavit.[107]

Probable cause challenges to computer search warrants arise particularly often in cases involving the possession and transmission of child pornography images.[108] Defendants in these types of cases often claim that the passage of time between the warrant application and the occurrence of the incriminating facts alleged in the affidavit left the magistrate or judge without

---

99 See *United States v Leon* 468 US 897 (1984) and Sharpe *Search and Surveillance* 57.

100 *Illinois v Gates* 462 US 213, 238 (1983).

101 *Brinegar v US* 338 US 160, 175 (1949).

102 *Illinois v Gates* 462 US 213, 236 (1983).

103 In *United States v Reyes* 798 F2d 380, 382 (10th Cir 1986), the Court noted that "in the age of modern technology..., the warrant could not be expected to describe with exactitude the precise forms the records would take".

104 See *United States v Prandy-Binett* 995 F2d 1069, 1073 (DC Cir 1993).

105 See *United States v McNally* 473 F2d 934, 942 (3rd Cir 1973).

106 See *Illinois v Gates* 462 US 238 (1983).

107 Law enforcement officers should, however, exercise care in articulating details in the affidavit. In *United States v Tamura* 694 F2d 591, 595 (9th Cir 1982), it was, for example, noted that probable cause to seize specific paper files enumerated in a warrant technically does permit the seizure of commingled innocent files.

108 An unusual number of computer search and seizure decisions involve child pornography because computer networks provide an easy means of possessing and transmitting contraband images of child pornography. Also, the fact that possession of child pornography transmitted over state lines is a felony often leaves defendants with little recourse but to challenge the procedure by which law enforcement officers obtained the contraband images. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 98.

sufficient reason to believe that images of child pornography would be found in the defendant's computer(s).[109] The courts have generally found little merit in these staleness arguments, in part because the courts have taken judicial notice of the fact that collectors of child pornography rarely dispose of such material.[110] Courts have also noted that advances in computer forensic analysis allow investigators to recover files even after they have been deleted, casting greater doubt on the validity of staleness arguments.[111]

Probable cause challenges may also arise when supporting evidence in an affidavit is derived heavily from records of a particular Internet account or Internet Protocol (IP) address. The identity or location of the person who used an account or address cannot be conclusively established by the fact that such an account or address was, in fact, used. An affidavit based heavily on account or IP address logs must accordingly demonstrate a sufficient connection between the logs and the location that is to be searched so as to establish a fair probability that contraband or evidence of a crime will be found in the particular place to be searched.[112]

5.2.3.4 The quest for an e-evidence search strategy

The third step in drafting a successful search warrant operable in a computing context is to provide an exposition of the envisaged search strategy encapsulating both its practical and legal considerations in the affidavit accompanying the search warrant. Although searches for electronic evidence may be executed in a variety of ways, the four most common search strategies are[113]

(a) to search the computer and print out a hard copy of particular files at that time;[114]

(b) to search the computer and make an electronic copy of particular files at that time;[115]

---

109 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 48.

110 See *United States v Hay* 231 F3d 630, 636 (9th Cir 2000), *United States v Horn* 187 F3d 781, 786-87 (8th Cir 1999), *United States v Lacy* 119 F3d 742, 745-46 (9th Cir 1997) and *United States v Sassani* 139 F3d 895 (4th Cir 1998). But also consider *United States v Zimmerman* 277 F3d 426, 433-34 (3rd Cir 2002), where the Court distinguished between the retention of adult pornography and the retention of child pornography. Evidence of adult pornography that had been on computer at least six months before a warrant was issued was found stale.

111 See *United States v Hay* 231 F3d 630, 634, 636 (9th Cir 2000) and *United States v Cox* 190 F Supp 2d 330, 334 (NDNY 2002).

112 See *Illinois v Gates* 462 US 213, 238 (1983). In *United States v Cervini* 16 Fed Appx 865 (10th Cir 2001), the Court upheld a finding of probable cause to search a house based on evidence of the following: that a particular IP address was used to transmit child pornography at a particular time; that the IP address and the time of transmission were associated with the suspect's account with an Internet service provider; and that the suspect had two active phone lines connected to his house. In *United States v Hay* 231 F3d 630, 634 (9th Cir 2000) evidence that child pornography images were sent to an IP address associated with the defendant's apartment, combined with other evidence of the defendant's interest in young children, created probable cause to search the defendant's apartment for child pornography. In *United States v Grant* 218 F3d 72, 76 (1st Cir 2000), evidence that an Internet account belonging to the defendant was involved in criminal activity on several occasions, and that the defendant's car was parked at his residence during at least one such occasion, created probable cause to search the defendant's residence.

113 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 32.

114 Printing out hard copies of particular files during a search is rarely a good strategy to follow, as it may lead to a substantial loss of valuable information (such as the file date and time stamps, file path names, "undo" histories and comment fields). See in this respect paragraph 2.3.1.1 above.

115 The electronic copying of individual files is different from making an image an entire drive. When a computer file is saved to a storage disk, it is saved in randomly scattered sectors on the disk rather than in contiguous, consolidated blocks. When the

(c) to create a duplicate electronic copy of the entire storage device on site, and then later to recreate a working copy of the storage device off site for review; and

(d) to seize the equipment, remove it from the premises, and review its contents off site.

To assist with the collection of *e*-evidence, the assembly of a computer search warrant team is recommendable. Operating in much the same manner as a high-risk warrant execution team, a search warrant team trained for the execution of search warrants involving digital evidence ensures quick and accurate seizure of evidence from computers and other technological devices. Ideally, the team should be made up as follows: a case supervisor, an interview team, a sketch and photo team, a physical search team, a security and arrest team and a technical evidence seizure and logging team. The United States Secret Service and the United States Department of Justice have prepared first responder guidelines to guide search warrant teams focused on collecting electronic evidence.[116]

The likelihood that search and seizure will be successful can be maximised by acquiring as much detailed and accurate information as possible about the computer system(s) targeted by the search before devising a search strategy or drafting the search warrant. This step cannot be overemphasised and has serious practical[117] and legal[118] implications that feed on each other.

---

file is retrieved, the scattered pieces are reassembled from the disk in the computer's memory and presented as a single file. A file-by-file copy (also known as a "logical file copy") merely creates a copy of an individual file by reassembling and then copying the scattered sectors of data associated with the particular file. By contrast, the imaging of a disk copies the entire disk exactly as it is, including all the scattered pieces of various files (as well as other data such as deleted file fragments). The image allows a computer technician to recreate (or "mount") the entire storage disk and have an exact copy just like the original. See paragraph 2.3.1.2.1. above in this respect.

116 These guidelines have been criticised by some scholars, among others, on the basis that both these guidelines merely assume that the suspect will be using the Microsoft Windows Operating System. Although Microsoft Windows is the operating system most commonly in use today, the execution of a search warrant following the guidelines for a Windows machine could potentially damage evidence if a Linux or Macintosh computer system is encountered. For example, the guidelines agree that the solution to powering down a computer is to turn off the computer. While this method is recommended for computers running Microsoft-related operating systems, there are numerous dangers associated with conducting a hard shut down of a computer running the Linux operating system that could result in the loss of valuable evidence. Although the majority of evidence that would be lost would relate to command line operations, this may nevertheless be important to a case involving a hacker. "Command line operations" is an expression used to refer to commands that run from the command prompt, with the command prompt being closely related to the traditional DOS (Disk Operating System) prompt screen. Such commands are run by typing the command. Linux is actually preferred by many hackers because of its command line use. A case involving a hacker may result in evidence being stored in the operating system's memory. Because Linux updates its command line when the computer is shut down, powering down the computer without going through the power down process may result in a loss of evidence. Additionally, some operating systems such as Linux and Macintosh may suffer from file integrity damage if they are not adequately shut down. With this in mind, it is recommended that an officer always go through the proper shut down procedures when dealing with operating systems other than Microsoft systems. It should also be noted that there are programs available that would allow a user to delete files if the computer is not powered down by the actual owner of the system. With operating systems such as Windows, it is accordingly recommended that the officer power down the computer by pulling the plug from the back of the computer. The power should never be pulled from the wall, as there are devices that allow for the destruction of digital evidence if the power is cut from the wall. If computer criminals truly want to protect their data from being seized, there are hundreds of methods of booby-trapping their computers. Some computer forensic professionals believe that computers can be booby-trapped with small explosives or with magnetic devices that will delete the data stored on the hard drive. However, if an officer attempts to counter all the various methods, it would require extensive training in order to execute a search warrant for digital evidence. This is, of course, the most desirable scenario, but it is also the most unlikely, due to financial constraints. See Moore *Search and Seizure of Digital Evidence* 136 and 142.

117 It might be impossible to get to know how the information contained in the system can be retrieved, or even where the information may be located, until the law enforcement officer has learned what kinds of computers and operating systems the suspect uses. Every computer and computer network is different and subtle differences in hardware, software, operating systems and system and network configuration can alter the search plan dramatically. A particular search strategy may work well if a targeted network runs the Linux operating system, but might not work if the network runs Windows NT instead. These concerns are exacerbated when searches involve complicated computer networks. The mere fact that a business uses computers in its offices does not mean that the devices found there actually contain any useful information. Businesses may

Various avenues may lead to such a reconnaissance of the computing environment that is to be penetrated. A useful source of information for networks connected to the Internet is, of course, the Internet itself, as it is often possible for members of the public to use network queries to determine the operating system, machines and general layout of a targeted network connected to the Internet. Caution must be exercised that these queries do not set off alarms at the target network. Alternatively, law enforcement officers can interview the system administrator of the targeted network, albeit in an undercover capacity. When this is impossible or dangerous, more piecemeal strategies may prove effective. Law enforcement officers may occasionally conduct on-site visits (often undercover) that will at least reveal some elements of the hardware involved.

In many cases, law enforcement officers are unable to learn enough about the computer system that is to be searched to devise a single or comprehensive search strategy. Even where a considerable amount is known about a system, the law enforcement officers and/or the computer forensic professionals conducting a review of the data often have to use a number of different techniques in order to search thoroughly a computer and its storage media.

Seemingly commonplace data or configurations can sometimes not be copied, reviewed or analysed by one search program or protocol, so other(s) search tools must be tried.[119] Keyword searches[120] may also not be possible until a careful review of a portion of the files has been conducted. A careful data search may reveal non-apparent aspects of how the system was used and the data sought was generated, accessed, transmitted and stored. It is important for law enforcement officers to bear in mind unforeseen complexities and to consider and address them as they formulate their strategy. Law enforcement officers should therefore also recognise how the aspects of the system that they do not know about can affect the search strategy. In

---

contract with network service providers that store the business's information on remote network servers located miles away or even on other continents. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 32. This further illustrates why a working knowledge of computer and computing environments are vital for the law enforcement practitioners who set out to penetrate them. See generally paragraph 2.5 above.

118 The incidental seizure and subsequent search through network accounts may, for example, raise issues under the Electronic Communications Privacy Act. See the discussion in paragraph 5.3 below. The incidental seizure of First Amendment materials (such as drafts of newsletters or web pages) may also implicate section 2000aa of the Privacy Protection Act 42 United States Code Collection (hereinafter referred to as 42 USC). See the discussion in paragraph 5.2.3.4.5 below. To minimise liability under these two statutes, law enforcement officers should conduct a careful investigation into whether and where First Amendment materials and network accounts may be stored on the computer system targeted by the search. At least one court has suggested that a failure to conduct such an investigation can deprive the government of a good faith defence against liability under these statutes. See *Steve Jackson Games Inc v United States Secret Service* 816 F Supp 432 (WD Tex 1993).

119 See paragraph 2.3.1.2.2 above for a reference to some of the available computer forensic software tools.

120 An important feature of computer forensics software tools is that it allows for keyword string searches of text-based evidence media. Many different keywords can be critical to an investigation, including user IDs, passwords, sensitive data such as code words, known filenames and subject-specific words (for example "marijuana", "mary jane", "bong" and "dope"). Keyword searches must be planned carefully to minimise exposure of the data while balancing the requirement for discovery of data relevant to the investigation. String searches can be conducted on the logical file structure or at the physical level to examine the contents of an entire drive. Many keyword search utilities provide a window of information around the key word or phrase which allows the reviewer to determine its applicability to the investigation. In specialised cases involving privileged data, this window can present serious legal issues if it is believed that it lead to excessive review of data. Most disk-search tools that are marketed as forensic software perform raw reads from the hard drive, conducting a physical-level string search of the drive. Commonly used disk-search utilities include dtSearch, offered by dtSearch COpr. These utilities perform the search from a physical level. See Prosise and Mandia *Incident Response & Computer Forensics* 302.

most cases, the search team should decide on a preferred search strategy, and then plan a series of backup strategies if the preferred strategy proves to be impractical.[121]

In general, the issues that must be considered when formulating a strategy to search and seize *e*-evidence can be divided into four questions:[122] Firstly, what is the role that the computer played in the commission of the offence and how can this enable the most effective search strategy that will comply with Rule 41 and the Fourth Amendment? Secondly, will the search require multiple warrants? Thirdly, should law enforcement officers request special permission to conduct a no knock or surreptitious search, without having to notify the person whose premises are searched at the time of the search? And fourthly, does the search strategy need to be modified and will it be necessary to search and sift before the actual seizure of the relevant data, to minimise liability issues? These four questions are considered in more detail below.[123]

5.2.3.4.1 Role of the computer

The role of computer hardware in the commission of the offence has been singled out as the most important consideration in conceptualising a particular search strategy.[124] If the hardware is itself an instrumentality,[125] evidence, contraband or a fruit of crime,[126] law enforcement officers will usually plan to seize the hardware and search its contents off site. If the hardware is merely a storage device for evidence,[127] the hardware is generally only seized if less disruptive alternatives are not feasible. As Rule 41(1)(b) of the Federal Rules of Criminal Procedure authorises the seizure of hardware in the former case, but not in the latter, the search strategy for a particular computer search hinges initially on the role of the hardware in the commission of the offence. In practice, this translates into the point of departure that law enforcement officers should only seize the equipment if a less intrusive alternative that permits the effective recovery of the evidence is not feasible in the particular circumstances of the case. The general strategy is flexibility in pursuing the quickest, least intrusive, and most direct search

---

121 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 32.

122 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 32.

123 See paragraphs 5.2.3.4.1 to 5.2.3.4.5 below.

124 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 32. See also paragraph 5.2.3.1 above with regard to how the role of the computer could affect the specificity and particularity requirements of a search warrant.

125 For example, a computer used to transmit child pornography is considered an instrumentality of the crime (see, for example, *Davis v Gracey* 111 F3d 1472, 1480 (10th Cir 1997), where a computer was used to store obscene images and in *United States v Lamb* 945 F Supp 441, 462 (NDNY 1996), where a computer was used to store child pornography). This distinction may also be important from the perspective of asset forfeiture as, for example, property used to commit or promote an offence involving obscene material may be forfeited criminally pursuant to section 1467 of 18 USC; property used to commit or promote an offence involving child pornography may be forfeited criminally and civilly pursuant to section 2254 of 18 USC.

126 Stolen computers can be considered the fruits of crime.

127 If, for example, a suspect keeps evidence of her fraud schemes on her personal computer, the hardware itself is merely a container for evidence. Other examples are where drug traffickers store transactional data such as client names, dates and amounts on computers, or records of stolen credit card numbers or stolen passwords. See Collier *Criminal Law and the Internet* 323.

strategy that is consistent with securing the evidence described in the warrant. This will permit an on-site search in some cases and a seizure for off-site review in others.

Whilst law enforcement officers may succeed in obtaining a warrant to seize an entire network where the hardware is used as an instrumentality, evidence, contraband, or the fruit of a crime, a complicated network may require a more nuanced approach. Where a network is owned and operated by a criminal enterprise, it may be appropriate to seize the network to stop ongoing criminal activity and prevent further or substantial loss to victims. However, the carting off and wholesale seizure of the entire network may cripple a legitimate, functioning business, disrupt the lives of hundreds of people and cause a multitude of practical problems. Such a seizure may require a significant commitment of resources and advanced planning, the absence of which may subject the government to civil suits arising from collateral damage.[128]

Circumstances may dictate the seizure of equipment and the search of its contents off-site. Due to the vast amounts of data stored on storage media, it may take days or weeks to find the specific information described in the warrant. It may also be practically impossible for officers to search quickly through a computer for specific data, a particular file, or a broad set of files while they are on-site. Even if the officers know specific information about the sought after files, the data may be mislabelled, encrypted, stored in hidden directories, or embedded in slack space that a simple file listing will ignore. Recovering such evidence may require painstaking analysis by an expert in the controlled environment of a forensics laboratory. An inept attempt to search files on-site may even risk damaging the evidence itself.[129] A technically adept criminal may know how to trip-wire her computers with self-destruct programs that could erase vital evidence if the system were to be examined by anyone other than an expert.[130] In these cases, it is best to seize the equipment and permit an off-site expert to disarm the program before any search occurs.[131]

An on-site search may be possible where, for example, a cooperative employee or system administrator agrees to pinpoint a file or record or introduce a recent backup, permitting the officers to obtain a hard copy of the files they seek while they are on-site.[132] Alternatively, officers may be able to locate the targeted set of files and make electronic copies, or may be able to mirror a segment of the storage drive based on knowledge that the information exists

---

128 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 33.

129 Officers executing a search may learn on-site that the computer employs an uncommon operating system that the on-site technical specialist does not fully understand. The best strategy may be to remove the hardware so that a government expert in that particular operating system can examine the computer later.

130 For example, a criminal could write a very short program that would cause the computer to demand a password periodically, and if the correct password is not entered within a few seconds, it would trigger the automatic destruction of the computer's files.

131 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 34.

132 In *United States v Longo* 70 F Supp 2d 225 (WDNY 1999), the Court upheld a pinpoint search aided by the suspect's secretary for two particular computer files.

within that segment of the drive. Relatively few cases, however, call for a limited set of known files as searches for evidence of a particular crime are usually more open-ended.[133]

5.2.3.4.2 Knock-and-announce

The "knock-and-announce" rule[134] requires law enforcement officers to announce their presence and authority prior to executing a search warrant, in an attempt to reduce the risk of violence and destruction of property.[135] When law enforcement officers have reason to believe that knocking and announcing their presence would be dangerous or futile in preventing the destruction of evidence or could otherwise inhibit the effective investigation of crime, the issuance of a no knock warrant should be requested.[136] The failure to obtain judicial authorisation to dispense with the knock-and-announce rule does not preclude the officers from conducting a no knock search, however. In some cases, officers may neglect to request a no knock warrant, or may not have reasonable suspicion that evidence will be destroyed until they execute the search.[137]

5.2.3.4.3 Multiple warrants

Law enforcement officers should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations. In terms of Rule 41(a) of the Federal Rules of Criminal Procedure, a magistrate located in one judicial district may issue a search warrant for a search of property within that district or a search of property outside that district if the property is within the district when the warrant is sought but might move outside the district before the warrant is executed. Although the courts have not directly addressed the matter, it has been argued that the language of Rule 41 combined with the Supreme Court's interpretation of "property" may limit searches of computer data to data that resides in the district in which the warrant was issued.[138]

---

133 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 34.

134 Although a statutory "knock and announce" rule is provided in section 3109 of 18 USC, it is also embedded in the interpretation of the Fourth Amendment. See *United States v Ramirez* 532 US 65, 71-73 (1998).

135 *Wilson v Arkansas* 514 US 927, 934 (1995).

136 Officers may need to conduct no knock searches in computer crime cases because technically adept suspects may "hot wire" their computers in an effort to destroy evidence. Technically adept computer hackers have been known to use "hot keys" (computer programs that destroy evidence when a special button is pressed). If officers knock at the door to announce their search, the suspect can simply press the button and activate the program to destroy the evidence. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 40.

137 In *Richards v Wisconsin* 520 US 385, 394-396 (1997), the Supreme Court made it clear that the reasonableness of the decision by a law enforcement officer to dispense with the knock-and-announce rule must be evaluated as of the time that the officer entered the area to be searched. Accordingly, law enforcement officers may exercise independent judgment and decide to conduct a no knock search when they execute the search, even if they did not request such authority or the magistrate specifically refused to authorise a no-knock search. The question in all such cases is whether there was a reasonable suspicion that knocking and announcing the presence of law enforcement officers, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence.

138 In this respect, search warrants under Rule 41 of the Federal Rules of Criminal Procedure differ from federal search warrants issued under section 2703(a) of 18 USC, which may be served outside the issuing district. See the discussion in paragraph 5.3.4.1.5 below. In *United States v Walters* 558 F Supp 726, 730 (D Md 1980), a limit in a case involving telephone records was suggested. See also USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 39.

When, prior to the search, it becomes known that some of or all the data described by the warrant is stored in a location other than that where the search will be performed, the best course of action depends upon where the remotely stored data is located. When the data is stored remotely in two or more different places within the United States and its territories, law enforcement officers should obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(a) of the Federal Rules of Criminal Procedure. A thorough explanation of the location of the data and the proposed means of conducting the search should be provided in the affidavits accompanying the warrants. Matters become more complicated when it becomes known, prior to the search, that some of or all the data is stored remotely, outside the United States.[139] When law enforcement officers do not or cannot know that data searched for in one district within the United States is actually located outside that district, evidence seized remotely from another district should ordinarily not lead to suppression of the evidence obtained.[140]

5.2.3.4.4 Sneak and peek

A court may grant the delay of notice associated with the execution of a search warrant[141] if it finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have one of the adverse effects enumerated in section 2705 of 18 USC. These adverse effects include endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation or otherwise seriously jeopardising an investigation or unduly delaying a trial.

Law enforcement officers must provide delayed notice within a reasonable period following the execution of a warrant,[142] although a court can delay further notification for a good cause.

---

139 The mutual legal assistance requirements applicable in these circumstances do not constitute part of the scope of this study (see footnote 5 in paragraph 5.1 above). Suffice it to say that the United States may be required to take action ranging from informal notice, to a formal request for assistance to the country concerned. It must be borne in mind that some countries may object to attempts by United States law enforcement to access computers located within their borders. Also, although a search may seem domestic to a United States law enforcement officer executing the search in the United States pursuant to a valid warrant, other countries may view matters differently. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 40.

140 Courts generally deny motions to suppress when law enforcement cannot know whether the search violates Rule 41 either legally or factually. Evidence thus acquired from a network search that accessed data stored in multiple districts should not lead to suppression, unless the agents intentionally and deliberately disregarded Rule 41(a) of the Federal Rules of Criminal Procedure or if prejudice resulted for the accused. See *United States v Trost* 152 F3d 715, 722 (7th Cir 1998) and USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 40.

141 Section 3103a of 18 USC (as amended by section 213 of the USA PATRIOT Act). Under the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (see also footnote 17 in paragraph 5.1 above), officials must notify the person whose premises are being searched within a reasonable time that is not to exceed 30 days, unless a longer time is expressly approved by the court issuing the warrant. See Belt "Domestic Security" found on the Internet http://www.pbs.org/newshour/bb/terrorism/homeland/patriotact.html 3.

142 Section 3103a of 18 USC. This standard may reduce some of the inconsistencies among jurisdictions in rules governing sneak and peek warrants that existed prior to the USA PATRIOT Act. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 41. A reasonable period is a flexible standard to meet the circumstances of each individual case. Prior to the amendment of section 3103a, it was held in *United States v Villegas* 899 F2d 1324, 1337 (2nd Cir 1990) that a seven-day delay, subject to extensions, was reasonable. In *United States v Freitas* 800 F2d 1451, 1456 (9th Cir 1986), the Court ruled that a reasonable period should not exceed seven days, except upon a strong showing of necessity. In *United States v Simons* 206 F3d 392, 403 (4th Cir 2000), however, it was held that a 45-day delay in notice of execution of warrant does not render the search unconstitutional.

Delaying notice of a search must be discerned from delaying notice of a seizure. Unless a court finds a reasonable necessity for a seizure, sneak and peek warrants must prohibit the seizure of any tangible property, any wire or electronic communication, or any stored wire or electronic information.[143] Every attempt should be made to ensure that the period of delayed notice is as brief as reasonably possible.

5.2.3.4.5 Search and sift

Special care must be exercised when planning a search for electronic evidence that may result in the seizure of legally privileged documents. Law enforcement officers should devise a special strategy for reviewing the seized *e*-evidence following the search so that no breach of a privilege occurs. This post-seizure strategy to screen out privileged files should be described in the affidavit. Typically this entails the use of a trustworthy third party to comb through the files to separate those files within the scope of the warrant from files that contain privileged material. After reviewing the files, the third party offers those files that fall within the scope of the warrant to the law enforcement officers.[144] Generally, there are three options to facilitate this post-seizure screening:

(a) The court itself may review the files *in camera*. Due to the ever-expanding extensive storage capacities of storage media, judges only rarely undertake an *in camera* review of computer files.[145]

(b) A "taint team" or "privilege team", consisting of a team of prosecutors or law enforcement officers who are not working on the case, may assist in performing the search and reviewing the files afterwards. The taint team sets up a so-called "Chinese Wall" between the evidence and the prosecution team, permitting only unprivileged files that are within the scope of the warrant to slip through the wall. A taint team can usually screen the seized computer files fairly quickly. Although most prosecutors prefer to use a taint team if the court consents, some courts have expressed discomfort with taint teams.[146] Although no single standard has emerged, the general indication is that evidence screened by a taint team is admissible only if law enforcement shows that its procedures adequately protected the defendants' rights and that no prejudice to them

---

143 Except as expressly provided for in chapter 121 of 18 USC. If law enforcement officers intend to make surreptitious copies of information stored on a suspect's computer, the officers must obtain authorisation from the court in advance. USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 41.

144 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 42.

145 In *Black v United States* 172 FRD 511, 516-17 (SD Fla 1997), an *in camera* review was accepted due to unusual circumstances. In *United States v Skeddle* 989 F Supp 890, 893 (ND Ohio 1997), an *in camera* review was declined.

146 See *United States v Neill* 952 F Supp 834, 841 (DDC 1997). In *United States v Hunter* 13 F Supp 2d 574, 583 n2 (D Vt 1998), with reference to *In re Search Warrant for Law Offices Executed on March 19 1992* 153 FRD 55, 59 (SDNY 1994), the Court held that a review by a magistrate or special master may be preferable to reliance on a taint team.

occurred.[147] One approach to limit the amount of potentially privileged material in dispute is to have defence counsel review the output of the taint team to identify those documents for which counsel intends to raise a claim of privilege. Files thus identified that do not seem relevant to the investigation need not be litigated. Although this approach may not be appropriate in every case, judicial officers may appreciate the fact that defence counsel has been given the opportunity to identify potential claims before the court decides what to provide to the prosecution team.

(c) In unusual circumstances, the presiding judge may appoint a neutral third party known as a "special master" to undertake the task of reviewing the files.[148] Special masters, however, often take several years to complete their review.[149]

Confidential information from disinterested third parties constitutes an example of legally privileged material that may call for a search and sift strategy. Under the Attorney General's regulations,[150] federal law enforcement officers should not use a search warrant to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer or member of the clergy where the material sought or likely to be reviewed during the execution of the warrant contains confidential information on patients, clients or parishioners.[151] A narrow exception is provided for in that a search warrant can be used in the following circumstances:

(a) if using less intrusive means would substantially jeopardise the availability or usefulness of the materials sought;

(b) if access to the documentary materials appears to be of substantial importance to the investigation; and

---

147 *United States v Neill* 952 F Supp 834, 840-842 (DDC 1997) FN142(5) and *United States v Hunter* 13 F Supp 2d 574, 583 (D Vt 1998).

148 See *United States v Abbell* 914 F Supp 519 (SD Fla 1995) and *DeMassa v Nunez* 747 F2d 1283 (9th Cir 1984). The law enforcement officers charged with executing the search must provide the special master with copies of all the files seized pursuant to a warrant, while retaining a complete backup copy of those files under seal. The special master must review the files provided to her and must determine whether each file is encompassed by the provisions of the search warrant or, if not, falls within some valid exception to the search warrant which would justify the file's review by the officers executing the warrant. The special master must also determine whether each file is protected by an applicable evidentiary or constitutional privilege and, if so, if any exception to that privilege defeats its application and allows the files to be reviewed by the officers executing the warrant. See Brenner and Frederiksen 2001/2002 *Michigan Telecommunications and Technology Law Review* 102-106.

149 See *Black v United States* 172 FRD 511, 514, 516-517 (SD Fla 1997).

150 The Attorney General issued guidelines for federal law enforcement officers who want to obtain documentary materials from such disinterested third parties. See section 2000aa-11(a), section 59(4)(b) of 28 United States Code of Federal Regulations (hereinafter referred to as CFR) and the *United States Attorney's Manual* section 9-13 420 (1997). A copy of the *United States Attorney's Manual* can be found on the Internet http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/index.html.

151 See section 59.4(b) of 28 CFR. Kerr points out that the Tenth Circuit (in *United States v Carey* 172 F3d 1268 (10th Cir 1999) is the only circuit court, thus far, that has suggested that the search and seizure of a computer may require special rules because digital evidence of crime may be commingled with legitimate materials on a computer hard drive or other storage device. He argues that the need for a "special approach" applies only when law enforcement actually starts to search the computer files and then finds out that the materials that the officers are looking for are commingled with other unrelated materials. See Kerr 2003 *Journal of Internet Law* 25.

(c) if the application for the warrant has been recommended by the United States Attorney and approved by the appropriate Deputy Assistant Attorney General.[152]

Another example of privileged material calling for a search and sift strategy is First Amendment material that relates to freedom of speech and freedom of the press activities. The Privacy Protection Act[153] is aimed at protecting the press and certain other persons not suspected of committing a crime with protections not provided by the Fourth Amendment.[154] Publishers are granted certain statutory rights to discourage law enforcement officers from targeting publishers simply because they often gather mere evidence of crime. The use of personal computers for publishing and the World Wide Web (WWW) has dramatically expanded the scope of who is deemed to be involved in First Amendment activities. Nowadays, anyone with a computer and access to the Internet may be a publisher who possesses materials protected in terms of the Privacy Protection Act on her computer.[155]

Although the purpose of the Privacy Protection Act is not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation, law enforcement must take special steps when planning a search that officers have reason to believe may result in the seizure of certain First Amendment materials. Subject to certain exceptions, it is unlawful for a law enforcement officer to search for or seize materials when

(a) the materials are work product materials prepared, produced, authored, or created in anticipation of communicating such materials to the public;[156]
(b) the materials include mental impressions, conclusions, or theories of its creator;[157] and
(c) the materials are possessed for the purpose of communicating the material to the public by a person reasonably believed to have a purpose to disseminate to the public some form of public communication.[158]

---

152 See section 59.4(b)(1) and (2) of 28 CFR and USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 42.

153 Codified at section 2000aa of 42 USC. A copy of the Privacy Protection Act can be found on the Internet at http://www.4.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00002000--aa000-.html. Winnick opines that the Privacy Protection Act was enacted in order to lessen the chilling effect of intrusive searches on those engaged in First Amendment activities. The Act does not immunize the press from searches, but by requiring that searches be conducted via subpoena rather than by search warrant, the Act mandates that searches be conducted through a relatively unintrusive method. See Winick 1994 *Harvard Journal of Law & Technology* 101.

154 Before the Supreme Court decided *Warden v Hayden* 387 US 294, 309 (1967), law enforcement officers could not obtain search warrants to search for and seize mere evidence (as opposed to contraband, instrumentalities or fruits) of crime (see, for example, *Boyd v United States* 116 US 616 (1886)). In *Warden v Hayden* 387 US 294 (1967), the Court reversed course and held that the Fourth Amendment permitted the government to obtain search warrants to seize mere evidence. This ruling set the stage for a collision between law enforcement and the press, due to the fact that law enforcement officers could use search warrants to target the press for evidence of crime it had collected in the course of investigating and reporting news stories. In *Zurcher v Stanford Daily* 436 US 547 (1978), the Court held that neither the First or Fourth Amendment prohibited such searches, although it did note that the Fourth Amendment does not prevent or advise against legislative or executive efforts to establish non-constitutional protections for searches of the press. The Privacy Protection Act was passed in 1980 in response to *Zurcher v Stanford Daily* 436 US 547 (1978).

155 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 35.

156 Section 2000aa – 7(b)(1) of 42 USC.

157 Section 2000aa – 7(b)(3) of 42 USC.

Although these provisions are broad, the statute contains several exceptions in that searches will not violate the Privacy Protection Act when

(a) the only materials searched for or seized are contraband, instrumentalities or fruits of crime;[159]

(b) there is reason to believe that the immediate seizure of such materials is necessary to prevent death or serious bodily injury;[160]

(c) there is probable cause to believe that the person who possesses such materials has committed or is committing the criminal offence to which the materials relate (an exception which is itself subject to several exceptions);[161] and

(d) in a search for or the seizure of "documentary materials",[162] a subpoena has proven inadequate or there is reason to believe that a subpoena would not result in the production of the materials.[163]

Federal law enforcement searches that involve the Privacy Protection Act must be pre-approved by a Deputy Assistant Attorney General of the Criminal Division. The Computer Crime and Intellectual Property Section serves as the contact point for all such searches involving computers. Violations of the Privacy Protection Act do not necessarily result in suppression of the evidence,[164] but can result in civil damages against the sovereign whose officers executed the search.[165] If law enforcement officers violate the Privacy Protection Act and the state does not waive its sovereign immunity and is thus immune from a suit,[166] individual officers can be held liable for acts within the scope or under the colour of their employment, subject to a reasonable good faith defence.[167]

The Privacy Protection Act applies only when law enforcement intentionally targets First Amendment material that relates to a crime and not where the seizures result from a search for and the seizure of contraband or evidence of a crime that incidentally happens to be commingled with protected materials.[168] When officers collaterally seize First Amendment protected materials because they are commingled on a computer with other materials properly

---

158 Sections 2000aa – 7(b)(3) and 2000aa(a) of 42 USC.
159 Section 2000aa – 7(a)(b) of 42 USC.
160 Sections 2000aa(a)(2) and 2000aa(b)(2) of 42 USC.
161 Sections 2000aa(a)(1) and 2000aa(b)(1) of 42 USC.
162 As defined by section 2000aa-7(a).
163 Section 2000aa(b)(3) – (4) of 42 USC.
164 Section 2000aa – 6(d) of 42 USC.
165 Section 2000aa – 6(a)(e) of 42 USC. In *Davis v Gracey* 111 F3d 1472, 1482 (10th Cir 1997), a suit against municipal officers in their personal capacities in terms of the Privacy Protection Act was dismissed because it was held that such suits must be filed only against the "government entity", unless the government entity has not waived sovereign immunity.
166 *Barnes v State of Missouri* 960 F2d 63, 65 (8th Cir 1992).
167 Section 2000aa – 6(a)(2),(b) of 42 USC. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 35.
168 Investigations into illegal businesses that publish images of child pornography over the Internet have revealed that such businesses frequently support other publishing materials (such as drafts of adult pornography) that may be protected in terms of the Privacy Protection Act. Seizing the computer for the contraband necessarily results in the seizure of commingled protected materials. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 37.

targeted by law enforcement, such protected materials may not necessarily relate to any crime at all.[169] The so-called suspect exception eliminates liability in terms of the Privacy Protection Act when there is probable cause to believe that the person who possesses such materials has committed or is committing the criminal offence to which the materials relate.[170]

Incidental seizure of protected materials on a non-suspect's computer is an uncertain area of the law. In one case, when the owner of the seized computer was not a suspect, a district court held the United States Secret Service liable for the inadvertent seizure of materials protected by the Privacy Protection Act.[171] To date, no other court has followed this approach.[172] Law enforcement officers can often avoid the seizure of materials protected in terms of the Privacy Protection Act on a non-suspect's computer by using a subpoena or process under the

---

169 Materials protected by the Privacy Protection Act might be drafts of a horticulture newsletter that just happen to sit on the same hard drive as images of child pornography or records of a fraud scheme. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 37.

170 In *Guest v Leis* 255 F3d 325, 341-342 (6th Cir 2001), two lawsuits were brought against the Sheriff's Department in Hamilton County, Ohio. The suits arose from the seizures of two servers that had been used to host bulletin board systems suspected of housing evidence and contraband relating to obscenity, phone tapping, child pornography, credit card theft and software piracy. It was explicitly held that the incidental seizure of material protected in terms of the Privacy Protection Act that was commingled on a suspect's computer with evidence of a crime does not give rise to liability. It was noted that when law enforcement executes a search warrant for documents on a computer, it is often difficult or impossible (particularly without the cooperation of the owner) to separate the offending materials from other "innocent" material on the computer at the site of the search. These pragmatic concerns could essentially prevent law enforcement officers from seizing evidence located on a computer. The Court cautioned, however, that although the incidental seizure of protected material did not violate the Privacy Protection Act, the subsequent search of such material was forbidden. Also, in *United States v Hunter* 13 F Supp 2d 574, 582 (D Vt 1998), the Court concluded that materials for a weekly legal newsletter published by the defendant from his law office related to the defendant's alleged involvement in his client's drug crimes when the former was inadvertently seized in a search for evidence of the latter.

171 See *Steve Jackson Games Inc v Secret* Service 816 F Supp 432, 441 (WD Tex 1993). Steve Jackson Games, Inc. ("SJG") was primarily a publisher of role playing games, but it also operated a network of thirteen computers that provided its customers with email, published information about SJG products and stored drafts of upcoming publications. Believing that the system administrator of SJG's computers had stored evidence of crimes, the Secret Service obtained a warrant and seized two of the thirteen computers connected to SJG's network, in addition to other materials. The Secret Service did not know that SJG's computers contained publishing materials until the day after the search. However, the Secret Service did not return the computers it seized until months later. At no time did the Secret Service believe that SJG itself was involved in the crime under investigation. The district court ruled that the Secret Service had violated the Privacy Protection Act, but the Court's exact reasoning is difficult to discern. The Court, for example, did not explain exactly which of the materials the Secret Service had seized were deemed to be protected by the Privacy Protection Act. Similarly, the Court indicated that the search of SJG and the initial seizure of its property did not violate the Privacy Protection Act, but that the Secret Service's continued retention of SJG's property after it had learned of SJG's publisher status, despite a request by SJG for return of the property, was the true source of the violation. The Court also suggested that it might have ruled differently if the Secret Service had made copies of all information seized and returned the hardware as soon as possible, but did not answer whether in fact it would have reached a different result in such case. On appeal, the only issue raised was whether the seizure of stored private email, which had been sent to an electronic bulletin board, but had not yet been retrieved by the recipients, constituted an intercept in terms of section 2511(1)(a) of 18 USC. See *Steve Jackson Games Inc v Secret Service* 36 F3d 457, 460 (5th Cir 1994) and Freeman *Information Systems Security* 14-16.

172 In *State Ex Rel Macy v One (1) Pioneer CD-ROM Changer* 891 P2d 600, 607 (Okla Civ App 100 1994), the apparent premise of *Steve Jackson Games* that the seizure of computer equipment could violate the Privacy Protection Act merely because the equipment also contained or was used to disseminate potential documentary materials was questioned. In *Davis v Gracey* 111 F3d 1472, 1482 (10th Cir 1997), a suit in terms of the Privacy Protection Act improperly filed against municipal employees in their personal capacities was dismissed for lack of jurisdiction. In *Berglund v City of Maplewood* 173 F Supp 2d 935, 949-950 (D Minn 2001), the Court held that the police seizure of a defendant's videotape fell under the criminal suspect and destruction of evidence exceptions to the Privacy Protection Act, because the tape might have contained documentary evidence of the defendant's disorderly conduct. In *DePugh v Sutton* 917 F Supp 690, 696-97 (WD Mo 1996), the Court rejected a challenge in terms of the Privacy Protection Act to seizure of materials relating to child pornography, because there was probable cause to believe that the person possessing the materials had committed the criminal offence to which the materials related. In *Powell v Tordoff* 911 F Supp 1184, 1189-1190 (ND Iowa 1995), a claim in terms of the Privacy Protection Act was dismissed because the plaintiff did not have the standing to challenge search and seizure under the Fourth Amendment. In *Lambert and Palmer Communications Incorporated v Polk County, Iowa, The City of Des Moines* 723 F Supp 128, 132 (SD Iowa 1989), a claim based on the Privacy Protection Act was rejected after the law enforcement officers seized videotape which the officers could not reasonably have believed was intended for dissemination to the public.

Electronic Communications Privacy Act to require the non-suspect to produce the desired information.[173]

5.2.4 Search and seizure of e-evidence without a warrant

The development of warrantless search powers in the United States has been constrained by the reasonableness requirement of the Fourth Amendment. Because warrantless searches have been viewed essentially as exceptions to the normative warrant procedure,[174] the Supreme Court has long recognised the need for warrantless searches and seizures in the physical world where law enforcement agencies can prove that circumstances justify the waiving of the warrant requirement.[175] The Supreme Court has ruled only on a few matters involving technology, but the circuit courts have ruled extensively and conflictingly on warrantless searches involving electronic evidence.[176] In examining warrantless search and seizure, the issue of privacy is one of the greatest considerations and it drives the arguments behind most warrantless search doctrines.[177]

The following warrantless search and seizure doctrines are considered below:[178] searches incident to arrests,[179] inventory searches,[180] exigent circumstances searches,[181] the plain view doctrine,[182] consensual searches,[183] and private searches.[184]

---

173 See the discussion in paragraph 5.3 below. USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 38.

174 *Coolidge v New Hampshire* 403 US 443 (1970).

175 In *Parkhurst v Trapp* 77 F 3d 707 (3rd Cir 1996), three law enforcement officers searched a suspect's home without a search warrant and in the absence of the suspect. The Court determined there were no exigent circumstances and that the government bore the responsibility of proving that there was justification for a warrantless search.

176 Some of these judgements are discussed below, in the context of the warrantless exception to which they relate.

177 Moore *Search and Seizure of Digital Evidence* 137.

178 Two other warrantless search and seizure doctrines provided for in the United States legislative framework are school searches and border searches. The area of warrantless school searches is one area of jurisprudence that is in a state of considerable transformation. It is generally accepted that a warrantless search may be based upon as little as reasonable suspicion. None of the cases has yet involved direct mention of computers or technological devices, but opinions issued by the courts have laid a foundation for developments in the future. The search of a computer in a school search setting would require a belief that the device contains some form of information that is in violation of state or federal law, endangers the other students, or violates an established rule in the school system. See Moore *Search and Seizure of Digital Evidence* 125. The term "border search" refers to searches conducted at international border crossings and not to searches conducted on boundaries between states. Searches that are especially intrusive, however, require at least reasonable suspicion. These rules apply to people and property both entering and exiting the United States. Conducting searches and seizures at border points has a limited impact on the investigation of high technology crimes that are investigated by state and local law enforcement agencies. Border searches do not solve most "high tech" crime investigations. Occasionally, an officer may uncover evidence of child pornography or identity theft during the course of one of these searches, but rarely does an investigation hinge on evidence uncovered during a warrantless border search. See Moore *Search and Seizure of Digital Evidence* 146. Moore points out that despite several searches, there appears to be only one case concerning the issue of computer technology and warrantless border searches. In the case of *United States v Roberts* 86 F Supp 2d 678 (SD Texas 2000), an individual was arrested as he attempted to leave the United States for Paris with child pornography on zip disks stored within his shaving kit. After Robert's disks were seized, he admitted that he had child pornography on the disks, but argued that they were for his own viewing pleasure and were not for sale. At his trial he moved to have the evidence dismissed because the officers had no right to stop him as he was leaving the country. The Court determined that Roberts's claim had no merit and that customs officials had a right to search the outgoing baggage of anyone entering or leaving the United States. Relying on prior cases in Fourth Amendment jurisprudence that stated that computer storage media could be treated in the same way as filing cabinets; the Court determined that computers and storage disks could be searched at the border without a search warrant.

179 Paragraph 5.2.4.1.1 below.

180 Paragraph 5.2.4.1.2 below.

181 Paragraph 5.2.4.1.3 below.

182 Paragraph 5.2.4.1.4 below.

183 Paragraph 5.2.4.1.5 below.

184 Paragraph 5.2.4.1.6 below.

5.2.4.1 Warrantless search and seizure doctrines

5.2.4.1.1 Searches incident to arrests

After a lawful arrest, law enforcement officers may, without a warrant,[185] conduct a full search of the arrested person and a more limited search of her surrounding area.[186] It is generally accepted that in order for a search incident to an arrest to be considered lawful, there must be a lawful arrest and the search must be contemporaneous with the arrest.[187] If law enforcement officers attempt to make a warrantless search on the basis of an illegal arrest, the evidence is considered to have been seized outside the parameters of the Fourth Amendment and is not admissible in trial.[188]

Although searches incident to arrests have been justified on the basis of law enforcement safety, a search for weapons is not the only item justified under this warrantless search doctrine. The seizure of any destructible evidence found during a search incident to an arrest may also be permissible.[189]

Due to the increasing use of handheld and portable computers, pagers, cellular phones and other electronic storage devices, officers often encounter computers when they conduct searches incident to lawful arrests. The question is whether the search incident to arrest exception to the warrant requirement permits both the seizure and the search of such storage

---

185 In *United States v Robinson* 414 US 218, 234-235 (1973), a police officer, while conducting a pat-down search incident to an arrest for a traffic offence, discovered a crumpled cigarette package in the suspect's breast pocket. Not knowing what the package contained, the officer opened the package and discovered fourteen capsules of heroin. The Supreme Court held that the search of the package was permissible, even though the officer had no articulable reason to open the package. In light of the general need to preserve evidence and prevent harm to the arresting officer, the Court reasoned, it was *per se* reasonable for an officer to conduct a full search of the person pursuant to a lawful arrest. The Court also ruled that the search was not excessive, as there is no requirement that officers only conduct a search for evidence of the crime for which the defendant was arrested. See also Kuras *et al* 2002 *Georgetown Law Journal* 1130-1209 for an overview of the warrantless doctrines.

186 In *Agnello v US* 269 US 20 (1925), the Supreme Court, whilst recognising a right to search both a person lawfully arrested and the place where the arrest is made, stressed that this right is an incident of the arrest. Thus, a search of an accused's premises several blocks from the scene of the arrest and after all the accused were in custody elsewhere violated the Fourth Amendment. It has been affirmed in more recent jurisprudence that draws a distinction between those circumstances where there is opportunity to obtain a warrant (*Trupiano v US* 334 US 699 (1947) and those of urgency and hot pursuit (*Warden v Hayden* 387 US 294 (1967)). See also Sharpe *Search and Surveillance* 35. Moore, however, submits that the extension of the search incident to arrest doctrine is certain to be tested in the near future as courts reconsider the question whether searches ought to be allowed beyond the room in which the arrest takes place. In *Chimel v California* 395 US 752, 762-763 (1969), the United States Supreme Court held that searches could not extend beyond the room in which the arrest was executed. Today, however, there is an increased possibility of weapons being stored in adjacent rooms. See Moore *Search and Seizure of Digital Evidence* 94 and 95.

187 In *United States v Moorehead* 57 F 3d 875 (1995), the defendant was stopped for speeding. Because the suspect had no driver's license, the officer ran a background check on the basis of an identification card. The background check revealed that there was a warrant for the defendant's arrest. After arresting the defendant, a search of the vehicle turned up a firearm. Being a felon, the defendant was not allowed to be in possession of a firearm. The court found that the search was valid because there was a lawful arrest and the search was contemporaneous with the arrest.

188 Moore *Search and Seizure of Digital Evidence* 94.

189 In *United States v Bizier* 111 F 3d 214 (1st Cir 1997), the defendant and a friend were pulled over for speeding. The officers were alerted that the individual was under investigation for the sale of narcotics (on the basis of information obtained from an informant). After removing the individuals from the car, the defendant granted consent to search the vehicle. After searching the vehicle, officers found narcotics on the defendant's person. The Court found that the search incident to arrest doctrine not only applies to searches for weapons, but also to searches involving the protection of evidence.

media. The accessing of stored memory on electronic pagers has been found permissible,[190] but it is uncertain whether warrantless searches of electronic storage devices that contain more information than pagers is permitted. In the paper world, extensive searches of written materials discovered incident to lawful arrests have been allowed when they seemed reasonable.[191] If officers can examine the contents of wallets, address books and briefcases without a warrant, it could be argued that they should be able to search the electronic counterparts of such items as well. While a search of physical items found on the arrestee's person may always be reasonable, more invasive searches under different circumstances may violate the Fourth Amendment.[192]

In criticising a reliance on the decision in *United States v Tank*[193] in extending searches incident to arrest to computer storage media, Moore[194] argues that few situations would allow for the search of a technological device. He asserts that it is unreasonable to believe that digital evidence can provide a physical threat to law enforcement officers, and that an officer could search an entire CD-ROM, much less an entire laptop, incident to an arrest. Due to the considerable storage capacities of contemporary technological devices, the length of time between the seizure of a disk and the search of its contents also poses problems.[195] Numerous courts have held that lengthy searches after an arrest are invalid because the exigency of the situation diminishes and disappears over time.

---

190 Relying on *United States v Robinson* 414 US 218, 235 (1973), courts have uniformly permitted officers to access electronic pagers carried by the arrested person at the time of arrest. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 20. In *United States v Reyes* 922 F Supp 818, 833 (SDNY 1996), the accessing of numbers in a pager found in a bag attached to defendant's wheelchair within twenty minutes of his arrest was allowed within the search incident to arrest exception. See also *United States v Chan* 830 F Supp 531, 535 (ND Cal 1993), *United States v Lynch* 908 F Supp 284, 287 (DVI 1995), *Yu v United States* 1997 WL 423070 at *2 (SDNY Jul 29 1997) and *United States v Thomas* 114 F3d 403, 404 n2 (3rd Cir 1997). In *United States v Ortiz* 84 F3d 977, 984 (7th Cir 1996), the accessing of a pager was allowed on the basis of the exigency theory.

191 See *Swain v Spinney* 117 F3d 1, 6 (1st Cir 1997). Courts have uniformly held that officers may inspect the entire contents of a suspect's wallet found on her person. See *United States v Castro* 596 F2d 674, 676 (5th Cir 1979) and *United States v Molinaro* 877 F2d 1341, 1347 (7th Cir 1989). Similarly, in *United States v Rodriguez* 995 F2d 776 778 (7th Cir 1993), the Court held that officers could photocopy the entire contents of an address book found on the defendant's person during the arrest and others have permitted the search of a defendant's briefcase that was at the person's side at the time of arrest. See also *United States v Johnson* 846 F2d 279, 283-84 (5th Cir 1988) and *United States v Lam Muk Chiu* 522 F2d 330, 332 (2nd Cir 1975).

192 In *Mary Beth G v City of Chicago* 723 F2d 1263, 1269-71 (7th Cir 1983), it was held that the precedent set in *United States v Robinson* 414 US 218, 235 (1973) does not permit strip searches incident to arrest, because such searches are not reasonable within the context.

193 In *United States v Tank* 200 F 3d 627 (9th Cir 2000), the Court ruled that a law enforcement officer did not violate the Fourth Amendment when he searched an individual's pockets and the contents of an address book found within a pocket. It was the belief of the Court that the search was conducted in accordance with a valid arrest and was therefore acceptable. The Court also held that a zip disk found in the car was properly seized, but failed to discuss whether the law enforcement officers had obtained a warrant before searching the disk for images of child pornography. The Court relied on the prior decision in *Illinois v Lafayette* 462 US 640, 103 S Ct 2605, 77 L Ed 2d 65 (1983), where it was ruled that any article or container in an individual's possession during the booking process was subject to a warrantless search. This decision was, however, handed down at a time when there was little or no consideration of technology. The defendant was arrested for disturbing the peace and had his shoulder bag searched upon his arrival at the police station. The search of the shoulder bag revealed narcotics. The Supreme Court found that the Fourth Amendment was not violated, because law enforcement officers maintained a right to search any containers found in the possession of a suspect when conducting inventory procedures after a valid arrest.

194 Moore *Search and Seizure of Digital Evidence* 116.

195 A search of a floppy disk that only stored up to 1.4 MB of data, which is the equivalent of 500 pages of text or 25 to 30 image files, could be completed in twenty minutes in accordance with the time grace allowed in *United States v Reyes* 922 F Supp 818, 833 (SDNY 1996). See also Moore *Search and Seizure of Digital Evidence* 145. See paragraph 2.5.1.1. above for a reference to different storage media.

Law enforcement officers are encouraged to seize the technological device upon the arrest of the individual in order to protect the data on the disk or device, but to obtain a search warrant before they search the contents of the device.[196]

5.2.4.1.2 Inventory searches

Law enforcement officers routinely inventory the items they have seized. Such inventory searches must follow standardised procedures[197] and must serve a legitimate, non-investigatory purpose that outweighs the intrusion on the individual's Fourth Amendment rights.[198] Typically, an inventory search could be aimed at guarding law enforcement officers from danger, or at protecting an owner's property while the owner is in custody, so as to protect law enforcement officers and agencies against claims for lost, stolen, or vandalised property.

It is unlikely that a search through seized computer files would be supported under this doctrine.[199] Even assuming that standard procedures authorised such a search, the legitimate purposes served by inventory searches in the physical world do not translate well into the intangible realm. Information does not generally need to be reviewed to be protected and does not pose a risk of physical danger. It is advisable that law enforcement officers generally obtain a search warrant in order to examine seized computer files held in custody.[200]

5.2.4.1.3 Exigent circumstances searches

Under the exigent circumstances exception to the warrant requirement, a warrantless search and seizure would be allowed if the circumstances would cause a reasonable person to believe that entry was necessary to

(a) prevent physical harm to the law enforcement officers or other persons;
(b) prevent the destruction of relevant evidence;
(c) prevent the escape of the suspect; or
(d) some other consequence that would improperly frustrate legitimate law enforcement efforts.[201]

---

196 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 20. Moore *Search and Seizure of Digital Evidence* 118.

197 See *Colorado v Bertine* 479 US 367, 374 (1987) and *Florida v Wells* 495 US 1, 4-5 (1990).

198 See *Illinois v Lafayette* 462 US 640, 644 (1983) and *South Dakota v Opperman* 428 US 364, 369-70 (1976).

199 In *United States v O'Razvi* 1998 WL 405048 at *6-7 (SDNY 1998), the difficulties of applying the inventory search requirements to computer disks were noted. In *United States v Flores* 122 F Supp 2d 491, 493-95 (SDNY 2000), a search of a cellular telephone was found to be purely investigatory in nature and thus not a lawful inventory search.

200 An owner could claim that her computer files were altered or deleted while in police custody because examining the contents of the files would offer little protection from tampering. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 20. Producing a forensic image of the *e*-evidence seized could, in exceptional circumstances, prove helpful, as the hash value of the data will indeed prove its integrity. See the discussion relating to computer forensic images in paragraph 2.3.1.2.1 above.

201 In *United States v Alfonso* 759 F 2d 728 (9th Cir 1985), the defendant was arrested in his hotel room after a search by customs revealed that the ship in which he had arrived was loaded with narcotics. The defendant claimed that the search of the hotel was illegal. The Court disagreed, finding that law enforcement officers are allowed to conduct a warrantless search when it

The following factors are considered in determining whether circumstances qualify as exigent: the degree of urgency; the amount of time needed to obtain a warrant, whether the evidence is about to be moved or destroyed, the possibility of danger at the scene, whether the suspect knows that a law enforcement officer is after the evidence and the ready destructibility of the evidence.[202]

Exigent circumstances often arise in computer cases because electronic data is perishable. Computer commands can destroy data in a matter of seconds, as can humidity, extreme temperatures, physical mutilation or magnetic fields.[203] The main issue with regard to the exigent circumstance seizure of digital evidence is how likely it is that the data would be lost if law enforcement officers were to take the time to obtain a warrant. It is important that the existence of exigent circumstances does not permit officers to search or seize beyond what is necessary to prevent the destruction of the evidence. When the exigency ends, the right to conduct warrantless searches ends as well. The need to take certain steps to prevent the destruction of evidence does not authorise law enforcement officers to take further steps without a warrant.[204] Accordingly, the seizure of computer hardware to prevent the destruction of any information it contains does not ordinarily support a subsequent search of that information without a warrant.[205] Of course, in computer cases, as in all others, the existence of exigent circumstances is absolutely tied to the facts.[206]

---

becomes apparent that they have probable cause to suspect that evidence may be removed or damaged. See also *United States v McConney* 728 F2d 1195, 1199 (9th Cir 1984) (en banc).

202 In *United States v Reed* 15 F 3d 928 (9th Cir 1994), the manager of a hotel contacted law enforcement and told them of his concerns that guests were acting suspiciously. Using the hotel's master key, the manager went into the room. The officer stood in the doorway after entering just far enough to ensure the manager was safe. At this time, the officer merely watched the manager conduct a search. The Court denied the government's claim they were the beneficiaries of a private search. The Court laid out the factors to be considered in considering whether exigent circumstances exist.

203 Created, for example, where a strong magnet is passed over a disk.

204 See *United States v Doe* 61 F3d 107, 110-11 (1st Cir 1995).

205 For example, in *United States v David* 756 F Supp 1385, 1392 (D Nev 1991), law enforcement officers saw the defendant deleting files on his data memo book and seized the computer immediately. The District Court held that the officers did not need a warrant to seize the memo book because the defendant's acts had created exigent circumstances. The Court found that the seizure of the organiser was constitutional, as the evidence was in danger of being destroyed by the suspect, but the search of the device was unlawful. The Court dismissed the government's argument that exigent circumstances supported the search of a battery-operated computer because the agent did not know how much longer the computer's batteries would live. In *United States v Gorshkov* 2001 WL 1024026 at *4 (WD Wash 2001), the Court concluded that circumstances justified a warrantless download of data from a computer in Russia where probable cause existed that the Russian computer contained evidence of crime and good reason existed to fear that delay could lead to the destruction or loss of access to evidence. Law enforcement officers, in this case, merely copied the data and subsequently obtained a search warrant.

206 Not all lower courts have agreed with the decision in *United States v Ortiz* 84 F3d 977, 984 (7th Cir 1996), where law enforcement officers were ruled justified in retrieving numbers from a pager because pager information is easily destroyed during a search incident to an arrest. In *United States v Reyes* 922 F Supp 818, 835-36 (SDNY 1996), the Court concluded that exigent circumstances could not justify the search of a pager, as the exigency was created by the turning on of the pager. In *United States v Romero-Garcia* 991 F Supp 1223, 1225 (D Or 1997) the Court held that a search of a battery-operated computer without a search warrant was invalid. The Court rejected the law enforcement officer's claim that exigent circumstances were present because of the possibility of lost data should the battery have died. Ultimately, the Court determined that, unlike a pager, which loses its settings and data when the battery is turned off, a computer can maintain its data if the battery dies. When considering this, it is doubtful that an exigency claim to search a computer or laptop will ever be successfully argued.

The case of *Illinois v McArthur*[207] has added a new perspective to this area of law by stating that law enforcement officers may prevent a suspect from gaining access to an area that contains potential evidence during the time frame when another officer is obtaining a search warrant. The Court found that the inconvenience the suspect suffered from not being allowed to return inside his home until a warrant was obtained was outweighed by the potential discovery of important evidence. If a court finds that preventing a suspect from entering her home is not unreasonable, the removal of a computer from a suspect's possession until a search warrant is drafted should also be acceptable.[208] A law enforcement officer has the right to prevent a suspect from gaining access to potential evidence while a search warrant is being requested. For this reason, Moore[209] recommends that an investigator only use warrantless search doctrines to justify seizing a computer or other storage media. Once the device has been seized and is in custody, then a proper search warrant satisfying the requirements of particularity and specificity should be acquired.

5.2.4.1.4 Plain view doctrine

Under the plain view exception to the warrant requirement, additional evidence can be seized if the following two conditions are met:

(a) The incriminating nature of the evidence must be immediately apparent.[210] If an item is moved before the law enforcement officer is able to articulate its illegality, the evidence cannot be seized.

(b) The law enforcement officer must be in a lawful position to observe and access the evidence. Should the officer enter a residence without a warrant or permission, all evidence seized under the plain view doctrine is inadmissible, barring some other warrantless search exception that justifies the entrance into the home.[211]

---

207 531 US 326 (2001). The Supreme Court ruled in this case that an officer did not violate a suspect's rights when he prevented the suspect from re-entering his home while the officer was waiting for a search warrant. It was the Court's opinion that an officer may prevent an individual from gaining access to a residence if there is the possibility that a suspect could damage evidence.

208 Moore *Search and Seizure of Digital Evidence* 115.

209 Moore *Search and Seizure of Digital Evidence* 145.

210 An example is where a law enforcement officer conducts a valid search of a hard drive and comes across evidence of an unrelated crime while conducting the search. Such evidence may be seized under the plain view doctrine. See *Horton v California* 496 US 128 (1990).

211 In *Arizona v Hicks* 480 US 321 107 S Ct 1149, 94 L Ed 2d 347 (1987), the Supreme Court extended the plain view doctrine to legal searches. Officers entering an apartment discovered evidence of another crime. The Court determined that officers who are in a place where they are legally entitled to be might seize evidence as long as they do not move the evidence to determine its legality. In this case, the issue was whether moving a radio to see serial numbers violated plain view. The Court agreed that it did. In *United States v Bradshaw* 102 F 3d 204 (6th Cir 1996), law enforcement officers discovered narcotics lying on the seat beside the defendant during a traffic stop. Upon reaching in to seize the evidence, the officer noticed a handgun sticking out from the seat. The defendant attempted to argue that the plain view doctrine did not apply because the stop was inappropriate. The Court found that the stop was valid and the plain view search was therefore acceptable. The Court did imply that had the officer had no reason for the stop, then the search would have been invalid, because the officer was not in a place he maintained a legal right to be. In *United States v Villarreal* 963 F2d 770, 776 (5th Cir 1992), the Court concluded that labels fixed to opaque 55-gallon drums do not expose the contents of the drums to plain view. The Court noted that a label on a container is not an invitation to search it. If the government seeks to learn more than the label reveals by opening the container, it must generally obtain a search warrant.

A straightforward "plain view" seizure of a computer file is only likely to arise where law enforcement officers lawfully observe a monitor attached to an operating computer displaying material evidencing criminal activity. The grey areas typically arise in situations where an officer lawfully searching computer files pursuant to a warrant comes upon evidence of criminal activity unrelated to that specified in the warrant.[212]

It is important to note that law enforcement officers cannot rely upon the plain view exception to justify opening a closed computer file they are not otherwise authorised to view.[213] The contents of such a closed computer file that must be opened to be viewed are not in "plain view".[214] Courts have, however, reached different conclusions over whether each individual file stored on a computer should be treated as a separate closed container.[215] This distinction is important when considering the scope of the plain view exception.

In the case of *United States v Carey*,[216] the Court found that a law enforcement officer had exceeded the scope of his search warrant for digital evidence of narcotics when he searched a suspect's computer for digital evidence of child pornography. In this case the officer had acted under the authority of a search warrant that specified a search for evidence related to narcotics trafficking, but he had noticed a filename that he believed could be related to child pornography. *United States v Carey*[217] provides a cautionary example of the restrictive approach. As best as can be discerned, the rule advanced in this case seems to be that the law enforcement officer could seize the first file with a .jpg[218] file extension that came into plain view while the officer was executing the search warrant, but could not rely on the plain view exception to justify the search solely for additional .jpg files containing child pornography on the defendant's computer(s), which is evidence beyond the scope of the warrant.[219]

---

212 Patzakis and Limongelli 2005 *EnCase Legal Journal* 86-97. Courts are affording special protection to computer data stored on computers by narrowly construing the articulated terms of the warrant. See paragraph 5.2.3.1 above for a reference to the particularity and specificity requirements.

213 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 19.

214 See *United States v Maxwell* 45 MJ 406, 422 (CAAF 1996). Of course, law enforcement officers executing a search pursuant to a valid warrant or an exception to the warrant requirements need not rely on the plain view doctrine, as the warrant or the warrantless exception itself justifies the search.

215 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 19. See also paragraph 5.2.2 above generally regarding the right to privacy and, more specifically, for a reference to the closed container analogy in a computing context.

216 172 F3d 1268 (10th Cir 1999).

217 In *United States v Carey* 172 F3d 1268 (10th Cir 1999), a law enforcement officer searching a hard drive with a warrant for drug trafficking evidence opened a .jpg file and instead discovered child pornography. At that point, the officer spent five hours accessing and downloading several hundred .jpg files in a search not for evidence of the narcotics trafficking that he was authorised to seek and gather pursuant to the original warrant, but for more child pornography. When the defendant moved to exclude the child pornography files on the ground that they were seized beyond the scope of the warrant, the state argued that the detective had seized the .jpg files properly because the contents of the contraband files were in plain view. The Court rejected this argument in respect of all the files except for the first .jpg file the detective discovered.

218 .jpg or JPEG is a term for any graphic image file produced by using a JPEG standard. A JPEG file is created by choosing from a range of a suite of compression algorithms. See Web Services Definitions "JPEG" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,290660,sid26_gci212425,00.html 1.

219 In *United States v Walser* 275 F3d 981, 986-87 (10th Cir 2001), the Court found no Fourth Amendment violation when a law enforcement officer with a warrant to search for electronic records of drug transactions opened a single computer file containing child pornography, suspended the search and then returned to magistrate for a second warrant to search for child pornography.

Moore[220] submits that it is not necessarily true nowadays that there is no reason for a law enforcement officer to open a file with an extension outside the bounds of the relevant search warrant. Traditionally, an officer could identify these files by their file name extensions.[221] However, by merely changing the file name extension, files can be hidden.[222] Deceptive techniques like this complicate the forensic examiner's task, since every file on the computer must be examined in order to verify that the file is not a piece of evidence authorised under the search warrant.

The opening of files on a computer can be compared to the searching of many rooms within a residence. Because files can so easily be hidden, it becomes necessary to enter each "room" of a digital storage medium, just as an officer would enter rooms in search of a physical residence. If a law enforcement officer encounters evidence of an additional crime, then she should immediately end her search for evidence of the new crime and apply for an additional search warrant. To refuse the forensic examiner the opportunity to search each file would be the equivalent of refusing an officer access to certain rooms within a residence. Moore[223] expressed the hope that future courts, when next facing this issue, will consider these facts and continue the line of reasoning developed in the decision of *United States v Carey*.[224] Moore[225] further advises that law enforcement officers must exercise extreme care when opening files that are outside the scope of their warrant.

To attempt opening any file under the plain view doctrine, it is required that a law enforcement officer has gained access to the site via a search warrant, consent or another warrantless search exception. Although the discovery of digital storage media that could potentially contain evidence of a crime usually allows for the seizure of such media under the plain view exception, the examination of its content should be done under the authority of a separate search warrant. Where an officer is examining a computer for evidence of one crime and inadvertently discovers evidence of another crime, then evidence of the new crime is admissible under the plain view doctrine. This evidence, however, does not grant an officer the right to continue searching for additional evidence of this new crime. This newly discovered evidence is merely admissible after an application for an additional search warrant has been granted.[226]

Whereas *United States v Carey*[227] provides that a law enforcement officer may not manually search through individual files in an effort to obtain information outside a warrant's articulate

---

220 Moore *Search and Seizure of Digital Evidence* 147.
221 Such as, for example, .jpeg, .gif, .mpeg or .avi.
222 A .jpeg picture file can, for example, be altered with little or no prior technical experience to appear as a .doc document file. See paragraph 2.3.1.3 above for a reference to anti-forensic techniques.
223 Moore *Search and Seizure of Digital Evidence* 148.
224 *United States v Carey* 172 F3d 1268 (10th Cir 1999).
225 Moore *Search and Seizure of Digital Evidence* 120.
226 Moore *Search and Seizure of Digital Evidence* 120.
227 *United States v Carey* 172 F3d 1268 (10th Cir 1999) was followed in, for example, *People v Carratu* 194 Misc 595, 755 NYS 2d 800 (2003).

scope, Patzikis and Limongelli[228] argue that most judges are becoming more sophisticated regarding electronic evidence. These writers contend that while the decision in *United States v Carey*[229] has not been directly overruled, there are various cases that seek to distinguish it,[230] and they argue that there appears to be little chance that its reasoning will spread widely to other jurisdictions.[231]

Several courts have issued published decisions involving the search and seizure of computer media that feature a discussion of the *Carey* decision, while other courts have addressed the plain view doctrine in the context of forensic searches of computer files, without specifically referring to the *Carey* decision. While not addressing the *Carey* decision, the decision in *United States v Scott*[232] provides an indication that text string searches performed across an entire hard drive or other form of media would not subject the forensic examiner to questions of exceeding the scope of a warrant, as long as such text searches were generally within the course of the investigation delineated by the warrant.

In a case similar to the *Carey* case, but with a different ruling, the Court in *United States v Gray*[233] found that a law enforcement officer did not violate the scope of a search warrant when he seized all the files on a suspect's computer while he was looking for evidence of intrusion into a federal computer. During the course of the officer's search for evidence of hacking, he discovered several images of child pornography. The Court denied the defendant's motion to have all the evidence of child pornography excluded because a successful search pursuant to the officer's warrant would have required him to examine every possible location for potential evidence. It was during a just search that each of the images of child pornography was discovered.[234]

Also in contrast to the approach taken in *Carey* decision, the Court of Appeals for the Armed Forces held, in the case of *United States v Maxwell*,[235] that an officer had violated the Fourth Amendment when he opened files found under a different Internet screen name. The officer argued that the files from the additional screen name were admissible because they came into plain view during his search for child pornography, which was authorised by a search warrant.

---

228 See generally Patzikis and Limongelli 2005 *EnCase Legal Journal* 86-101.

229 *United States v Carey* 172 F3d 1268 (10th Cir 1999).

230 See *United States v Gray* 78 F Supp 2d 524 (ED Va 1999), *Wisconsin v Shroeder* 2000 WL 675942 (Wisconsin Supreme Court Decision), *United States v Balon* 384 F3d 38 41 (2nd Cir 2004) and *Frazier v State* 172 F3d 1268 (10th Cir 1999). The Court's reasoning in the *Carey* decision has been rejected in *United States v Hill* 322 F Supp 1081 (CD Cal 2004), although the Court did not directly refer to the *Carey* decision by name. In *United States v Rossby* 81 Fed Appx 109, 110 (9th Cir 2003) the Court was not persuaded by the defendant's reliance on the *Carey* decision and noted that "even in the Tenth Circuit, *Carey* has been limited to its facts".

231 Patzikis and Limongelli 2005 *EnCase Legal Journal* 101.

232 83 F Supp 2d 187 (D Mass 2000).

233 78 F Supp 2d 524 (ED Va 1999).

234 Moore *Search and Seizure of Digital Evidence* 76.

235 See *United States v Maxwell* 45 MJ 406 (CAAF 1996). Although this case is a military Court decision, it has been referenced in several cases concerning the plain view doctrine and as such bears careful consideration. Moore *Search and Seizure of Digital Evidence* 147. See also a discussion of this case in Jackson 1999 *Temple Environmental Law and Technology Journal* 97.

It was the opinion of the Court that the files were not admissible under the plain view doctrine, because the files had to be opened in order for them to be seen. The Court applied this doctrine in accordance with the case of *United States v Villarreal*,[236] in which the Court found that the plain view exception does not apply when law enforcement officers have to open a closed container. The Court suggested that the plain view of a single file on a computer or storage device could provide a basis for a more extensive search.[237] Thus, a more extensive search of the computer or storage device by law enforcement was found not to violate the Fourth Amendment.

5.2.4.1.5 Consensual searches

Law enforcement officers may search a place or object without a warrant or even probable cause if a person with authority has voluntarily consented to the search. Whether consent was voluntarily given is a question of fact that must be decided by considering the totality of the circumstances, including the following important factors: the age, education, intelligence, physical and mental condition of the person giving consent, whether the person was under arrest and whether the person has been advised of her right to refuse consent.[238] The individual giving consent must be capable of understanding that she is granting consent to a search that could result in evidence's being collected that may be used against her.[239] Law enforcement generally bears the burden of proving that the suspect did in fact grant consent and understood what the consent related to.[240]

---

236 In *United States v Villarreal* 963 F 2d 770 (5th Cir 1992), the United States customs service was alerted to the potential presence of narcotics in a 55-gallon drum. Upon the arrival of the customs officers, a search of the drum was conducted and marijuana was discovered. The officers then closed the drum and made a controlled delivery. Defendants appealed, arguing that their Fourth Amendment rights had been violated by the initial search. The Court determined that an individual does maintain privacy in mailed items, but that private carriers are allowed to search items that are mailed. In the case at hand, however, the search was conducted by government agents and was ruled unconstitutional.

237 *United States v Runyan* 275 F3d 449, 464-65 (5th Cir 2001) and *United States v Slanina* 283 F3d 670, 680 (5th Cir 2002). In these two cases, the Court held that when a warrantless search of a portion of a computer or storage device had been proper, the defendant no longer retained any reasonable expectation of privacy in the remaining contents of the computer or storage device (*Slanina* at 680; *Runyan* at 464-65).

238 In *Ohio v Robinette* 519 US 33 (1996), law enforcement officers stopped the defendant for speeding. After issuing the citation, the officer asked the defendant whether there were any narcotics or weapons in the car. After the defendant responded "no" the officer asked to search the car. Later, the defendant attempted to argue that the search was illegal because he was unaware of his right to refuse consent. The Supreme Court found that an officer does not have to inform a suspect of their "right to go" before obtaining consent. In *Schneckloth v Bustamonte* 412 US 218, 226 (1973), the defendant was charged with possession of stolen cheques. The checques were obtained after an officer stopped the defendant and asked permission to search the car. At trial, the defendant also attempted to argue that he was not aware of his right to refuse consent. The Supreme Court found that consent searches should be examined by taking a totality of the circumstances approach. Officers must ensure that the individual is old enough and intelligent enough to understand exactly what their consent agreement covers. Several states require that officers provide suspects with information informing them that they may refuse the consent request. The reasoning for this would appear to be that providing the suspect with information concerning a right to refuse consent assures the courts that the individual is mature enough to understand the gravity of the consent which she is granting. See also Moore *Search and Seizure of Digital Evidence* 108.

239 In *Boyd v United States* 116 US 616 (1886), the issue was whether a law requiring a suspect to provide papers as evidence against themselves was invalid under the Fourth Amendment. While some justices felt the issue was more akin to a criminal proceeding, under the Fifth Amendment, the Court also found that the use of such laws would result in a defendant's granting too broad a consent. To use consent the individual must be aware of the ability to deny permission.

240 See *United States v Matlock* 415 US 164, 177 (1974) and *United States v Price* 599 F2d 494, 503 (2nd Cir 1979). However, in *Bumper v North Carolina* 391 US 543 (1968), the defendant was convicted of rape. During the trial he argued that evidence introduced in trial was obtained illegally because his grandmother had granted consent. The Supreme Court found that the grandmother could have granted consent but the government failed to prove that law enforcement had proved the grandmother understood her consent and her right to refuse. In fact, the officers informed the grandmother that they were in possession of a search warrant and therefore did not need her consent.

There are several dangers inherent in using consent in place of a written search warrant. The greatest risk lies in the ability of the owner of the property to withdraw her consent to the search. In the physical realm, it may take an investigator three to four minutes to search an address book based on consent, whilst searches of *e*-evidence may take much longer. There is accordingly a greater possibility that the owner may change her mind and revoke the search and/or claim afterwards that she attempted to revoke her consent but was denied the opportunity to do so. An individual withdraws her consent when one or more of the following occurs: she withdraws consent verbally; she withdraws consent through an act such as grabbing the law enforcement officer's hand to stop the search of a specific area;[241] or she flees during the search.[242] The existence of a signed consent form does not remove the owner's right to revoke consent.[243] It is recommended that a law enforcement officer who attempts to search for and seize a digital device should use consent only as a means of seizing the device. The subsequent search of the contents should be conducted under the auspices of a properly drafted search warrant. This method may slow the process of the investigation down somewhat, but this slowness is preferable to having the evidence removed from trial completely.[244]

The permitted scope of consent searches depends on the facts of each case.[245] The scope of consent to search is generally defined by its expressed object and is limited by the breadth of the consent given.[246] The standard for measuring the scope of consent under the Fourth Amendment is objective reasonableness.[247] This requires a fact-intensive inquiry into whether it was reasonable for the law enforcement officer to believe that the scope of consent included the items searched. Of course, when the limits of the consent are clearly given, either before or during the search, these bounds must be respected.[248] Once consent is given, an officer must take care and ensure that she does not overstep the bounds of the consent agreement.[249] This

---

241 In *Jimenez v State* 643 So 2d 70 (Fla 2d DCA 1994), an off-duty law enforcement officer discovered cocaine while conducting pat-down searches of individuals who attended a dance. The individual initially consented to the search as a condition of entering the building for the dance. During the pat-down, however, the officer discovered two cigarette packs. When the officer attempted to search the packs, the individual moved his hand to prevent the officer from finishing the search. The officer completed the search and discovered the cocaine. It was the opinion of the Court that the defendant's placing of his hand over the pack was equivalent to withdrawing consent and there was no need for verbal withdrawal.

242 In *Davis v State* 497 So 2d 1344 (Fla 5d DCA 1986), law enforcement officers encountered the defendant when an officer mistook the defendant for a narcotics suspect. While the officer was searching the defendant's person, the defendant ran away. When the defendant was caught, he was searched. The Court found that the officers had no grounds to detain the defendant and his consent to be searched was revoked when he ran.

243 Moore *Search and Seizure of Digital Evidence* 149.

244 Moore *Search and Seizure of Digital Evidence* 149.

245 The suspect's consent to examine the pager he was carrying does not necessarily extend to consent to search the contents of the pager. In *Schneckloth v Bustamonte* 412 US 218 (1973), the Court opined that the individual's consent to look inside his vehicle was an implied consent for the law enforcement officer to examine the contents of the pager found within. It is recommended that any search that could result in possible confusion be documented with an in-depth written consent form completed by the law enforcement officer and the suspect. The consent form should include the area to be searched, what it is the officer intends to search for, and the officer's desire to search within any computer or technological device found within the area.

246 *United States v Pena* 143 F3d 1363, 1368 (10th Cir 1998).

247 *Florida v Jimeno* 500 US 248, 251 (1991).

248 *Vaughn v Baldwin* 950 F2d 331, 333 (6th Cir 1991).

249 In *United States v Carey* 172 F 3d 1628 (10th Cir 1999) the Court ruled on plain view with regard to digital searches (see the discussion in paragraph 5.2.4.1.4 above). Officers investigating evidence of an assault encountered evidence of an additional crime while searching a suspect's computer. The investigator then immediately abandoned his search for evidence of assault and began searching for evidence of the new crime. It was the opinion of the Court that had the investigator stopped with the

is an important issue in high-tech crimes because of the large-scale storage capabilities of today's computers.[250]

Consent may be explicit or implicit.[251] Individuals often enter into agreements with the government in which they waive some of their Fourth Amendment rights.[252] Similarly, users of computer systems may waive their rights to privacy as a condition of using certain computer systems. When individuals who have waived their rights are searched and then challenge the searches on Fourth Amendment grounds, courts typically focus on whether the waiver eliminated the individual's reasonable expectation of privacy against the search.[253] A few courts have approached the same problem from a slightly different angle and have asked whether the waiver established implied consent to the search.

It is good practice for law enforcement officers to use written consent forms that state explicitly that the scope of consent includes the consent to search computers and other electronic storage devices.[254] In the absence thereof, courts look to whether the particular circumstances of the officer's request for consent limited the scope of the search to a particular type, scope or duration.

According to the doctrine of implied consent, consent to a search may be inferred from an individual's conduct.[255] This approach ultimately relies on fact-driven notions of common sense

---

initial discovered evidence, the evidence would have been admissible on an application for a search warrant. The Court found that an investigating officer overstepped the bounds of the search agreement when he took the suspect's computer off the property before he searched it, but after the suspect had granted consent to search and seize any property "in his house".

250 See paragraph 2.5.1.1. above for a reference to the storage capacities of some of the different storage media available today.

251 In *State v Hammonds* 557 So 2d 179 (Fla Ed DCA 1990), the defendant granted law enforcement officers the right to search her two pieces of luggage. After searching the first bag, the defendant began searching the second bag. When the officer indicated he would rather search the bag himself, the defendant said nothing, but subsequently indicated she was embarrassed because of her undergarments in the bag. The Court found the initial search legitimate but found the second garment bag to have been illegally searched. The Court did not agree that the defendant's silence granted consent to a search. See also *United States v Milian-Rodriguez* 759 F2d 1558, 1563-64 (11th Cir 1985).

252 An example is where visitors to government buildings agree to a limited search of their person and property as a condition of entrance.

253 In *American Postal Workers Union Columbus Area Local AFL-CIO v United States Postal Service* 871 F2d 556, 56-61 (6th Cir 1989), it was held that postal employees retained no reasonable expectation of privacy in government lockers after signing waivers.

254 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 14.

255 In *United States v Ellis* 547 F2d 863, 865, 866-867 (5th Cir 1977), a civilian visiting a naval air base agreed to post a visitor's pass on the windshield of his car as a condition of bringing the car on to the base. The pass stated that "acceptance of this pass gives your consent to search this vehicle while entering, aboard, or leaving this station". During the visitor's stay on the base, a station investigator who suspected that the visitor had stored marijuana in the car approached the visitor and asked him if he had read the pass. After the visitor admitted that he had, the investigator searched the car and found 20 plastic bags containing marijuana. The Court ruled that the warrantless search of the car was permissible, because the visitor had impliedly consented to the search when he knowingly and voluntarily entered the base with full knowledge of the terms of the visitor's pass. However, notwithstanding this case, it must be noted that several courts have been critical of the implied consent doctrine in the Fourth Amendment context. Other courts have proven reluctant to apply the doctrine absent evidence that the suspect actually knew of the search and voluntarily consented to it at the time the search occurred. In *McGann v Northeast Illinois Regional Commuter Rail Road Corporation D/B/A Metra/Metropolitan Rail* 8 F3d 1174, 1180 (7th Cir 1993), the Court was confronted with claims of implied consent and was reluctant to uphold a warrantless search based simply on actions taken in the light of a posted notice. In *Securities and Law Enforcement Employees, District Council 82 v Carey* 737 F2d 187, 202 n23 (2nd Cir 1984), the argument that prison guards impliedly consented to being searched by accepting employment at a prison where consent to search was a condition of employment was rejected. In the absence of such evidence, these courts have preferred to examine general waivers of Fourth Amendment rights solely under the reasonable expectation of privacy test.

and often hinges upon subtle distinctions.[256] By relying on analogous cases involving closed containers, the argument that the scope of consent included consent to search electronic storage devices can be strengthened.[257] Special care should be exercised when relying on consent as the basis for a search of a computer when the consent has been obtained for one reason, but the search is then conducted for another reason.[258]

Another issue in the use of consent searches is third party consent. The term "third party consent" is used to describe a search that is not authorised by the suspect of the crime, but that is authorised by another individual who has common control over the area to be searched. When examining third party consent to search technological devices, there are several considerations, but perhaps the most important is whether the individual has the right to grant consent to search the computer in question.[259]

Most spousal and domestic partner consent searches are valid. In the absence of an affirmative showing that the consenting spouse has no access to the property searched, the courts generally hold that either spouse may consent to a search of all the couple's property.[260]

---

256 In *United States v Reyes* 922 F Supp 818, 834 (SDNY 1996), the Court held that consent to look inside a car included consent to retrieve numbers stored inside pagers found in the car's back seat. However, in *United States v Blas* 1990 WL 265179 at *20 (ED Wis Dec 4 1990), the Court ruled that consent to look at a pager did not include consent to activate the pager and retrieve numbers, because looking at the pager could be construed to mean what the device is, or how small it is, or what brand of pager it may be. In *United States v Carey* 172 F3d 1268, 1274 (10th Cir 1999), a written consent form was read extremely narrowly, so that consent to seizure of any property under the defendant's control and to a complete search of the premises and property at the defendant's address merely permitted the law enforcement officers to seize the defendant's computer from his apartment, not to search the computer off-site because it was no longer located at the defendant's address.

257 In *United States v Galante* 1995 WL 507249 at *3 (SDNY 1995), it was held that a general consent to search a car included consent to have the officer access the memory of a cellular telephone found in the car, relying on a precedent involving closed containers. See also *United States v Reyes* 922 F Supp 818, 834 (SDNY 1996).

258 In *United States v Turner* 169 F3d 84, 86, 88 (1st Cir 1999), law enforcement officers searching for physical evidence of an attempted sexual assault obtained written consent from the victim's neighbour to search the neighbour's "premises" and "personal property". Before the neighbour signed the consent form, the officers discovered a large knife and blood stains in the neighbour's apartment, and explained to him that they were looking for more evidence of the assault that the suspect might have left behind. While several officers searched for physical evidence, one officer searched the contents of the neighbour's personal computer and discovered stored images of child pornography. The neighbour was charged with possessing child pornography. On interlocutory appeal, the Court held that the search of the computer exceeded the scope of consent and suppressed the evidence. According to the Court, the officers' statements that they were looking for signs of the assault limited the scope of consent to the kind of physical evidence that an intruder might have left behind. By transforming the search for physical evidence into a search for computer files, the detective had exceeded the scope of consent. In *United States v Carey* 172 F3d 1268 (10th Cir 1999) the Court concluded that law enforcement officers had exceeded the scope of consent by searching a computer after the defendant had signed a broadly-worded written consent form, because officers told the defendant that they were looking for drugs and drug-related items, rather than computer files containing child pornography.

259 In *United States v Smith* 27 F Supp 2d 1111 (CD Ill (1998), the Court found there was no violation of the Fourth Amendment when law enforcement officers searched a suspect's computer on the basis of consent obtained from the suspect's girlfriend. The Court based its decision upon the fact that the two individuals lived together and that the suspect had taken no steps to ensure that his files were password-protected, thereby making the files inaccessible to others in the house. Other Courts have further ruled that neither ownership nor family relationship can overcome this requirement of access. In *United States v Durham* 139 F3d 1325 (10th Cir 1998), the Court found that a mother could not grant consent to the search of a computer, despite the fact that she owned some of the computer equipment. It was the Court's belief that the suspect had taken adequate steps to ensure that his mother could not gain access to the computer. The child in question paid a small rental fee to his parents for his room, which was a factor the Court deemed important to the loss of control over the child's belongings. These belongings included the computer in question. Despite the mother's owning a portion of the computer, the loss of control over the room rendered the mother's consent invalid.

260 In *United States v Duran* 957 F2d 499, 504-05 (7th Cir 1992) the Court concluded that the wife could consent to the search of the barn she did not use because her husband had not denied her the right to enter the barn. In *United States v Long* 524 F2d 660, 661 (9th Cir 1975), it was held that the wife, who had left her husband, could consent to the search of their jointly-owned home, even though the husband had changed the locks. In *United States v Smith* 27 F Supp 2d 1111, 1115-1116 (CD Ill 1998), a suspect was living with a woman and her two daughters. When allegations of child molestation were raised against the suspect, the woman consented to the search of his computer, which was located in the house in an alcove connected to the master bedroom. Although the woman used the suspect's computer only rarely, the Court held that she could consent to the search of the suspect's computer. Because the woman was not prohibited from entering the alcove and

When the perpetrator is a minor, parental consent to search the perpetrator's property and living space is almost always valid.[261] If children are 18 or older and reside with their parents as adults, the parents may or may not be able to consent, depending on the facts.[262] Although courts have offered divergent approaches, they have paid particular attention to three factors: the suspect's age; whether the suspect pays rent; and whether the suspect has taken affirmative steps to deny her parents access to her room or private area. When suspects are older, pay rent, and/or deny access to parents, courts have generally held that parents may not consent.[263] By contrast, parents may usually consent if their adult children do not pay rent, are fairly young, and have taken no steps to deny their parents access to the space to be searched.[264]

It is common for several people to use or own the same computer equipment. If the individual lives in the same residence, has access to the room in which the computer is placed, and has access to the data on the computer, law enforcement officers should not encounter any problems with regard to the validity of the search. If any one of those people gives the law enforcement officers permission to search for data, the officers may generally rely on that consent, provided that the person has authority over the computer. All users have assumed the risk that a co-user might discover everything in the computer and might also permit law enforcement to search this common area.[265]

Because the joint access test does not require a unity of interests between the suspect and the third party, third party consent is permitted even when the target of the search is present and

---

the suspect had not password-protected the computer, the Court reasoned she had authority to consent to the search. Even if the woman lacked actual authority to consent, the Court added, she had apparent authority to consent.

261 It has been noted that the courts have rejected even rather extraordinary efforts by minor children to establish exclusive use. See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 16.

262 Under *United States v Matlock* 415 US 164 (1974), it is clear that parents may consent to a search of common areas in the family home regardless of the perpetrator's age. In *United States v Lavin* 1992 WL 373486 at *6 (SDNY Nov 30 1992), the right of the parents to consent to the search of the basement room where their son kept his computer and files was recognised.

263 In *United States v Whitfield* 939 F2d 1071, 1075 (DC Cir 1991), the Court held the "cursory questioning" of the suspect's mother insufficient to establish the right to consent to a search of her 29-year-old son's room. In *United States v Durham United States v Durham* 139 F 3d 1325 (10TH Cir 1998), the mother had neither the apparent nor the actual authority to consent to the search of her 24-year-old son's room, because the son had changed the locks to the room without telling his mother, and the son also paid rent for the room.

264 In *United States v Rith* 164 F3d 1323, 1331 (10th Cir 1999), the Court suggested that the parents were presumed to have authority to consent to a search of their 18-year-old son's room because he did not pay rent. In *United States v Block* 590 F2d 535, 541 (4th Cir 1978), the Court ruled that the mother could consent to law enforcement officers' search of her 23-year-old son's room when the son did not pay rent. However, she could not consent to a search of a locked footlocker found in the room.

265 The watershed case in this area is *United States v Matlock* 415 US 164, 171 (1974), in which the Supreme Court stated that anyone who has common authority over premises or effects may consent to a search, even if an absent co-user objects. According to the Court, the common authority that establishes the right of third-party consent requires mutual use of the property by persons who generally have joint access or control for most purposes, so that it is reasonable to recognise that any of the co-inhabitants has the right to permit the inspection in her own right and that the others have assumed the risk that one of their number might permit the common area to be searched. Under this approach, a private third party may consent to a search of property under the third party's joint access or control. Law enforcement officers may view what the third party may see without violating any reasonable expectation of privacy so long as they limit the search to the zone of the consenting third party's common authority. In *United States v Jacobsen* 466 US 109, 119 (1984), the Court noted that the Fourth Amendment is not violated when a private third party invites law enforcement officers to view the contents of a package under the third party's control.

refuses to consent to the search.[266] Although the co-users of a computer generally have the ability to consent to a search of its files,[267] a search warrant should be obtained before continuing the search if any of the files are password-protected or if the entire computer is password-protected. Regardless of whether the password may be obtainable from or by a third party, a court could easily view the use of a password as an attempt to ensure privacy from a third party.[268] When an individual protects her files with passwords and has not shared the passwords with others who also use the computer, the authority of those other users to consent to a search of the computer does not extend to password-protected files.[269] Conversely, if the co-user has been given the password by the suspect, then she probably has the requisite common authority to consent to a search of the files.[270] This rule often requires a law enforcement officer to inquire into third parties' rights of access before conducting a consent search and to draw lines between areas that fall within the third party's common authority and those areas outside the third party's control. As a practical matter, officers may have little way of knowing the precise bounds of a third party's common authority when the officers obtain third-party consent to conduct a search. When queried, consenting third parties may falsely claim that they have common authority over property.[271]

Every computer network is managed by a system administrator or system operator whose job it is, *inter alia*, to keep the network running smoothly, to monitor security and to repair the network when problems arise. System operators have root level access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems. When law enforcement officers suspect that a network account contains relevant evidence, they may feel inclined to seek the system administrator's consent to search the contents of that account.

As a practical matter, the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional. System administrators typically serve as agents of providers of electronic communication services under the Electronic Communications

---

266 In *United States v Sumlin* 567 F2d 684, 687-88 (6th Cir 1977), it was held that a woman had authority to consent to the search of the apartment she shared with her boyfriend, even though her boyfriend refused consent.

267 In *United States v Smith* 27 F Supp 2d 1111, 1115-16 (CD Ill 1998), the Court concluded that a woman could consent to a search of her boyfriend's computer, located in their house, and noted that the boyfriend had not password-protected his files.

268 Moore *Search and Seizure of Digital Evidence* 112 and 113.

269 In *Trulock v Freeh* 275 F3d 391, 403-404 (4th Cir 2001), password-protected files were compared to locked footlockers inside a bedroom, which the Court had previously held to be outside the scope of common authority consent.

270 In *United States v Murphy* 506 F2d 529, 530 (9th Cir 1974) (*per curiam*), the Court concluded that an employee could consent to a search of an employer's locked warehouse because the employee possessed the key (which was delivered to the employee by the employer himself).

271 In *Illinois v Rodriguez* 497 US 177, 188-189 (1990), the Supreme Court held that the Fourth Amendment does not automatically require suppression of evidence discovered during a consent search when it later comes to light that the third party who consented to the search lacked the authority to do so. Instead, the Court held that the officers can rely on a claim of authority to consent, based on the facts available to the officer at the moment, if a man of reasonable caution would believe that the consenting party had authority to consent to a search of the premises. When officers reasonably rely on apparent authority to consent, the resulting search does not violate the Fourth Amendment. See also *Terry v Ohio* 392 US 1, 21-22 (1968) and USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 15.

Privacy Act[272] and any attempt to obtain a system administrator's consent to search an account must be compliant with these provisions. The resulting consent searches in most cases do comply with the Fourth Amendment. Most fundamentally, it may be argued that individuals retain no reasonable expectation of privacy in the remotely stored files and records that their network accounts contain. If an individual does not retain a constitutionally reasonable expectation of privacy in her remotely stored files, it does not matter whether the system administrator has the necessary joint control over the account, because a subsequent search will not violate the Fourth Amendment. In the event that a court holds that an individual does possess a reasonable expectation of privacy in remotely stored account files, whether a system administrator's consent would satisfy the joint access requirement would depend on the circumstances. Clearly, the system administrator's access to all network files does not in itself provide the common authority that triggers authority to consent.[273]

The company may grant the system administrator of the company network full rights to access employee accounts for any work-related reason and the employees may know that the system administrator has such access. In circumstances such as this, the system administrator is likely to have sufficient common authority over the accounts to be able to consent to a search.[274] As for obtaining consent in private sector workplaces, law enforcement officers can defeat a reasonable expectation of privacy argument by obtaining the consent of a party who exercises common authority over the area to be searched.[275] Private-sector employers and supervisors generally enjoy a broad authority to consent to searches in the workplace.[276] An employment

---

272 See sections 2701-2712 of 18 USC which regulates law enforcement efforts to obtain the consent of a system administrator to search an individual's account. See also paragraph 5.3 below for a discussion of these sections.

273 Prior to the case of *United States v Matlock* 415 US 164 (1974), the Supreme Court held in *Stoner v California* 376 US 483, 490 (1964) that a hotel clerk lacked the authority to consent to the search of a hotel room. Although the clerk was permitted to enter the room to perform his duties, and the guest had left his room key with the clerk, the Court concluded that the clerk could not consent to the search. If the hotel guest's protection from unreasonable searches and seizures was left to depend on the unfettered discretion of an employee of the hotel, the Court reasoned, the required protection would "disappear". In *Chapman v United States* 365 US 610 (1960), the Court ruled that a landlord lacks the authority to consent to a search of premises used by a tenant. In *United States v Most* 876 F2d 191, 199-200 (DC Cir 1989), it was held that a store clerk lacks authority to consent to a search of packages left with the clerk for safekeeping. To the extent that the access of a system operator to a network account can be compared to the access of a hotel clerk to a hotel room, the claim that a system operator may consent to a search of Fourth Amendment-protected files is weak. Of course, the hotel clerk analogy may be inadequate in some circumstances. For example, an employee generally does not have the same relationship with the system administrator of her company's network as a customer of a private Internet Service Provider might have with the system administrator of the Internet Service Provider. In *United States v Barth* 26 F Supp 2d 929, 938 (WD Texas 1998), it was held that a computer repairman's right to access files for the limited purpose of repairing the computer did not create the authority to consent to a government search through those files.

274 By comparison, see *United States v Clarke* 2 F3d 81, 85 (4th Cir 1993). In this case the Court held that a drug courier hired to transport the defendant's locked toolbox containing drugs had common authority to consent to a search of the toolbox stored in the courier's trunk.

275 *United States v Matlock* 415 US 164, 171 (1974). In practice, this means that law enforcement officers can often overcome the warrant requirement by obtaining the consent of the suspect's employer or supervisor. Depending on the facts, a co-worker's consent may suffice as well. See Burnes 2002 *Privacy and Data Protection* 12 and Stahlman 2001 *Army Lawyer* 21-23.

276 For example, in *United States v Gargiso* 456 F2d 584 (2nd Cir 1972), law enforcement officers conducting a criminal investigation of an employee of a private company sought access to a locked, wired-off area in the employer's basement. The officers explained their needs to the company's vice-president, who took the officers to the basement and opened the basement with his key. When the employee attempted to suppress the evidence that the officers discovered in the basement, the Court held that the vice-president's consent was effective. Because the vice-president shared supervisory power over the basement with the employee, the Court reasoned that he could consent to the officers' search of that area (at 586-587). In *United States v Bilanzich* 771 F2d 292, 296-97 (7th Cir 1985), it was held that the owner of a hotel could consent to the search of a locked room used by a hotel employee to store records, even though the owner did not carry a key, because the employee worked at the owner's bidding. In *JL Foti Constr Co v Donovan* 786 F2d 714, 716-17 (6th Cir 1986) (*per curiam*), it

policy or computer network banner that establishes the employer's right to consent to a workplace search can help to establish the employer's common authority to consent.

Law enforcement should be careful to rely on a co-worker's consent to conduct a workplace search. While employers generally retain the right to access their employees' work spaces, co-workers may or may not have such a right, depending on the facts. When co-workers do exercise common authority over a workspace, however, investigators can rely on a co-worker's consent to search that space.[277] The expectation of privacy of an employee may be completely removed with well-drafted policies concerning the rights of employers to search computers and work areas at any time for any legitimate reason in both private and public workplaces. These policies may range from documents distributed at the time of hiring an employee that indicate the employer's ability to conduct such searches, or the employer may elect to use a banner[278] to inform their employees. Either method will greatly diminish the expectation of privacy an individual may maintain in the workplace.[279]

In the case of a government network, the Fourth Amendment rules are likely to differ from the rules that apply to private networks.[280] Although public employers may search employees' workplaces without a warrant for work-related reasons, public workplaces offer a more restrictive milieu in one respect. In government workplaces, employers acting in their official capacity generally cannot consent to a law enforcement search of their employees' offices.[281] The question in such cases is not whether the public employer had common authority to consent to the search, but rather whether the combined law enforcement and employer search satisfied the Fourth Amendment standards of *O'Connor v Ortega.*[282] An individual's reasonable expectation of privacy in a government work environment greatly diminishes when the

---

was held that a general contractor's superintendent could consent to an inspection of an entire construction site, including a subcontractor's work area.

277 For example, in *United States v Buettner-Janusch* 646, 765-766 F2d 759 (2nd Cir 1981), a professor and an undergraduate research assistant at New York University (NYU) consented to a search of an NYU laboratory managed by a second professor suspected of using his laboratory to manufacture drugs. Although the search involved opening vials and several other closed containers, the Court held that the search was authorised because both consenting co-workers had been authorised to make full use of the lab for their research. In *United States v Murphy* 506 F2d 529, 530 (9th Cir 1974) (*per curiam*), and *United States v Jenkins* 46 F3d 447, 455-58 (5th Cir 1995), an employee was allowed to consent to a search of the employer's property. In *United States v Longo* 70 F Supp 2d 225, 256 (WDNY 1999), a secretary was allowed to consent to a search of the employer's computer. But in *United States v Buitrago Pelaez* 961 F Supp 64, 67-68 (SDNY 1997), it was held that a receptionist could consent to a general search of the office, but not to a search of a locked safe to which the receptionist did not know the combination.

278 A banner is a message that appears on the screen of a computer when it is turned on and the user logs onto the system. This banner could inform users that their actions are subject to monitoring by employers.

279 Moore *Search and Seizure of Digital Evidence* 127.

280 In *O'Connor v Ortega* 480 US 709 (1987), the Court examined a search of a government physician's office and determined that an individual's expectation of privacy in the government workplace must be balanced against the employer's need to maintain control and order. A government search involving law enforcement officers does not in and of itself rule the search in violation of the Fourth Amendment, as each case requires an individual assessment of whether a reasonable expectation of privacy exists. USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 16.

281 In *United States v Blok* 188 F2d 1019, 1021 (DC Cir 1951), the Court concluded that a government supervisor cannot consent to a law enforcement search of a government employee's desk. The rationale for this is that the Fourth Amendment cannot permit one government official to consent to a search by another. Moore notes, however, that even a reasonable expectation of privacy does not bar a government employer from entering private workspace, if the intrusion is conducted as a means of investigating work-related activities or issues (Moore *Search and Seizure of Digital Evidence* 126).

282 480 US 709 (1987). See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 28-29.

individual's workspace is easily accessible to others in the office or to individuals who are allowed to enter the office space.[283]

It should be noted that at least one court has ruled that officers who relied on invalid consent did not violate the Fourth Amendment because they were acting in good faith and could not prove that the consent was invalid.[284]

5.2.4.1.6 Private searches

The Fourth Amendment is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual who is not acting as an officer of the government or with the participation or knowledge of any law enforcement officer. As a result, no violation of the Fourth Amendment occurs when a private individual acting on her own accord conducts a search and makes the results available to law enforcement.[285]

Law enforcement officers who learn of evidence via a private search can re-enact the original private search without violating any reasonable expectation of privacy. Law enforcement cannot, however, exceed the scope of the private search.[286] This standard requires law enforcement officers to limit their investigation to the scope of the private search when searching without a warrant after a private search has occurred. As long as the officers limit themselves to the scope of the private search, the search does not violate the Fourth

---

283 A good example of this would be a secretary who does not maintain a private office but only has a desk on which a computer is located. If this desk is located in a general area in which many people are constantly moving past and around the desk, the secretary may have a hard time arguing that she had a reasonable expectation of privacy and that the law enforcement officer's entry to a computer without a search warrant is in violation of the Fourth Amendment. Moore *Search and Seizure of Digital Evidence* 126.

284 In *United States v Elliot* 50 F 3d 180 (2nd Cir 1995), law enforcement officers conducted a search on the basis of consent. It was later determined that the individual in question did not have the necessary control over the area to validate the consent. The Court, however, ruled that the officers were acting in good faith, and therefore the search was validated. See also Moore *Search and Seizure of Digital Evidence* 98.

285 In *United States v Hall* 142 F3d 988, 933 (7th Cir 1998), the defendant took his computer to a private computer specialist for repairs. In the course of evaluating the defendant's computer, the repairman observed that many files stored on the computer had filenames characteristic of child pornography. The repairman accessed the files, saw that they did in fact contain child pornography and then contacted the state police. The tip led to a warrant, the defendant's arrest, and his conviction for child pornography offences. On appeal, the Court rejected the defendant's claim that the repairman's warrantless search through the computer violated the Fourth Amendment. Because the repairman's search was conducted on his own, the Court held, the Fourth Amendment did not apply to the search or his later description of the evidence to the state police. In *United States v Kennedy* 81 F Supp 2d 1103, 1112 (D Kan 2000), the Court concluded that searches of a defendant's computer over the Internet by an anonymous caller and employees of a private Internet service provider did not violate the Fourth Amendment because there was no evidence that the government was involved in the search. In *Walter v United States* 447 US 649 (1980), the defendant was arrested after a box containing videos of homosexual behaviour was accidentally delivered to the wrong company. Law enforcement officers obtained the videos and viewed them without a search warrant. The defendant argued that the search was illegal, because the government had no right to view the films without a search warrant. It was the opinion of the Court that the search was illegal, but the Court did maintain that private citizens are not governed by the Fourth Amendment. The Court also indicated it would have ruled differently had the private party first viewed the films before contacting law enforcement. Bayens argues that private computer owners as well as business owners need to be aware of the substantial risk in seeking computer assistance. The vast majority of computer-related problems could only be properly diagnosed and repaired by actually accessing specific files or file directories. It is accordingly no surprise that private computer technicians are rapidly becoming confidential informants for law enforcement agencies. Bayens opines that due to the number of these "dual purpose" technicians and the public's absolute reliance on these technicians for computer assistance, the analysis for when a private individual is converted into a government actor may need to be modified to protect privacy interests. See Bayens 2000 *Drake Law Review* 252.

286 In *United States v Jacobsen* 466 US 109, 115 (1984), the Supreme Court presented the framework that should guide law enforcement officers seeking to uncover evidence as a result of a private search. See also *United States v Miller* 152 F3d 813, 815-16 (8th Cir 1998) and *United States v Donnes* 947 F2d 1430, 1434 (10th Cir 1991).

Amendment. However, as soon as law enforcement exceeds the scope of the private warrantless search, any evidence uncovered may be vulnerable to a motion to suppress.

It is important to note that the fact that the person conducting a search is not a government employee does not always mean that the search is private for Fourth Amendment purposes. A search by a private party is considered a Fourth Amendment government search if the private party acts as an instrument or agent of the Government.[287]

In *United States v Runyan*,[288] it was held that law enforcement officers did not exceed the scope of a private search when they examined more files on privately searched disks than the private searchers had. A third party search of a single file on a computer accordingly allows a warrantless search by law enforcement of the computer's entire contents. Other courts, however, may not follow this approach and rule that government searchers can view only those files whose contents were revealed in the private search. In *United States v Barth*[289] it was held that law enforcement officers who viewed more files than the private searcher, exceeded the scope of the private search. The issue was whether an accountant's privacy was violated when a repairman searched his computer after inadvertently discovering images of child pornography during the course of a computer repair. The repairman in the case notified law enforcement and then continued to search for additional images of child pornography without a search warrant. The Court found the repairman's search illegal because he began working under colour of state law from the moment he notified law enforcement about the first image of child pornography on the computer's hard drive. One of the factors the Court mentioned was the fact that the repairman occasionally worked as an informant. The Court failed to place great emphasis on the issue, but it was mentioned when attempting to explain that the repairman should have known better than to continue searching for images of child pornography after the discovery of the original image. Law enforcement officers should ensure that individuals who alert them to the presence of digital evidence are aware of their responsibilities.

---

287 See *Skinner, Secretary of Transportation v Railway Labor Executives' Association* 489 US 602, 614-615 (1989). The Supreme Court merely stated that the question when private conduct can be attributed to the government necessarily turns on the degree of the government's participation in the private party's activities. This question must be resolved in the light of all the circumstances. In the absence of a more definitive standard, the various federal Courts of Appeal have adopted a range of approaches for distinguishing between private and government searches. Some circuit courts apply a totality of the circumstances approach that examines three factors: whether the government knows of or acquiesces in the intrusive conduct; whether the party performing the search intends to assist law enforcement efforts at the time of the search; and whether the government affirmatively encourages, initiates or instigates the private action (see *United States v Pervaz* 118 F3d 1, 6 (1st Cir 1997), *United States v Smythe* 84 F3d 1240, 1242-43 (10th Cir 1996), *United States v McAllister* 18 F3d 1412, 1417-18 (7th Cir 1994) and *United States v Malbrough* 922 F2d 458, 462 (8th Cir 1990)). Other circuits focused on only two of these factors. In *United States v Miller* 688 F2d 652, 657 (9th Cir 1982) and *United States v Paige* 136 F3d 1012, 1017 (5th Cir 1998), it was held that private action counts as government conduct if, at the time of the search, the government knew of or acquiesced in the intrusive conduct, and the party performing the search intended to assist law enforcement efforts. In *United States v Lambert* 771 F2d 83, 89 (6th Cir 1985), it was held that a private individual is a state actor for Fourth Amendment purposes if the law enforcement officer instigated, encouraged or participated in the search, and the individual engaged in the search with the intent of assisting the officer in her investigative efforts.

288 *United States v Runyan* 275 F3d 449, 464-65 (5th Cir 2001).

289 *United States v Barth* 26 F Supp 2d 929, 937 (WD Tex 1998). This case was decided prior to *United States v Runyan* 275 F3d 449, 464-65 (5th Cir 2001).

Even if courts follow the more restrictive approach, information gleaned from a private search is often useful in providing the probable cause needed to obtain a warrant for a further search. After viewing evidence of a crime stored on a computer, law enforcement officers may need to seize the computer temporarily to ensure the integrity and availability of the evidence before they can obtain a warrant to search the contents of the computer.[290] The Fourth Amendment permits officers to seize a computer temporarily as long as

(a) they have probable cause to believe that it contains evidence of a crime;
(b) they seek a warrant expeditiously; and
(c) the duration of the warrantless seizure is not unreasonable, given the totality of the circumstances.[291]

This issue becomes even more critical when electronic communications are involved. Under guidelines established by the Electronic Communications Privacy Act,[292] administrators of Internet accounts may notify law enforcement if they encounter any communications they believe contain valuable evidence of a crime. Once an administrator contacts law enforcement, the administrator is considered an actor under state law and may no longer turn over evidence without proper legal authorisation by a court order or search warrant.[293]

Although most private search issues arise when private third parties intentionally examine property and offer evidence of a crime to law enforcement, the same framework applies when third parties inadvertently expose evidence of a crime to plain view.[294]

5.3 Domestic production devices

5.3.1 Backgound

Instead of a physical home, when using the Internet, for example, "home" is typically a network account consisting of a block of computer storage that is owned by a network service provider. Homes in cyberspace do not necessarily have an equal amount of privacy protection from law

---

290 See *United States v Hall* 142 F3d 988 (7th Cir 1998) and *United States v Grosenheider* 200 F3d 321, 330 n10 (5th Cir 2000).

291 See *United States v Place* 462 US 696, 701 (1983), *United States v Martin* 157 F3d 46, 54 (2nd Cir 1998) and *United States v Licata* 761 F2d 537, 540-42 (9th Cir 1985).

292 See generally paragraph 5.3 below.

293 Moore *Search and Seizure of Digital Evidence* 122. McLean warns that although "trusted, non-targeted, inside personnel" can provide an enormous amount of detail about the computer system's configuration and structure, law enforcement officers should be careful in not making such cooperatives "agents of the government". See McLean "Basic Considerations in Investigating Computer Crime, Executing Computer Search Warrants and Seizing High Technology Equipment" found on the Internet http://www.bileta.ac.uk/99papers/maclean.html 4.

294 For example, in *United States v Procopio* 88 F3d 21, 26-27 (1st Cir 1996), a defendant stored incriminating files in his brother's safe. Later, thieves stole the safe, opened it, and abandoned it in a public park. Law enforcement officers investigating the theft of the safe found the files scattered on the ground nearby, gathered them, and then used them against the defendant in an unrelated case. The Court held that the use of the files did not violate the Fourth Amendment, because the files were made openly available by the thieves' private search.

enforcement.[295] The Fourth Amendment generally requires law enforcement officers to obtain a warrant to search a physical home, but it does not require a warrant to obtain the stored contents of a network account of a user. Instead, the Fourth Amendment generally permits the issuance of a subpoena directly to a network provider. The subpoena then orders the provider to divulge the contents of an account within a specified period of time.[296] As long as the subpoena is not overbroad, seeks relevant information and is served in a legal manner, the required information must be provided.[297] This applies equally to a case where a suspect has stored materials remotely with a third party.[298] By sending information to network providers, an account holder may have relinquished her reasonable expectation of privacy of information, as the sending of this information may constitute a disclosure to a third party.[299]

The stored communication portion of the Electronic Communications Privacy Act[300] constitutes a safety net for the uncertain application of the Fourth Amendment legal protections to cyberspace and it is aimed at addressing imbalances between cyberspace and the physical world. Network account holders have a range of statutory privacy rights in respect of access to stored account information held by network service providers.[301]

To protect the array of privacy interests identified by its drafters, the Electronic Communications Privacy Act offers varying degrees of legal protection, depending on the perceived importance of the privacy interest involved.[302] Generally, the greater the perceived privacy interest, the greater the privacy protection that is afforded. The proper procedure that law enforcement officers need to follow to obtain specific information is, first, to classify the network service provider; second, to classify the information sought; and third, to classify the action involved.[303] These steps are discussed below.[304]

---

295 See Bertron 1996 *American Criminal Law Review* 164 (this article is quite aptly given the title: "Home Is Where Your Modem Is".

296 See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 56.

297 See *United States v Dionisio* 410 US 1, 7-12 (1972) and *In re Horowitz* 482 F2d 72, 75-80 (2nd Cir 1973).

298 In *United States v Barr* 605 F Supp 114, 119 (SDNY 1985), a subpoena for the defendant's undelivered mail in the possession of a third party was served on a private third party mail service. In *United States v Schwimmer* 232 F2d 855, 861-63 (8th Cir 1956), a subpoena was served on a third party storage facility for the defendant's private papers in the third party's possession. In *Newfields v Ryan; Ballentine v Florida Tex Oil Co* 91F2d 700, 702-05 (5th Cir 1937), a subpoena was served on a telegraph company for copies of the defendant's telegraphs in the telegraph company's possession.

299 A container of electronic information may, for example, be offered to a third party by bringing a malfunctioning computer to a repair shop, or by shipping a floppy diskette in the mail to a supplier. A user may also transmit information to third parties electronically, such as by sending data across the Internet. See the discussion pertaining to the reasonable expectation of privacy and third-party possession in paragraph 5.2.2 above.

300 Sections 2701-2712 of 18 USC. The Electronic Communications Privacy Act applies to all parties, private and law enforcement alike.

301 See USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 56.

302 Stored emails harbour, for example, greater privacy interests than subscriber account information. Similarly, computing services available to the public require more strict regulation than services not available to the public. This probably reflects the view that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers' privacy. Some information can be obtained from providers with a mere subpoena; other information requires a special court order and still other information requires a search warrant. See Bayens 2000 *Drake Law Review* 275-278 and Hellums 2002 *William and Mary Bill of Rights Journal* 856.

303 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 57.

304 See paragraphs 5.3.2, 5.3.3 and 5.3.4 below.

Attempts to introduce legal regulation of encryption[305] in the United States have in the past attracted considerable opposition.[306] The nature of encryption technology is such that the most severe laws could not completely curtail its use. Although current policy in the United States allows consumers access to privacy-enhancing encryption, the government continues to impose restrictions on the export of encryption.[307] In 2000, the United States government published new encryption export regulations that made it easier for companies and individuals in the United States to widely export strong encryption.[308] Cryptographers have argued that that the requirement to obtain an export license before publishing encryption source code[309] on the Internet constitutes censorship of protected First Amendment speech. By designating source code as expressive speech, a ban on encrypted computer code would be subject to the same exacting scrutiny that applies to all content-based restrictions on speech.[310]

Law enforcement agencies have asserted that the use of encryption has presented a significant problem to legitimate law enforcement efforts.[311] As with any kind of stored and transmitted data, law enforcement may obtain both encrypted text and decryption keys pursuant to lawful process, which may include a wiretap order, a search warrant, a subpoena or the consent of the party possessing the required item.[312] No specific provision is made for decryption assistance, *per se*. Law enforcement officers need to exhaust existing search and seizure and production mechanisms to gain access to encrypted data and/or decryption keys.

In the United States, the government has introduced the key escrow[313] device under which the government can unlock encrypted communications. To this effect, it has devised the "clipper chip" for telephones and the "capstone chip" for email and file encryption. Use of these chips, however, remains voluntary and those wanting to encrypt can do so only if the software or

---

305 See paragraph 2.3.1.3.2 above for an explanation of the privacy measure of cryptography.

306 Sutter "A Tale of Two Interception Regimes: RIP v CALEA, a comparison" found on the Internet http://www.bileta.ac.uk/01papers/sutter.html 10. The so-called "E-Privacy (Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace) Act" of 1996 was introduced in the United States but never adopted. It sets out to, *inter alia*, establish privacy standards and procedures for law enforcement officers to follow to obtain decryption assistance for encrypted communications and information. For an analysis of the E-Privacy Act see Center for Democracy & Technology "Section-By-Section Analysis of the E-Privacy Act" found on the Internet http://www.cdt.org/crypto/legis_105/eprivacy/eprivsec.shtml 1-9.

307 For an interesting perspective on national security export controls on data encryption, see Hartzler 1994 *Texas International Law Journal* 437-456.

308 See Piper, Wilson and Mitchell "IS Auditing Procedure: Evaluation of Management Controls Over Encryption Methodolies (sic) Document P9" found on the Internet http://www.isaca.org/Template/cfm??Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18824 7.

309 Source code expresses a cryptographic algorithm, which is a precise set of programming operating instructions that enables a computer to transform data into an unintelligible form (see Aldesco 2002 *Loyola of Los Angeles Entertainment Law Review* 105.

310 Aldesco 2002 *Loyola of Los Angeles Entertainment Law Review* 104-105.

311 See also Bertron 1996 *American Criminal Law Review* 192.

312 See US Department of Justice "Department of Justice FAQ on Encryption Policy" found on the Internet http://www.usdoj.gov/criminal/cybercrime/cryptfaq.htm 8. The Department of Justice contends that it is difficult to see how use of recovery systems under the present voluntary regime might violate the Fourth Amendment. Wolfe argues that while the First, Fourth and Fifth Amendments merely restrict the powers given to the government in other sections of the Constitution, it is also true that the Bill of Rights does not ensure absolute privacy, but merely reasonable privacy. Within this context, he submits that legislation banning encryption that does not allow key recovery is reasonable, and thus constitutional. According to him, an appropriate key recovery system, such as one requiring private party trustee, has more safeguards against government abuse that the current requirements to procure, for example, a telephone wiretap. See Wolfe 2000 *Emory Law Journal* 726-744.

313 "Key escrow" is a mechanism by which a master key to each encryption device is held in a central repository for release to law enforcement agencies when necessary. See Esen 2002 *Journal of Criminal Law* 269.

hardware products are not exported out of the United States. Encryption key recovery has its own disadvantages. The most prominent one being that the centralisation of keys or the storage of master keys may make it much easier for criminals to have unauthorised access to such keys.[314]

5.3.2 Categories of service providers

The question that needs to be asked in classifying the service provider involved is whether the provider provides an electronic communication service, a remote computing service or neither. The Electronic Communications Privacy Act protects communications held by providers of electronic communication services when those communications are in electronic storage, as well as communications held by providers of a remote computing service. Whether an entity is a provider of an electronic communication service, a provider of a remote computing service, or neither, depends on the nature of the particular communication that is sought. A single provider can simultaneously provide an electronic communication service with respect to one communication and a remote computing service in respect of another communication. Law enforcement officers need to focus on drafting the appropriate order based on the information that they seek. Requesting a service provider to disclose files in electronic storage translates into the disclosure of all unopened emails in an account. A request for the disclosure of all files in an account, except for those in electronic storage, generally provides access to all opened emails and stored files.[315]

The statutory definitions of an electronic communication service, electronic storage and a remote computing service are explained below.

5.3.2.1 Electronic communication service

An electronic communication service is any service which provides its users with the ability to send or receive wire or electronic communications.[316] Telephone companies and electronic mail companies generally act as providers of electronic communication services.[317]

The key issue in determining whether a company provides an electronic communication service is the role of the company in providing the ability to send or receive the precise communication at issue, regardless of the company's primary business. Any company or government entity

---

314 Esen 2002 *Journal of Criminal Law* 269.

315 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 60.

316 Section 2510(15) of 18 USC. The right to privacy of the innocent users of electronic communication services are to be protected (see Adair and David 2001 *Federal Probation* 68). See also generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 58.

317 In *Federal Trade Commission v Netscape Communications Corp* 196 FRD 559, 560 (ND Cal 2000) the Court noted that Netscape, a provider of email accounts through netscape.net, is a provider of an electronic communication service.

that provides others with a means of communicating electronically can be a provider of an electronic communication service relating to the communications it provides, even if providing a communication service is merely incidental to the primary function of such a service provider.[318] Conversely, a service provider cannot provide an electronic communication service in respect of a communication if the service provider does not provide the ability to send or receive that communication.[319] It is important to note that a mere user of an electronic communication service provided by another is not an electronic communication service. A web site is accordingly not a provider of an electronic communication service, even though it may send and receive electronic communications from customers.[320]

5.3.2.2 Electronic storage

Electronic storage is defined as any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof or, alternatively, as any storage of such a communication by an electronic communication service for the purposes of the backup protection of such communication.[321]

The mismatch between the everyday meaning of electronic storage and its narrow statutory definition has been a source of considerable confusion. It is important to remember that electronic storage refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.[322] To determine whether a communication is in electronic storage, it is helpful to identify the communication's final destination. A copy of a communication is in electronic storage only if it is a copy of a communication created at an intermediate point and if it is designed to be sent on to its final destination. An email that has been received by a recipient's service provider but has not yet been accessed by the recipient is accordingly in electronic storage.[323] At that stage, the copy of the stored communication exists only as a temporary and intermediate measure, pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the

---

318 In *Bohach v City of Reno* 932 F Supp 1232, 1236 (D Nev 1996), it was held that a city that provided a pager service to its law enforcement officers can be a provider of an electronic communication service. In *United States v Mullins* 992 F2d 1472, 1478 (9th Cir 1993), the Court ruled that an airline that provides travel agents with a computerised travel reservation system accessed through separate computer terminals can be a provider of an electronic communication service.

319 In *Sega Enterprises Ltd; Sega of America Inc. v MAPHIA* 948 F Supp 923, 930-31 (ND Cal 1996), it was held that a video game manufacturer that accessed private email stored on another company's bulletin board service in order to expose copyright infringement was not a provider of electronic communication service. In *State Wide Photocopy v Tokai Financial Services Inc* 909 F Supp 137, 145 (SDNY 1995), the Court ruled that a financing company that used fax machines and computers, but did not provide the ability to send or receive communications, was not a provider of an electronic communication service.

320 In *Crowley v Cybersource Corporation and amazon.Com Inc* 166 F Supp 2d 1263, 1270 (ND Cal 2001), the plaintiff argued that Amazon.com, to whom the plaintiff sent his name, credit card number, and other identification information, was an electronic communications service provider, because without recipients such as Amazon.com, users would have no ability to send electronic information. The Court rejected this argument, holding that Amazon was properly characterised as a user rather than a provider of an electronic communication service.

321 Section 2510(17) of 18 USC. See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 58.

322 For example, the Court in *In re Doubleclick Inc Privacy Litigation* 154 F Supp 2d 497, 511-12 (SDNY 2001), held that "cookies" (information stored on a user's computer by a web site and sent back to the web site when the user accesses the web site) fall outside of the definition of electronic storage and hence outside of the Electronic Communications Privacy Act because of their long-term residence on hard drives.

323 See *Steve Jackson Games Inc v United States Secret Service* 36 F3d 457, 461 (5th Cir 1994).

communication reaches its final destination. If a recipient then chooses to retain a copy of the accessed communication on the service provider's system, the copy stored on the network is no longer in electronic storage, because the retained copy is no longer in temporary, intermediate storage incidental to electronic transmission.[324] Instead, because the process of transmission to the intended recipient has been completed, the copy is simply a remotely stored file.[325]

Whether a communication is held in electronic storage by a service provider governs whether that service provides an electronic communication service in respect of the communication. The two concepts are coextensive: a service provides an electronic communication service with regard to a communication only if the service holds the communication in electronic storage. It follows that if a communication is not in temporary, intermediate storage incidental to its electronic transmission, the service provider cannot provide an electronic communication service for that communication. Instead, the service must provide either a remote computing service or else neither an electronic communication storage nor a remote computing service.

5.3.2.3 Remote computing service

The term "remote computing service" is defined as the provision to the public of computer storage or processing services by means of an electronic communications system.[326] An electronic communications system is any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications.[327]

A remote computing service is generally provided by an off site computer that stores or processes data for a customer. Examples of remote computing services include a service provider that processes data in a time-sharing arrangement or a mainframe computer that stores data for future retrieval.[328] A provider of a remote computing service does not hold customer files on their way to a third intended destination but, instead, stores or processes files for the convenience of the account holder. Such files held by a service provider acting as a remote computing service cannot be in electronic storage.[329]

---

324 Section 2501(17) of 18 USC. See Adair and David 2001 *Federal Reporter* 68.

325 In *Fraser v Nationwide Mutual Insurance Co.* 135 F Supp 2d 623, 635-38 (ED Pa 2001), it was held that because an email was acquired from post-transmission storage, it was not in electronic storage and its acquisition was not prohibited under the Electronic Communications Privacy Act. Opened email and voicemail left on a service provider's system are intended to be covered by provisions relating to remote computing services, rather than provisions relating to services holding communications in electronic storage.

326 Section 2711(2) of 18 USC. See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 59.

327 Section 2510(14) of 18 USC.

328 In *Steve Jackson Games Inc v United States Secret Service* 816 F Supp 432, 443 (WD Tex 1993) the Court held that the provider of bulletin board services was a remote computing service.

329 Section 2510(17) of 18 USC.

A service can only be a remote computing service if it is available to the public.[330] Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees.[331] Service providers whose services are open only to those with a special relationship with the provider, such as an employee-employer relationship, are not available to the public.[332]

5.3.3 Information categories

The question to be asked when classifying the information sought is whether the information is content in electronic storage, content held by a remote computing service, a record pertaining to a subscriber or other information enumerated by the Electronic Communications Privacy Act. Network service providers can store different kinds of information relating to an individual customer or subscriber, including opened and unopened emails, account logs that reveal when a user logged on to and off from the Internet service provider, credit card information for billing purposes and the user's name and address. When law enforcement agencies wish to obtain such records, they must be able to classify these types of information using the language of the Electronic Communications Privacy Act, in terms of which information is classified into the three categories discussed below.[333]

5.3.3.1 Basic subscriber information

Basic subscriber information includes the name, address, local and long distance telephone connection records or records of session times and durations, length of service (inclusive of its starting date), the types of service utilised, the telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address and the means and source of payment for such a service, such as a credit card or bank account number.[334] The items generally listed as subscriber information relate to the identity of a subscriber, the person's relationship with the service provider and the person's basic session connection records. It does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded during a prior session.[335]

---

330 Section 2711(2) of 18 USC.

331 It may seem odd that a service can charge a fee but still be considered available to the public. However, this mirrors commercial relationships in the physical world. For example, movie theatres are open to the public because anyone can buy a ticket and see a show, even though tickets are not free.

332 In *Andersen Consulting LLP v UOP and Bickel & Brewer* 991 F Supp 1041, 1043 (ND Ill 1998), the Court interpreted the "providing to the public" clause in section 2702(a) of 18 USC to exclude an internal email system that was made available to a hired contractor but was not available to any member of the community at large.

333 See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 61.

334 Section 2703(c)(2) of 18 USC.

335 USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 61.

The USA PATRIOT Act[336] enhanced the categories of basic subscriber information in three respects, adding the following information to section 2703(c)(2) of 18 USC:

(a) records of session times and durations, as well as any temporarily assigned network address, such as the Internet protocol address assigned by an Internet service provider to a customer for a particular session;

(b) other information relating to account access, such as the originating telephone number for dial-up Internet access or the Internet protocol address of a user accessing an account over the Internet; and

(c) the means and source of payment that a customer uses to pay for an account, including any credit card or bank account number.[337]

5.3.3.2 Records or other information pertaining to a customer or subscriber to such a service

This is a catch-all category. It includes all records that are not contents, including basic subscriber information.[338] Common examples of records pertaining to a subscriber include transactional records such as account logs that record account usage, cell site data for cellular telephone calls, and email addresses of other individuals with whom the account holder has corresponded.[339]

5.3.3.3 Contents

The contents of a network account are the actual files stored in the account.[340] The term "contents", when used in respect of any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. Examples of contents include stored emails or voicemails, word processing files stored in employee network accounts and the subject headers of emails.[341] Contents can be further divided into three subcategories:

---

336 Section 210 of the USA PATRIOT Act.

337 While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information. See USA CCIPS "Field Guidance on New Authorities That Related to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001" found on the Internet http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm 1 and USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 61.

338 Section 27039(c)(1) of 18 USC

339 In *United States v Allen* 53 MJ 402, 409 (CAAF 2000), the Court concluded that a log identifying the date, time, user, and detailed Internet address of sites accessed by a user constituted a record or other information pertaining to a subscriber or customer of such a service under the Electronic Communications Privacy Act. In *Hill v MCI Worldcom Communications Inc.* 120 F Supp 2d 1194, 1195-96 (SD Iowa 2000), it was ruled that names, addresses, and phone numbers of parties called constituted a record or other information pertaining to a subscriber or customer of such service for a telephone account. The purpose of separating the basic subscriber information from other non-content records was to distinguish basic subscriber information from more revealing transactional information that could contain a person's entire online profile.

340 Section 2510(8) of 18 USC.

341 In *Brown v Waddell* 50 F3d 285, 292 (4th Cir 1995), it was noted that numerical pager messages provide such an unlimited range of number-coded substantive messages in the course of holding that the interception of pager messages requires compliance with Title III (see footnote 9 in paragraph 5.1 above for a reference to the term "Title III").

(a) contents stored in electronic storage by the providers of an electronic communication service;

(b) contents stored by providers of remote computing services; and

(c) contents held by neither.

5.3.4 *Different production devices*[342]

The question to be asked when classifying the action involved in the production of information is whether law enforcement is seeking to compel disclosure or seeking to accept information that is disclosed voluntarily by the provider. If a law enforcement officer seeks compelled disclosure, the officer needs to determine whether she needs a search warrant, a section 2703(d)[343] court order or a subpoena to compel the disclosure. If a law enforcement officer wishes to accept information that is voluntarily disclosed, it must be determined whether the disclosure is permitted.

Section 2703 of 18 USC offers five mechanisms that law enforcement agencies can use to compel a provider to disclose, for example, the contents of stored wire or electronic communications, including email and voicemail and other information, such as account records and basic subscriber information. The five mechanisms, in ascending order of required threshold showing, are the following:

(a) a subpoena;[344]

(b) a subpoena with prior notice to the subscriber or customer;[345]

(c) a section 2703(d) court order;[346]

(d) a section 2703(d) court order with prior notice to the subscriber or customer;[347] and

(e) a search warrant.[348]

It must be borne in mind that greater process generally includes access to information that can be obtained with lesser process.[349] A higher-level process will always prevail, meaning that a court order will always be acceptable to obtain subscriber information and a warrant will always be acceptable to obtain transactional information or subscriber information.[350] As a result, the additional work required to satisfy a higher threshold is often justified, both because it can

---

342 See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 62-66.

343 Of 18 USC.

344 See paragraph 5.3.4.1.1 below.

345 See paragraph 5.3.4.1.2 below.

346 See paragraph 5.3.4.1.3 below.

347 See paragraph 5.3.4.1.4 below.

348 See paragraph 5.3.4.1.5 below.

349 Thus, a section 2703(d) Court order can compel everything that a subpoena can compel (plus additional information) and a search warrant can compel the production of everything that a section 2703(d) order can compel (and more).

350 Moore *Search and Seizure of Digital Evidence* 106.

authorise a broader disclosure and because pursuing a higher threshold provides extra insurance that the process complies fully with the Electronic Communications Privacy Act. The notice requirement must, however, be considered a separate burden, as a subpoena with notice to the subscriber can be used to compel information that is not available using a section 2703(d) order without subscriber notice.

One small category of information can be compelled under the Electronic Communications Privacy Act without a subpoena. When investigating telemarketing fraud, law enforcement officers may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing.[351]

It must also be noted that the Cable Communications Policy Act[352] restricts law enforcement access to cable operator records only when the records relate to ordinary cable services. It does not restrict government access to records relating to Internet access or a telephone service provided by a cable operator. The Cable Act has been amended to specify that its disclosure restrictions apply only to records revealing what ordinary cable television programming a customer purchases, such as particular premium channels or pay per view shows.[353] In particular, cable operators may disclose subscriber information to law enforcement pursuant to the Electronic Communications Privacy Act, Title III and the Pen Register/Trap and Trace Devices Statute, except for records revealing the cable subscriber's selection of video programming.[354] Records revealing the subscriber's selection of video programming remain subject to the restrictions of section 551(h) of 47 USC.

5.3.4.1 Compelled disclosure

5.3.4.1.1 Subpoena for basic subscriber information

The Electronic Communications Privacy Act permits law enforcement officers to compel the disclosure of two kinds of information using a subpoena. First, law enforcement agencies may

---

351 Section 2703(c)(1)(D) of 18 USC.

352 Specifically section 551 of 47 USC. Section 551 of 47 USC sets forth a restrictive system of rules governing law enforcement access to records held by a cable company. Under these rules, even a search warrant was insufficient to gain access to cable company records. In the past, law enforcement officers could obtain personally identifiable information concerning a cable subscriber only by overcoming a heavy burden of proof at an in-court adversary proceeding, as specified in section 551(h) of 47 USC.

353 Sections 211 and 115 of the USA PATRIOT Act. Section 211 of the USA PATRIOT Act amends section 551(c)(2)(D) of 47 USC to clarify that the Electronic Communications and Privacy Act, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communications services (such as telephone and Internet users). The amendment preserves, however, the Cable Communications Policy Act's primacy in respect of records revealing what ordinary cable television programming a customer chooses to purchase, such as particular premium channels or "pay per view" shows. In a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a law enforcement agency can use legal process under the Electronic Communications and Privacy Act to compel the provider to disclose customer records relating to Internet service. See USA CCIPS "Field Guidance on New Authorities That Related to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001" found on the Internet http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm 1.

354 Section 551(c)(2)(D) of 47 USC.

compel the disclosure of basic subscriber information.[355] Law enforcement officers can also use a subpoena to obtain information that is outside the scope of the Electronic Communications Privacy Act. Information relating or belonging to a person who is neither a customer nor a subscriber is not protected by the Electronic Communications Privacy Act and it may be obtained using a subpoena.[356]

The legal threshold for issuing a subpoena is low.[357] Evidence obtained in response to a federal grand jury subpoena must be protected from disclosure.[358] Subpoenas other than federal grand jury subpoenas may be used to obtain disclosure pursuant to section 2703(c)(2) of 18 USC. Any federal or state grand jury or trial subpoena suffices, as does an administrative subpoena authorised by a federal or state statute.[359]

5.3.4.1.2 Subpoena with prior notice to the subscriber or customer for opened email from a provider

A subpoena with prior notice to the subscriber or customer for opened email from a service provider must comply with the notice provisions of sections 2703(b)(1)(B) and 2705 of 18 USC. Law enforcement officers who obtain a subpoena and either give prior notice to the subscriber or comply with the delayed notice provisions of section 2705(a) may obtain everything that can be obtained using a subpoena without notice. This includes the contents of any wire or electronic communication held by a provider of a remote computing service on behalf of a subscriber or customer of such a remote computing service[360] and the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than 180 days.[361]

Law enforcement officers may accordingly use a subpoena to obtain opened email and other stored electronic or wire[362] communications in electronic storage more than 180 days, as long as they comply with the notice provisions of the Electronic Communications Privacy Act. The notice provisions can be satisfied by giving the customer or subscriber prior notice of the disclosure.[363] However, notice may be delayed for 90 days upon the execution of a written certification by a supervisory official that there is reason to believe that notification of the

---

355 Section 2703(c)(2) of 18 USC.

356 The scope of the word "customer", within the context of the Electronic Communications Privacy Act, was discussed in *Organisation JD LTDA v United States Department of Justice* 124 F3d 354, 359-61 (2nd Cir 1997).

357 *United States v Morton Salt Co* 338 US 632, 642-43 (1949).

358 Pursuant to section 6(e) of the Federal Rules of Criminal Procedure.

359 For example, subpoenas authorised by section 6(a)(4) of the Inspector General Act may be used. However, at least one Court has held that a pre-trial discovery subpoena issued in a civil case pursuant to section 45 of the Federal Rules of Civil Procedure is inadequate. In *Federal Trade Commission v Netscape Communications Corp* 196 FRD 559 (ND Cal 2000) the Court held that a pre-trial discovery subpoena did not fall within the meaning of "trial subpoena".

360 Section 2703(b)(2) of 18 USC.

361 Section 2703(a) of 18 USC.

362 The inclusion of wire communications (such as voice mail) in this category, was made effective by the USA PATRIOT Act (sections 209, 224 and 115).

363 Section 2703(b)(1)(B) of 18 USC.

existence of the subpoena may have an adverse result.[364] Both "supervisory official"[365] and "adverse result"[366] are specifically defined terms for the purposes of delaying notice. This provision of the Electronic Communications Privacy Act provides a permissible way for law enforcement officers to delay notice when notice would jeopardise a pending investigation or endanger the life or physical safety of an individual.

Upon the expiration of the delayed notice period,[367] the statute requires the law enforcement agency to send a copy of the request or process, along with a letter explaining the delayed notice, to the customer or subscriber.[368]

The Electronic Communications Privacy Act's provision allowing opened email to be obtained using a subpoena combined with prior notice to the subscriber appears to derive from Supreme Court case law interpreting the Fourth and the Fifth Amendments.[369] In allowing the government to subpoena opened email, it seems that by "renting" computer storage space with a remote computing service, a customer places herself in the same situation as a person who gives business records to an accountant or attorney.

5.3.4.1.3 Section 2703(d) order

This section can be aimed at most account logs and transactional records. Law enforcement officers who obtain a court order under section 2703(d) of 18 USC may obtain anything that can be obtained using a subpoena without notice and all records or other information pertaining to a subscriber to or customer of such a service, not including the contents of the communications held by the providers of an electronic communications service and a remote computing service.[370]

A court order authorised by section 2703(d) of 18 USC may be issued by any federal magistrate, district court or equivalent state court judge.[371] To obtain such an order, known as an "articulable facts court order" or simply a "d" order, the government entity must offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. This standard does not permit law enforcement

---

364 Sections 2705(a)(1)(B) and 2705(a)(4) of 18 USC.
365 Section 2705(a)(6) of 18 USC.
366 Section 2705(a)(2) of 18 USC.
367 Section 2705(a)(4) of 18 USC. The government may extend the delay of notice for additional 90-day periods on application to a court.
368 Section 2705(a)(5) of 18 USC.
369 In *United States v Couch* 409 US 322 (1973), Fourth and Fifth Amendment challenges to a subpoena served on a defendant's accountant for the accountant's business records stored with the accountant were rejected. When an individual gives paper documents to a third party, such as an accountant, the government may subpoena the paper documents from the third party without running foul of either the Fourth or the Fifth Amendment.
370 Section 2703(c)(1) of 18 USC.
371 Sections 2703(d), 2711(3) of 18 USC.

agencies merely to certify that it has specific and articulable facts that would satisfy such a showing. Instead, the law enforcement officer must actually offer those facts to the court in the application for the order.[372] The court must find, based on the law enforcement agency's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation. In practice, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. The obtaining of a section 2703(d) court order requires a lower standard than probable cause.[373]

Section 2703(d) orders issued by federal courts have effect outside the district of the issuing court. The Electronic Communications Privacy Act permits a judge to enter section 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored.[374] Section 2703(d) orders may also be issued by state courts.[375] However, the statute does not confer extra-territorial effect on section 2703(d) orders issued by state courts.[376]

5.3.4.1.4 Section 2703(d) order with prior notice to the subscriber or customer

This type of order can be aimed at the full contents of a subscriber's account, except unopened email or voicemail[377] stored with a service provider for 180 days or less.

Law enforcement officers who obtain a court order under section 2703(d) of 18 USC and either give prior notice to the subscriber or else comply with the delayed notice provisions of section 2705(a), may obtain

(a) everything that can be obtained using a section 2703(d) court order without notice;
(b) the contents of any wire or electronic communication held by a provider of a remote computing service on behalf of a subscriber or customer of such a remote computing service;[378] and

---

372 In *United States v Kennedy* 81 F Supp 2d 1103, 1109-11 (D Kan 2000), the Court concluded that a conclusory application for a section 2703(d) order did not meet the requirements of the statute.

373 Moore *Search and Seizure of Digital Evidence* 105.

374 Section 2703(d) of 18 USC states that any court that is a court of competent jurisdiction may issue a section 2703(d) order; section 2711(3) of 18 USC states that a court of competent jurisdiction has the meaning assigned by section 3127 and includes any federal court within that definition, without geographical limitation; section 3127(2) of 18 USC defines a court of competent jurisdiction. The definition of "court of competent jurisdiction" was introduced by sections 220, 224 and 115 of the USA PATRIOT Act.

375 Sections 2711(3) and 3127(2)(B) of 18 USC defines a court of competent jurisdiction to include a court of general criminal jurisdiction of a state authorised by the law of the state to enter orders authorising the use of a pen register or trap and trace device.

376 Section 2711(3) of 18 USC.

377 The inclusion of wire communications (such as voicemail) in this category was introduced by sections 209, 224 and 115 of the USA PATRIOT Act.

378 Sections 2703(b)(1)(B)(ii) and 2703(b)(2) of 18 USC.

(c) the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than 180 days.[379]

As an alternative to giving prior notice, law enforcement officers can obtain an order delaying notice for up to 90 days when notice would seriously jeopardise the investigation.[380] In such cases, law enforcement officers generally obtain this order by including an appropriate request in the officers' 2703(d) application and proposed order. Law enforcement agencies may also apply to the court for extensions of the delay.[381] The applicant must satisfy the court that there is reason to believe that notification of the existence of the court order may

(a) endanger the life or physical safety of an individual;
(b) lead to flight from prosecution;
(c) lead to destruction of or tampering with evidence;
(d) lead to intimidation of potential witnesses;
(e) otherwise seriously jeopardise an investigation; or
(f) unduly delay a trial.[382]

It is important that the applicant satisfy this standard anew every time the applicant seeks an extension of the delayed notice.

5.3.4.1.5 Search warrant for the full contents of an account

Law enforcement officers who obtain a search warrant under Rule 41 of the Federal Rules of Criminal Procedure[383] or an equivalent state warrant may obtain

(a) everything that can be obtained using a section 2703(d) court order with notice; and
(b) the contents of a wire or electronic communication that is in electronic storage in an electronic communications system for 180 days or less.[384]

The Electronic Communications Privacy Act does not require that law enforcement officers notify the customer or subscriber when it obtains information from a provider using a search warrant.[385] Moreover, because the warrant is issued by a neutral magistrate based on probable cause, obtaining a search warrant effectively insulates the process from challenge under the Fourth Amendment.

---

379 Section 2703(a) of 18 USC.
380 Section 2705(a) of 18 USC.
381 Sections 2705(a)(1)(A) and 2705(a)(4) of 18 USC. The legal standards for obtaining a court order delaying notice mirror the standards for a certified delayed notice by a supervisory official.
382 Sections 2705(a)(1)(A) and section 2705(a)(2) of 18 USC.
383 See paragraph 5.2.3 above for an overview of searches and seizures under a warrant.
384 Section 2703(a) of 18 USC.
385 Section 2703(b) (1)(A) of 18 USC.

Although most search warrants obtained under Rule 41 of the Federal Rules of Criminal Procedure are limited to a search of property within the district of the authorising magistrate judge, search warrants under section 2703(a) of 18 USC may be issued by a federal court with jurisdiction over the offence under investigation, even for records held in another district.[386] State courts may also issue warrants under section 2703(a), but the statute does not give these warrants effect outside the limits of these courts' territorial jurisdiction. Otherwise, in practice, section 2703(a) search warrants are obtained just like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41.[387] Once a magistrate signs the warrant, however, law enforcement officers ordinarily do not themselves search through the service provider's computers in search of the materials described in the warrant. Instead, law enforcement officers serve the warrant on the provider as they would serve a subpoena, and the provider produces the material described in the warrant. Law enforcement officers preparing a warrant pursuant to section 2703 are advised to request in the search warrant application that the magistrate expressly permit them to fax the warrant to the Internet Service Provider and to execute the warrant without the officer present.[388]

---

386 Section 2703(a) of 18 USC. The emergency disclosure provisions of section 2702(b)(6)(C) and section 2702(c) were added by sections 212, 224 and 115 of the USA PATRIOT Act. The USA PATRIOT Act also simplified the treatment of voluntary disclosures of non-content records by providers by moving all such provisions from section 2703(c) to section 2702 and clarifying that service providers have the authority to disclose non-content records to protect their rights and property. See USA CCIPS "Field Guidance on New Authorities That Related to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001" found on the Internet http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm 4.

387 Section 2703(a) of 18 USC.

388 This guideline is due to the decision in *United States v Bach* 2001 WL 1690055 (D Minn Dec 14 2001). The practice of having service providers produce the materials specified in a search warrant was held to be unconstitutional. The court held that the Fourth Amendment mandates the protections codified in section 3105 of 18 USC, which requires that a law enforcement officer be present and act in the execution of a search warrant. According to the Court, section 2703 is not an exception to and does not provide an alternative mode of execution from section 3105, so federal law enforcement officers are mandated by statute to comply with section 3105 when they execute a search warrant under section 2703(a). The Court held that even in the absence of a statutory mandate, the Fourth Amendment requires a law enforcement officer to be present and to act in the execution of any search warrant, including a warrant issued under section 2703(a). See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 66. The decision in *United States v Bach* 2001 WL 1690055 (D Minn Dec 14 2001) was appealed by the government, *inter alia,* on the grounds that section 2703 search warrants are not traditional search warrants, but are to be used to obtain subscriber content as a form of compulsory process directed to third-party network providers. Sections 2702(b)(2) and (c)(1) of 18 USC explicitly state that a provider may disclose customer records in response to a section 2703 process. Furthermore, even if section 3105 of 18 USC were applicable to warrants served pursuant to the Electronic Communications Privacy Act, section 3105 does not require the presence of a law enforcement officer when service providers collect and produce information pursuant to a search warrant, because the problems associated with private exercise of search and seizure powers are not implicated when service providers collect and produce information in response to a warrant. Moreover, practically speaking, requiring the presence of a law enforcement officer at the execution of these search warrants would prove extremely burdensome, as searches can prove to be time-consuming, and Internet service providers maintain account information in a variety of locations. It is also difficult to imagine how a law enforcement officer could play a useful role in a service provider's actual retrieval of the specified records. This issue was not addressed by the Appeal Court and the recommendation accordingly still needs to be followed (see *United States of America v Bach* 400 F3d 622 (8th Cir 2005)).

5.3.4.2 Voluntary disclosure[389]

Providers of services not available to the public may freely disclose both contents and other records relating to stored communications, but the Electronic Communications Privacy Act imposes restrictions on voluntary disclosure by providers of services to the public. The voluntary disclosure provisions govern when a provider of a remote computing service or an electronic communication service is allowed to disclose contents and other information voluntarily, either to the government or to non-government entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, law enforcement must rely on the appropriate legal orders to compel disclosure.

When considering whether a provider of a remote computing service or an electronic communication service is permitted to disclose contents or records, it must be ascertained whether the relevant service offered by the provider is available to the public. If not, the Electronic Communications Privacy Act does not place any restrictions on disclosure.[390] However, if the services offered by the provider are available to the public, the Electronic Communications Privacy Act forbids both the disclosure of contents to any third party and the disclosure of other records to any governmental entity. Even a public provider may disclose customers' non-content records freely to any person other than a government entity.[391]

Certain statutory exceptions[392] apply that generally permit disclosure by a provider to the public when the needs of public safety and service providers outweigh the privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests. The voluntary disclosure of contents is therefore allowed when

---

389 Section 2702 of 18 USC. Section 212 of the USA PATRIOT Act changed the Electronic Communications Privacy Act so that section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 only covers compulsory disclosures. See USA CCIPS "Field Guidance on New Authorities That Related to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001" found on the Internet http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm 2. See also generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 67-68. Service providers were previously forbidden from allowing this voluntary access. See P&DPTeam 2002 *Privacy and Data Protection* 12.

390 Section 2702(a) of 18 USC. In *Andersen Consulting v UOP and Bickel & Brewer* 991, 1043 F Supp 1041 (ND Ill 1998), the petroleum company UOP hired the consulting firm Andersen Consulting and gave Andersen employees accounts on UOP's computer network. After the relationship between UOP and Andersen soured, UOP disclosed emails that Andersen employees had left on the UOP network to the *Wall Street Journal*. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated the Electronic Communications Privacy Act. The Court rejected the suit on the grounds that UOP did not provide an electronic communication service to the public. It was held that giving Andersen access to UOP's email system is not equivalent to providing email to the public. Andersen was hired by UOP to do a project and, as such, was given access to UOP's email system, like UOP employees. Andersen was not just any member of the community at large, but a hired contractor. Because UOP did not provide services to the public, the Electronic Communications Privacy Act did not prohibit disclosure of contents belonging to UOP's subscribers.

391 Sections 2702(a)(3) and (c)(5) of 18 USC.

392 Section 2702(b) contains exceptions for the disclosure of contents, and section 2702(c) contains exceptions for disclosure of other customer records.

(a) the disclosure may be necessarily incident to the rendering of the service or to the protection of the rights or property of the provider of that service;[393]

(b) the disclosure is made to a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime;[394]

(c) the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay;[395]

(d) the Child Protection and Sexual Predator Punishment Act[396] mandates the disclosure; or

(e) the disclosure is made to the intended recipient of the communication, with the consent of the intended recipient or sender, to a forwarding address, or pursuant to a court order or legal process.[397]

The voluntary disclosure of non-content customer records by a provider to a governmental entity is permitted when

(a) the disclosure may be necessarily incident to the rendering of the service or to the protection of the rights or property of the provider of that service;[398]

(b) the provider reasonably believes that an emergency involving immediate danger of death of serious physical injury to any person justifies disclosure;[399] or

(c) the disclosure is made with the consent of the intended recipient, or pursuant to a court order or legal process.[400]

5.4 Domestic preservation devices

5.4.1 Background

In view of the fact that all network service providers work differently,[401] law enforcement officers need to communicate with these service providers before issuing subpoenas or obtaining court orders that compel the disclosure of information. The Electronic Communications Privacy Act contains two provisions designed to aid law enforcement officials working with network service

393 Section 2702(b)(5) of 18 USC.
394 Section 2702(b)(6)(A) of 18 USC.
395 Section 2702(b)(6)(C) of 18 USC.
396 Section 13032 of 42 USC (the Child Protection and Sexual Predator Punishment Act of 1998) mandates the disclosure in terms of section 2702(b)(6)(B) of 18 USC.
397 Section 2702(b)(1)-(4) of 18 USC.
398 Section 2702(c)(3) of 18 USC.
399 Section 2702(c)(4) of 18 USC.
400 Section 2702(c) (1)-(2) of 18 USC.
401 Some network service providers, for example, retain very complete records for a long time; whereas others network service providers retain few records, or even none. Some providers can comply easily with law enforcement requests for information; others struggle to comply with even simple requests.

providers. These provisions are aimed at helping to ensure that providers do not delete the records needed or notify others about the investigation.[402]

5.4.1.1 Section 2703(f) preservation orders

No law regulates how long network service providers in the United States must retain account records. Some service providers retain records for months, others for hours, and others not at all. Evidence may accordingly be destroyed or lost before law enforcement agencies can obtain the appropriate legal order(s) to compel its disclosure. To minimise this risk, the Electronic Communications Privacy Act permits the government to direct providers to freeze stored records and communications pursuant to section 2703(f) of 18 USC. A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, is obliged to take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

There is no legally prescribed format for section 2703(f) requests. While a simple phone call to the service provider should therefore be adequate, a fax or an email is better practice, because it both provides a paper record and reduces the risk of miscommunication. Upon receipt of the law enforcement request, the provider must retain the records for 90 days, renewable for another 90-day period upon another law enforcement request.[403] A preservation request under section 2703(f) only applies to information in possession of the provider at the time of the request.[404]

Law enforcement officers who send section 2703(f) letters to network service providers should be aware of the following two limitations:

(a) The authority to direct providers to preserve records and other evidence is not prospective. A section 2703(f) letters can order a provider to preserve records that have already been created, but cannot order providers to preserve records not yet made.

(b) Some network service providers may be technically unable to comply effectively with section 2703(f) requests. Law enforcement officers should communicate with the network provider before ordering the provider to take steps that may have unintended adverse effects.

---

402 See generally USA CCIPS "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm 69-71.

403 Section 2703(f)(2) of 18 USC.

404 Kreston 2004 *Rutgers Computer and Technology Law Journal* 370.

5.4.1.2 Section 2705(b) order not to disclose the existence of a warrant, subpoena or court order

Law enforcement officers acting under section 2703, when not required to notify the subscriber or customer under section 2703(b)(1) or to the extent that such notice may be delayed pursuant to section 2703(a), may apply to a court for an order in terms of section 2705(b) of 18 USC. Under this section a provider of an electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, is not to notify any other person of the existence of the warrant, subpoena or court order.

The court can enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order can

(a) endanger the life or physical safety of an individual; or
(b) lead to flight from prosecution;
(c) lead to the destruction of or tampering with evidence,
(d) lead to the intimidation of potential witnesses; or
(e) otherwise seriously jeopardise an investigation or unduly delay a trial.

5.5 Brouter[405] to chapter 6

The main objective of this study is to consider whether the South African search and seizure, production and preservation mechanisms, when directed at electronic evidence, need to be augmented and/or aligned in accordance with those set out in the Cybercrime Convention. In serving this objective, this chapter was aimed at providing an overview of the different domestic search and seizure, production and preservation procedural mechanisms available in the United States legislative framework. This exposition also sought to illustrate the application of the equivalent United States domestic search and seizure, production and preservation mechanisms, when directed at electronic evidence. Precedents regarding the application of these equivalent mechanisms in the United States are considered instructive for the South African context.

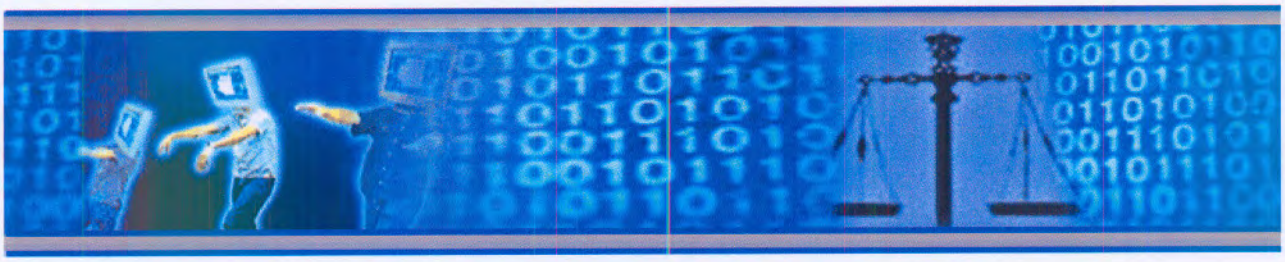
The rationale behind this chapter was essentially to enable a contextually comparative troubleshooting utility in respect of the application of these procedural mechanisms to electronic evidence in South Africa. It is therefore not considered an objective in itself to juxtapose the

[405] See chapter 7 for a list of the findings extracted from the contents of chapter 5.

devices proposed in the Cybercrime Convention to those available within the current United States catalogue of search and seizure, production and preservation mechanisms.

In the next chapter, the search and seizure, production and preservation mechanisms available in English law are investigated. Precedents regarding the application of these equivalent mechanisms in English law to electronic evidence are considered equally instructive for the South African context.

CHAPTER 6:
A SNAPSHOT OF TROUBLESHOOTING @ ENGLAND



6.1 BIOS BITS AND BYTES 310

6.2 DOMESTIC SEARCH AND SEIZURE OF E-EVIDENCE 313

6.2.1 Root domain 313
6.2.2 Right to privacy 316
6.2.3 Search and seizure of e-evidence with a warrant 319
6.2.3.1 Search warrant types 320
6.2.3.2 Particularity and specificity 326
6.2.3.3 Judicial supervision 329
6.2.3.4 Reasonable grounds 331
6.2.3.5 In search of an *e*-evidence strategy 333
6.2.4 Search and seizure of e-evidence without a warrant 340
6.2.4.1 Warrantless search and seizure doctrines 341

6.3 PRODUCTION DEVICES 355

6.3.1 Background 355
6.3.2 Information categories 357
6.3.2.1 Legally privileged material 357
6.3.2.2 Excluded material 359
6.3.2.3 Special procedure material 360
6.3.2.4 Communications data 360
6.3.2.5 Traffic data 361
6.3.2.6 Protected data 362
6.3.3 Different production devices 362
6.3.3.1 Production order in terms of Schedule 1 to PACE 362
6.3.3.2 Authorisations and notices for communications data in terms of RIPA 365
6.3.3.3 Notices for protected data in terms of RIPA 367

6.4 PRESERVATION AND PARTIAL DISCLOSURE DEVICES 374

6.5 BROUTER TO CHAPTER 7 378

6.1 BIOS bits and bytes[1]

A snapshot of the domestic[2] search and seizure, production and preservation mechanisms available in the legal framework of England,[3] similar to the one provided in the previous chapter of this thesis in respect of the United States, is provided in this chapter. The rationale behind this snapshot is to enable a comparative troubleshooting utility between the South African search and seizure, production and preservation mechanisms and those available in the legislative framework in England. This is done by, firstly, identifying these equivalent devices (if any exist), secondly, by gaining a broad understanding of the legislative frameworks from which they emanate and, lastly, by examining the ways in which they are applied to electronic evidence. In respect of the main objective of this thesis, the purpose behind the enablement of such a troubleshooting utility is to contribute towards an investigation into whether any alignments and/or augmentations are required in respect of the South African domestic search and seizure, production and preservation mechanisms.[4]

The law governing the preservation, production and search and seizure of electronic evidence in England has four primary sources. Firstly, sections 1 to 7 of Part I of the Police and Criminal Evidence Act (PACE)[5] provide law enforcement officers with powers to stop and search. Sections 8 to 23, encapsulated in Part II of PACE, impart general powers of entry, search and seizure. Section 50 of the Criminal Justice and Police Act[6] empowers law enforcement officers with an innovative search and sift power that caters for the off-site sorting of large quantities of seized material.

Secondly, sections 21 to 25 of the Regulation of Investigatory Powers Act (RIPA)[7] are aimed at

---

1 In this heading, BIOS means some introductory bits and pieces with which to contextualise the primary sources of preservation, production and search and seizure mechanisms in the law of England. It also broadly contextualises the relevance of this chapter within the overarching framework of this thesis. See footnote 1 of paragraph 3.1 above for a technical definition of the term "BIOS".

2 Although both the domestic and transborder procedural mechanisms available in the South African legal framework and those proposed in the Cybercrime Convention were investigated in chapters 3 and 4 respectively, only the domestic procedural mechanisms available in the United States and England are considered in chapters 5 and 6 respectively. An attempt to also incorporate the transborder mechanisms, from a comparative perspective, would have rendered the scope of this thesis too extensive. See footnote 109 in paragraph 1.2 above.

3 The rationale for choosing the legal systems of the United States and England for comparative purposes is set out in paragraph 1.3 above. The comparative reach of this chapter is limited to the position in English law and it is not concerned with the broader legislative framework of the United Kingdom as a whole (the positions in Scotland, Wales and Northern Ireland technically do not resort within the scope of this study). In this respect also see footnote 113 in paragraph 1.3 above.

4 Some of the most important findings that can be extracted from the snapshots provided of the different catalogues of search and seizure, production and preservation mechanisms available in the legislative frameworks of the United States and England are referred to in chapter 7.

5 Of 1984. Hereinafter referred to as PACE.

6 Of 2001. Hereinafter referred to as the Criminal Justice and Police Act.

7 Of 2000. Hereinafter referred to as either the Regulation of Investigatory Powers Act or RIPA. RIPA updated the Interception of Communications Act of 1985 in the light of the huge advances made in communications technology in recent years. RIPA was not only intended to implement article 5 of the Telecoms Privacy Directive 97/66, but has in addition been used by the Government to deal with those aspects of encryption which proved too controversial for inclusion in the Electronic Communications Act of 2000. See Chissick and Kelman *Electronic Commerce Law and Practice* 311. The Regulation of Investigatory Powers Act (RIPA) contains five parts, namely the interception of communications and the acquisition and disclosure of communications data; surveillance and covert human intelligence sources (including the powers to do intrusive surveillance on residential premises and in private vehicles, covert surveillance in the course of specific operations and the

the acquisition and disclosure of communications data, including traffic data.[8] Sections 49 to 56 of this Act also introduce a power to require the disclosure of protected data in an effort to maintain the effectiveness of existing law enforcement powers in the face of the increasing criminal use of encryption.

Thirdly, it is important to bear in mind that the retention of data is closely associated with the provision and accessing thereof and retained data is preserved by default. The retention of communications data in England is currently addressed by the voluntary code of practice on the retention of communications data issued by the Home Secretary in 2003 under authority of the Anti-Terrorism, Crime and Security Act.[9] In 2006, the European Union,[10] however, gave the final

---

use of covert human intelligence sources, including agents, informants and undercover officers); the investigation of protected electronic data; the scrutiny of investigatory powers and codes of practice; and miscellaneous and supplemental provisions. For each of the investigatory powers afforded by it, RIPA ensures that the law clearly covers the purposes for which these powers may be used, which authorities can use the powers, who should authorise each use of these powers, the use that can be made of the material gained, independent judicial oversight and a means of redress for the individual. Since the Act came into force, various supporting regulations have also been enacted in the form of statutory instruments. RIPA has caused considerable concern to commercial and human rights groups. One of the primary concerns is that widespread controls are introduced without a thorough and wide investigation of the extent of the problem. With regard to problems specifically concerning encryption, the issues revolve around the lack of clear evidence that a large number of professional criminals use encryption, the fact that regulation would not prevent dissemination of the technology in any event and that law enforcement agencies have long been able to crack codes. The point is also made that strong encryption prevents crime (for example, fraud). Part III of RIPA, which deals with decryption, has not yet been implemented (see paragraphs 6.3.2.6 and 6.3.3.3 below in this respect). RIPA contains a framework of accountability safeguards, but these have been subject to considerable criticism because of the lack of judicial control. Issues of accountability and justicability are linked to questions of the governance of powers. These issues extend beyond Internet-centred debates and into the mainstream concerns of criminal justice. The police are increasingly involved in information-gathering and systematic surveillance to support intelligence and risk analysis as the bases of modern policing. Issues of prevention and control slip into the hands of security services and the boundaries between an investigation and intelligence gathering tend to blur. See Palfrey 2000 *Information & Communications Technology Law* 178. Some have argued that RIPA was pushed through by blunt assertions by policemen and "spooks" to give M15 access to every digital packet flowing through the servers of all British Internet Service Providers. The Act has been described as consisting of draconian powers to control the Net, and its promulgation was based on scaring the citizenry by exaggerating the risks posed by paedophiles and other criminals to justify those powers. In asking what the real agenda behind RIPA was, it has been stated that it is the beginning of an Orwellian initiative from the government. See Left "Government launches Cybercrime Unit" found on the Internet http://www.guardian.co.uk/internetnews/story/0,7369,474518,00.html 2. The range of offences for which communications data may be obtained was also highly contentious. See Millar "Blunkett will not limit Scope of Measure to Terrorist Cases" found on the Internet http://www.guardian.co.uk/Archive/Article/0,4273,4293489,00.html 3.

8 Communications and traffic data as *per* the English law are defined in paragraphs 6.3.2.4 and 6.3.2.5 below.

9 Of 2003.

10 The European Union was established in 1993 after the ratification of the Maastricht Treaty of 1992 by members of the European Community. The United Kingdom joined the European Union on 1 January 1973. The European Union is an intergovernmental and supranational union of European nations and other organisations (with the same member nations) that are responsible for a common foreign and security policy and for cooperation on justice and home affairs. A total of 25 countries are full members of the organisations of the European Union. The members of the European Union have transferred to it considerable sovereignty, more than that of any other non-sovereign regional organisation. In certain areas, the European Union has begun to take on the character of a federation or confederation. However, in legal terms, member states remain the masters of the Treaties (meaning that the European Union does not have the power to transfer additional powers from states onto itself without their agreement through further international treaties). Furthermore, in many areas, member states have given up relatively little national sovereignty (particularly in key areas of national interest such as foreign relations and defence). Pillar III: Police and Judicial Co-operation in Criminal Matters is the third of the three pillars of the European Union, focusing on co-operation in law enforcement and combating racism (the other two pillars are Pillar I: European Community and Pillar II: Common Foreign and Security Policy). See Answers.com "European Union Law" found on the Internet http://www.answers.com/topic/european-union-law 3-6. European Union law comprises a large number of overlapping legal and institutional structures. This is a result of its being defined by successive international treaties, with each new treaty amending and supplementing earlier ones. In recent years, considerable efforts have been made to consolidate and simplify the treaties, culminating in the final draft of the Treaty Establishing a Constitution for Europe. The heads of state and government of the European Union signed a constitution in 2004, but the constitution subsequently failed to be ratified by member states. If this proposed Treaty is adopted, it will replace the set of overlapping treaties that form the current constitution of the European Union with a single text. See Answers.com "European Union" found on the Internet http://www.answers.com/European%20Union 1-33. The European Union is unique among international organisations in having a complex and highly developed system of internal law which has a direct effect within the legal systems of its member states. It is not a federal government. Nor is it an intergovernmental organisation. It involves a reciprocal agreement within its fields of activity, as if countries "have agreed to work together to agree". There are three types of European Union law, namely primary legislation (treaties); secondary legislation (regulations, directives, decisions, recommendations and opinions made by the European Union's institutions in accordance with the treaties); decisions of the European Court of Justice and the Court of First Instance. Directives by the European Union set goals which must be reached by the member states by a

thumbs-up to a controversial mandatory Data Retention Directive,[11] which it says is necessary to help in the fight against serious crime, particularly terrorism and organised crime. European Union countries have until August 2007[12] to implement the Directive, which was initially proposed after the Madrid bombings in 2004.[13]

These preservation, production and search and seizure mechanisms must, lastly, be considered against the backdrop of the Human Rights Act[14] and the pervasive influence of the European Convention on the Protection of Human Rights. The right to respect for private and family life embodied in article 8 of the European Convention on Human Rights is of particular importance. It states the following:

> Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

certain date, by making their own laws in order to reach this goal. A regulation takes precedence over any member state's domestic law that is inconsistent with it. Member states are not required to make additional domestic laws to implement regulations. See Adviceguide "Civil Rights – In England" found on the Internet http://www.adviceguide.org.uk/index/your_rights/the_european_union.htm 4. The whole body of European Union law together is called the *acquis communautaire*, broken into 31 chapters for purposes of accession negotiations. The European Union has no single seat of government, but many of its most important offices are in Brussels, Belgium. The most important European Union institutions include the Council of the European Union, the European Commission, the European Court of Justice, the European Central Bank and the European Parliament. The European Union is not to be confused with the Council of Europe, as the Council of Europe is a separate organisation and is not part of the European Union (see footnote 37 in paragraph 1.1 above for a reference to the Council of Europe). The Cybercrime Convention was developed under the auspices of the Council of Europe.

11 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection With the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 002/58/EC. Hereinafter referred to as the European Union Data Retention Directive.

12 Article 13 of the European Union Data Retention Directive requires that member states shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive no later than 18 months after its adoption at the latest. Each member state may, for a period of up to 18 months from the expiry of the deadline referred to in paragraph 1, defer application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet email.

13 The current European Union Data Retention Directive is by no means a new invention. See Quintessenz (2006) "EU Data Retention – Doqu/Base" found on the Internet http://www.quintessenz.at/cgi-bin/index?id=000100002986 1. The Directive has drawn fire from privacy advocates who believe the Directive is a threat to human rights. Adopting this Directive would cause an irreversible shift in civil liberties within the European Union. It will adversely affect consumer rights throughout Europe and it will generate an unprecedented obstacle to the global competitiveness of European industry. Telecommunications companies and Internet service providers have expressed concerns about the financial impact of the European Parliament's decision, as the new law will drastically increase companies' storage costs. See c/Net News.com (2006) "EU Data Retention Directive Gets Final Nod" found on the Internet http://news.com.com/2100-7348_3-60423032.html 1.

14 Of 1998. Hereinafter referred to as either the Human Rights Act or the HRA. The HRA gives further effect to the rights and freedoms guaranteed under the European Convention on the Protection of Human Rights. In terms of section 1 of the HRA, the rights and fundamental freedoms in, *inter alia*, articles 2 to 12 and 14 of the European Convention on the Protection of Human Rights are to have effect for the purposes of the HRA. The right to respect for private life and family life under article 8 of the European Convention on the Protection of Human Rights (also cited in Schedule 1 of the HRA) is accordingly specifically made applicable to the English legislative framework.

6.2 Domestic search and seizure of e-evidence

6.2.1 Root domain[15]

Adverse reaction to general warrants and to prerogative authority was just as evident in England as it was in the revolutionary days of the United States. In England, a dislike of the contentious warrant procedure formed an inherent part of the political struggle to establish the supremacy of the common law.[16]

There were two main objections to the issuance of warrants. The first related to the scope of the warrant and the second to the identity of the issuer. At the apotheosis of search powers under the authority of the Star Chamber,[17] these powers were deployed to repress political and religious dissent by seeking out sedition and unlicensed books at any time of the day or night. Reaction to the Star Chamber was one of the main causes of the Great Rebellion of 1642, the beheading of Charles I in 1649, and the Civil Wars of 1642 to 1660. It was, however, not until after the "Glorious" Revolution of 1689 that recognition of the oppressive nature of general warrants grew. The seminal case that established the need for specificity in respect of suspicion and of the items sought was *Wilkes v Wood*[18] where, reviewing a non-statutory authorisation, it was accepted that the law never admits of a general search warrant. The second objection to search warrants, pointed out in *Entick v Carrington*,[19] was that they could be issued by the executive under prerogative power and could thus be used as a tool of political

---

15 See footnote 21 in paragraph 5.2.1 above for a reference to the meaning of "root domain". In this context, a "root domain" is meant to refer to the historical origins of the power of search and seizure in England.

16 Sharpe *Search and Surveillance* 4.

17 The Star Chamber was an English court of law at the royal Palace of Westminster that sat between 1487 and 1641, when the court itself was abolished for abuses of power. See Answers.com "Star Chamber Historical Site, England (In Government)" found on the Internet http://www.answers.com/Star%20Chamber 3. It is useful to recapitulate here the current hierarchy and jurisdiction of the English courts within the criminal justice system for ease of reference. The Magistrate's Court tries summary offences and either-way offences suitable for summary trial; sends indictable-only offences in the Crown Court for trial; hears mode of trial proceedings in either-way offences; holds committal proceedings in either-way offences to be tried on indictment; and deals with preliminary matters including bail and representation orders. The Crown Court tries indictable-only offences and either-way offences committed for trial on indictment; sentences those transferred from the Magistrate's Court for sentence; and hears appeals against conviction and/or sentence from the Magistrate's Court. The High Court (Queen's Bench Division) hears appeals by way of case stated and hears judicial review cases. The Court of Appeal (Criminal Division) hears appeals against conviction and/or sentence from the Crown Court and issues practice directions on criminal procedure and sentencing. The House of Lords is the highest appeal court in almost all cases in England and Wales. The House of Lords hears appeals on points of law of public importance in cases referred from the Court of Appeal (Criminal Division). The Supreme Court of the United Kingdom will be created under the provisions of the Constitutional Reform Act of 2005 to take over the judicial functions of the Law Lords in the House of Lords and from the Judicial Committee of the Privy Council. The Supreme Court of the United Kingdom will then become the final court of appeal in all matters under English law, Welsh law (to the extent that the Welsh Assembly makes laws for Wales that differ from those in England) and Northern Irish law. Offences can be classified according to the place of trial. Summary offences are considered the least serious offences and are tried summarily in the Magistrate's Court. Examples include common assault (section 39 of the Criminal Justice Act of 1988), taking a conveyance without consent (section 12 of the Theft Act of 1968), careless and inconsiderate driving (section 3 of the Road Traffic Act of 1988) and causing harassment, alarm or distress (section 5 of the Public Order Act of 1986). Either-way offences are considered middle-ranking offences and are tried either summarily or on indictment in the Crown Court. The decision as to the trial venue is taken at the mode of trial hearing where the defendant indicates a not guilty plea or makes no indication of plea. Examples include assault occasioning actual bodily harm (section 47 of the Offences against the Person Act of 1861), theft (section 1 of the Theft Act of 1968), burglary (section 9 of the Theft Act of 1968) and affray (section 3 of the Public Order Act of 1986). Indictable offences are considered the most serious offences and, although the case commences in the Magistrate's Court, the trial takes place on indictment before a judge and a jury in the Crown Court. Examples include murder, robbery (section 8 of the Theft Act of 1968) and rape (section 1 of the Sexual Offences Act of 2003). See Hannibal and Mounteford *Criminal Litigation* 19-20.

18 (1763) 19 How St Tr 1153, 98 ER 489.

19 (1765) 19 How St Tri 1030, 95 ER 807.

oppression. These two cases clearly established the hostility of the English courts to any general power of entry that was not based on specific and clear authority. Thus, unless it was specifically authorised by statute, no search warrant was valid if it did not conform to the strict limits of the common law which imposed the requirements of judicial control, particularity and reasonable belief. These elementary requirements have remained in force in respect of contemporary warrants granted in England.[20]

Antagonism towards the warrant procedure resulted in a reluctance to develop any concept of a general power to grant warrants as instruments of criminal investigation. Traditionally, a piecemeal collection of statutes authorised law enforcement officers to enter premises to search for prohibited items and evidence relating to crimes. This caused some peculiar *lacunae* in the law, the best known of which was that there was no power to enter premises to search for evidence of murder.[21] It was not until the promulgation of PACE that a coherent statutory scheme of search and seizure, setting out the powers of and constraints on law enforcers seeking tangible evidence of crime, came into existence.[22] The main innovation effected by PACE was the creation of powers of search and seizure that are not offence-specific, but are instead to be exercised according to statutory criteria that attempt to maintain a balance between crime control and civil liberty. These powers include the right to stop and search a person and her property prior to arrest,[23] to effect road checks,[24] to apply for a warrant to a justice of the peace,[25] to make a warrantless search of persons and of premises on arrest[26] and to apply to a circuit judge for a production order or a warrant to obtain sensitive and/or confidential material.[27]

Most of the powers to authorise searches prior to the promulgation of PACE are retained, so the earlier law has been supplemented, rather than changed.[28] Some of the provisions of PACE,

---

20 Sharpe *Search and Surveillance* 3.

21 *Ghani v Jones* [1970] 1 QB 693; [1969] 3 All ER 1700.

22 Stone *The Law of Entry, Search and Seizure* 105.

23 Sections 1-3 of PACE and its Code of Practice A: Exercise by Police Officers of Statutory Powers of Stop and Search. Hereinafter referred to as the PACE Code of Practice A. Section 66 of PACE provides for the issue of Codes of Practice for the search of premises and the seizure of property. Contravention of a Code of Practice will not give rise to any criminal or civil liability, nor will it automatically render the police officer in question liable to disciplinary proceedings. A court may, however, take into account the breach of the Code of Practice in determining any proceedings to which the breach appears to be relevant. The text of all the Codes of Practice issued under PACE is available on the Home Office's website at www.homeoffice.gov.uk.

24 Sections 4 and 5 of PACE and PACE Code of Practice A.

25 Sections 8, 15 and 16 of PACE and its Code of Practice B: Searches of Premises by Police Officers and the Seizure of Property Found by Police Officers on Persons and Premises (hereinafter referred to as the PACE Code of Practice B) applies to applications for warrants made after midnight on 31 December 2005 and to searches and seizures taking place after midnight on 31 December 2005.

26 Sections 18 and 32 of PACE and the PACE Code of Practice B.

27 Sections 9, 11-14 and Schedule 1 of PACE and the PACE Code of Practice B.

28 Section 8(5) of PACE states that the power to issue a warrant conferred by section 8(5) is in addition to any such power otherwise conferred. Examples of specific entry, search and seizure statutory mechanisms established by the piecemeal legislation that pre-dated PACE include section 26(1) of the Theft Act of 1968; section 5 of the Public Stores Act of 1875; section 23 of the Misuse of Drugs Act of 1971; section 56 of the Drug Trafficking Act of 1994; section 3 of the Obscene Publications Act of 1959; section 2 of the Children and Young Persons (Harmful Publications) Act of 1955; section 4 of the Protection of Children Act of 1978; section 2 of the Indecent Displays Control Act of 1981; section 1 of the Criminal Libel Act of 1819; paragraph 25 of Schedule 2 of the Local Government (Miscellaneous Provisions) Act of 1982 relating to sex cinemas and sex shops; section 17 of the Video Recordings Act of 1984; sections 7 and 24 of the Forgery and Counterfeiting Act of

including the provisions relating to the formalities of warrants, privileged material and the powers of seizure are of general application to law enforcement powers under whatever statute they arise.[29] There is no evidence that the more specific search and seizure powers have been used any less since law enforcement agents have had the general power to obtain a search warrant under section 8 of PACE. The general power applies only to serious arrestable offences[30] and, in some cases, the specific powers may be thought more appropriate.[31]

1981; section 2(4) of the Criminal Justice Act of 1987; section 9 of the Official Secrets Act of 1911; section 2 of the Incitement to Disaffection Act of 1934; section 2 of the Public Order Act of 1936; paragraph 2 of Schedule 1 to the Emergency Laws (Re-enactments and Repeals) Act of 1964 regarding the provision of welfare foods; section 4 of the Biological Weapons Act of 1974; section 13 of the Aviation Security Act of 1982; paragraph 1 and 12 of Schedule 5 of the Terrorism Act of 2000; sections 65 and 66 of the Anti-Terrorism, Crime and Security Act of 2001 in respect of the controlling and storage of certain dangerous substances, such as pathogens and toxins; section 65 of the Offences against the Person Act of 1861; section 73 of the Explosives Act of 1875; section 46 of the Firearms Act of 1968; section 30 of the Firearms (Amendment) Act of 1997 relating to licensed pistol clubs; section 4 of the Crossbows Act of 1987; section 142 of the Criminal Justice Act of 1988 in relation to flick knives and gravity knives as defined in section 1(1) of the Restriction of Offensive Weapons Act of 1959; section 5 of the Knives Act of 1997; section 30 of the Transport and Works Act of 1992 in respect of the conducting of alcohol breath tests; section 26 of the Vehicles (Crime) Act of 2001 relating to the control of businesses supplying registration plates for vehicles and section 9 of the Vehicles (Crimes) Act of 2001 relating to motor salvage businesses; paragraph 17 of Schedule 2 to the Immigration Act of 1971; part 4 and section 161 of the Extradition Act of 2003; section 135 of the Mental Health Act of 1983; section 102 of the Children Act of 1989 supporting powers of search for children; section 48 of the Children Act of 1989 relating to emergency protection orders aimed at children; section 50 of the Children Act of 1989 regarding the recovery of abducted children; section 41 of the Adoption and Children Act of 2002; section 28 of the Children and Young Persons Act of 1933 in respect of the employment of children; section 1 of the Dogs Act of 1906 that provides a power of seizure of stray dogs; section 5 of the Protection of Animals Act of 1911 allowing powers of entry and inspection into a knacker's yard; section 3 of the Performing Animals (Regulation) Act of 1925; section 25 of the Animals (Scientific Procedures) Act of 1986 that controls the performing of experiments of animals; section 5 of the Dangerous Dogs Act of 1991; section 2 of the Game Laws (Amendment) Act of 1960; sections 10, 23 and 51 of the Betting, Gaming and Lotteries Act of 1963; section 43 of the Gaming Act of 1968; section 19 of the Lotteries and Amusement Parks Act of 1976; sections 7, 59, 96, 97, 100, 179 and 180 of the Licensing Act of 2003; section 15 of the Theatres Act of 1968; section 4 of the Exhibitions of Hypnotism Act of 1952; sections 109, 200 and 279(B) of the Copyright, Designs and Patents Act of 1988; section 6 of the Scrap Metal Dealers Act of 1964; section 24 of the Public Order Act of 1986 regarding the possession of racially inflammatory material; section 16 of the Stamp Act of 1891; sections 220 and 259 of the Inheritance Tax Act of 1984; section 187(3) of the Finance Act of 1993 in respect of petroleum revenue tax; section 61, 20C and 111 aimed at distress for taxes, tax fraud and capital gains tax of the Taxes Management Act of 1970, respectively; section 20, 25, 33, 84, 113, 118C, 112, 159, 160, 161A, 162 of the Customs and Excise Management Act of 1979; section 79 of the Alcoholic Liquor Duties Act of 1979; section 17 of the Hydrocarbon Oil Duties Act of 1979; paragraph 10 of Schedule 1 and paragraphs 4, 17 and 18 of Schedule 4 to the Finance Act of 1997 relating to betting; paragraph 4 of Schedule 7 to the Finance Act of 1994 in respect of insurance premium tax; section 139B of the Criminal Justice Act of 1988 that provides a special power of warrantless entry in relation to schools to search for offensive weapons; articles 20, 21 and 22 of European Council Regulation 1/2003, which constitutes part of the part of the enforcement of the European Union's competition law, as expressed in articles 81 and 82 of the European Treaty; section 15 of the Wireless Telegraphy Act of 1949; section 79 of the Telecommunications Act of 1984 and section 196 of the Cable and Broadcasting Act of 1984. Interestingly, section 14 of the Computer Misuse Act of 1990 provides law enforcement with a power to obtain a search warrant in connection with the offences relating to the obtaining of unauthorised access to programs or data held on a computer, as set out in section 1 of the Computer Misuse Act of 1991. The application for such a warrant must be made to a circuit judge, rather than a justice of the peace. The judge must be satisfied that an offence under section 1 has been or is about to be committed in any premises and that evidence relating to it is on those premises. Once on the premises, in addition to having the general powers of seizure under section 19 of PACE, the officer may seize any article which she reasonably believes is evidence that an offence under section 1 has been or is about to be committed. No special provision is made for dealing with items held in electronic form which may be believed to constitute such evidence, but the general provision relating to computerised information contained in section 20 of PACE will apply. See paragraph 6.2.3.1.1 below for a discussion of the section 20 power. An examination of these offence-specific search powers does not resort within the scope of this thesis, as the general criminal procedure powers of search and seizure constitute the real focus of this research. See also paragraph 4.2.1 above in this respect.

29 By virtue of section 15 of PACE and paragraph 1(3)(c) of the PACE Code of Practice B, these various powers referred to in footnote 28 above are now subject to the same due process limitations that apply to warrants authorised in terms of PACE.

30 Serious arrestable offences are defined in section 116 and Schedule 5 of PACE. The offences which are always serious arrestable offences are treason; murder; manslaughter; rape; kidnapping; incest with a girl under the age of 13; buggery with a person under 16; indecent assault concerning an act of gross indecency; causing an explosion likely to endanger life or property under section 2 of the Explosive Substances Act of 1883; intercourse with a girl under the age of 13 under section 5 of the Sexual Offences Act of 1956; possession of fire-arms with the intent to injure, to resist arrest or with criminal intent under sections 16, 17 and 18 of the Firearms Act of 1968; causing death by dangerous driving or by careless driving when under the influence of drink or drugs under section 1 or 37A of the Road Traffic Act of 1988; torture under section 134 of the Criminal Justice Act of 1988; endangering the safety at aerodromes, the hijacking of ships, seizing or exercising control of fixed platforms under sections 1, 9 and 10 of the Aviation and Maritime Security Act of 1990; hijacking of channel tunnel trains, seizing or exercising control of the tunnel system under articles 4 or 5 of the Channel Tunnel (Security) Order 1994 No 570; indecent photographs or pseudo-photographs of children under section 1 of the Protection of Children Act of 1978; publication of obscene matter under section 2 of the Obscene Publications Act of 1959; money-laundering under section 2 of the Proceeds of Crime Act of 2002 and various drug trafficking offences, as specified in paragraph 1 of Schedule 2 to the Proceeds of Crime Act of 2002. In addition, any arrestable offence (as defined in section 24 of PACE) becomes serious if its commission has led, or is intended to or likely to lead to the following consequences: serious harm to the security of the State

6.2.2 *Right to privacy*

In England, due process protections arose from common law and statute law. The absence of a clearly recognised tort of privacy or of any express right to be free from unjustified intrusions into private life[32] has left English lawyers with little room to manoeuvre when they specifically seek to exclude electronically recorded evidence. The case law in England has rarely addressed the human rights issues arising in terms of search powers and in this regard it is embryonic in comparison to that of the United States Supreme Court.[33] In the United States, there has been an entrenched protection against unreasonable searches for two centuries. A subsequent wealth of case law concerning the reconciliation of electronic searches with the Fourth Amendment has been accumulated.[34] The Human Rights Act has now, for the first time, incorporated into English domestic law a right of privacy and the right to a fair trial as *per* articles 8 and 6 of the European Convention on the Protection of Human Rights respectively. The general nature of these precepts leaves considerable room for uncertainty as to the extent to which existing law enforcement powers may be held to be compatible with the Human Rights Act. Law enforcement methodology has been subjected to an ongoing re-evaluation and, in the context of searches in particular, an examination of whether there has been an infringement of privacy through the carrying out of an unreasonable search.[35]

An important structural difference between the application of the Fourth Amendment and the Human Rights Act is the fact that, in England, the legislation conferring the right to privacy may be repealed like any other enactment. Also, any pre-existing legislation will not automatically be repealed to the extent that it is inconsistent with the Human Rights Act. The English courts must strive to interpret statutes in accordance with the Human Rights Act and with European Convention jurisprudence, but, where this is impossible, a declaration of incompatibility may be

---

or to public order, serious interference with the administration of justice or with the investigation of offences or of a particular offence, the death of any person, serious injury to any person, substantial financial gain to any person or substantial financial loss to any person.

31 It may be necessary to use the specific powers to seize items such as stolen goods or drugs covered by the power, but not intended to be used as evidence. Of the still effective pre-PACE legislation dealing with the issue of search warrants, by far the most important is section 26(1) of the Theft Act of 1968. There is an overlap between section 8 of PACE and section 26 of the Theft Act, in that the stolen goods might be evidence of a serious arrestable offence, but section 26 (unlike section 8) will apply even if the offence to which the goods relate is not a serious one. Moreover, under section 26, there is no express requirement that the magistrate must be satisfied that gaining entry otherwise than by a warrant would be unsatisfactory or impracticable. Thus, in cases where it seems on the fact of it that a warrant could be granted under either section, it is simpler to make the application under section 26 of the Theft Act of 1968. See Stone *The Law of Entry, Search, and Seizure* 98.

32 The English courts have consistently denied that in English law there is any separate legal right of privacy. In *Malone v Metropolitan Police Commissioner* [1979] Ch 344, counsel for the plaintiff did not even try to argue for a general right of privacy, accepting that such a right did not exist in English law, but contended for a more restricted right applying to telephone conversations. This, however, was also rejected (at 372-374). In *Wainwright v Home Office* [2003] 4 All ER 969, it was pertinently pointed out that there was no right of privacy at common law. See Stone *The Law of Entry, Search, and Seizure* 6.

33 An exception can be found in *R v Khan* [1996] 3 All ER 289, in which issues of trespass and the (then unincorporated) article 8 of the European Convention on Human Rights were addressed. Sharpe *Search and Surveillance* 6.

34 A number of the most pivotal of these cases were referred to in chapter 5.

35 It is important to remember that although the common law does not protect privacy directly, many of the values that underlie the concept of privacy are respected through other remedies, such as, in appropriate cases, the actions for breach of confidence, nuisance or trespass. This also constitutes the underlying basis for arguments that, since the HRA, the English courts should take the relatively small step of recognising that privacy itself should form the basis for protection. The courts have so far not been prepared to take this step, and seemingly await possible parliamentary intervention. See *A v B and C* [2002] EWCA Civ 337; [2003] QB 195, para 11(vi) and Sharpe *Search and Surveillance* xix.

made.[36] Striking down inconsistent legislation is not within the hands of the judiciary, but in those of a government minister, who may, by order, make amendments to the incompatible legislation if the minister considers that there are compelling reasons to do so.[37] The extent to which the search and seizure, production and preservation mechanisms may be circumscribed by reasonableness criteria is affected by the structural difference between constitutional protections in England and those in the United States.[38]

The Human Rights Act requires judges to determine whether a search has been conducted according to the law, in the light of the right to privacy and personal autonomy contained in article 8 of the European Convention on Human Rights.[39] This is the case whenever the subject of a search seeks legal redress, whether in the form of a civil action, a prerogative order quashing the search and seizure, or by seeking suppression of the evidence resulting from the search. The European Court of Human Rights is largely concerned with complaints arising from inquisitorial jurisdictions. The resultant case law has not necessarily been transmutable into an adversarial system. Whether article 8 of the European Convention on the Protection of Human Rights is really focused on legal formalism and whether it will prove as potent an instrument as the Fourth Amendment in striking down unreasonable searches remains to be seen.[40] Some comfort has been embedded in the *dicta* of the European Court of Human Rights to the effect that any incursion[41] into the right to privacy must be interpreted narrowly and must be convincingly stated.[42]

One important distinction between the Fourth Amendment of the United States Constitution and article 8 of the European Convention on the Protection of Human Rights is that the latter makes no specific reference to powers of search. Article 8(1) creates a general right to privacy by stating that everyone has the right to respect for her private and family life, her home and her correspondence. Article 8 is also engaged where the alleged interference takes place on business premises and relates to business activities.[43] The right to privacy under article 8(1) is not absolute, as article 8(2) permits derogation by a public authority.[44]

---

36 Section 4 of the HRA.

37 Section 10 of the HRA.

38 Sharpe *Search and Surveillance* 39.

39 Section 3(1) of the HRA states that a court must, whenever possible, read primary and subordinate legislation in a way that is compatible with the rights embodied in the European Convention on Human Rights. Section 2 of the HRA requires courts to take account of the jurisprudence of the European Court of Human Rights and of the Commission.

40 Sharpe *Search and Surveillance* 12.

41 A private party acting under the authority of a court order, for example, in the exercise of a civil search order, must also act in accordance with the requirements of article 8 of the European Convention on Human Rights. See *Chappell v The United Kingdom* [1989] ECHR 4; (1990) 12 EHRR 1.

42 *Cremieux v France* [1993] IIHRL 8, (1993) 16 EHRR 357 and *Funke v France* (1993) ECHR 7, 16 EHRR 297.

43 Since the notion of private life must include the right to establish relationships with others, there appears to be no reason why this understanding of privacy should exclude activities of a professional or business nature. It is in the course of their working lives that the majority of people have a significant opportunity of developing relationships with the outside world. See *Niemietz v Germany* 13710/88 [1992] ECHR 80 (1993) 16 EHRR 97 and *Halford v The United Kingdom* [1997] ECHR 32 (1997) 24 EHRR 523.

44 Such derogation must be in accordance with the law and must be necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of

There is no express prohibition on unreasonable searches in English law.[45] The general principle of proportionality, however, applies to all decisions of the European Court of Human Rights and it demands that action must be strictly limited to action necessary to obtain lawful objectives. If a search is made without reasonable suspicion or without reasonable grounds, it cannot be justified as a necessary activity in the prevention of crime and thus would arguably be unlawful, despite any adherence to statutory procedures. One difficulty with this analysis is that those who seek to disprove the existence of probable cause have an uphill struggle, because the information on which warrants and authorisations are granted is likely to be subject to public interest immunity. This immunity relieves law enforcement from the normative obligation to disclose unused material in criminal proceedings where this material might undermine the case for the prosecution or might reasonably be expected to assist the accused's defence. The immunity attaches to sensitive material which includes the identity of informants, covert surveillance locations and material supporting applications for search warrants.[46]

Prior to section 78(1) of PACE,[47] there was an acknowledged, but rarely applied, judicial discretion in English law to exclude evidence that had been improperly obtained.[48] Section 78 now provides for a clear discretion to exclude the fruits of an illegal search.[49] Whilst there have been examples of the exclusion of evidence under this section when there have been flagrant breaches of the provisions of PACE,[50] it is unusual for evidence obtained as a result of a search to be excluded in order to deter law enforcement from impropriety. The courts have traditionally been slow to disallow evidence on this basis and the Court of Appeal will be reluctant to interfere with the trial judge's discretion.[51] The inherent reliability of this kind of evidence means that a trial judge is likely to conclude that the fairness of the proceedings is not adversely affected, despite the way in which the evidence was obtained.[52] In England, maintaining the reputation and integrity of the criminal justice system is not the crucial concern when judicial discretion to exclude evidence is being exercised.[53] The adversarial common law culture that applies to proceedings in the United States, however, permits the argument that evidence

---

health and morals or the protection of the rights and freedoms of others. Section 8(2) of the European Convention on Human Rights.

45 Paragraph 1.3 of the PACE Code of Practice B, however, states that the right to privacy and respect for personal property are key principles of the HRA. Powers of entry, search and seizure should be fully and clearly justified before use, because they may significantly interfere with the occupiers' privacy. The principle of proportionality is also explicitly introduced by requiring law enforcement officers to consider whether the necessary objectives can be met by less intrusive means.

46 Sharpe *Search and Surveillance* 12.

47 Section 78(1) provides that the Court may refuse to allow evidence on which the prosecution proposes to rely to be given, if it appears to the Court that, taking into account all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the Court ought not to admit it.

48 *Kuruma v The Queen* [1955] AC 197; *Callis v Gunn* [1964] 1 QB 495; [1963] 3 All ER 677 and *R v Sang* [1980] AC 402; [1979] 2 All ER 1222.

49 *R v Wright* [1994] Crim LR 55.

50 *R v Quinn Lexis UK CD* 510, [1995] 1 Cr App Rep 480 and *R v Canale* [1990] 2 All ER 187; [1990] Crim LR 329.

51 See Sprack *A Practical Approach to Criminal Procedure* 52/3.

52 The Court of Appeal in *R v Chalkley; R v Jeffries* [1998] QB 848; [1998] 2 All ER 155 has endorsed this approach, stating that, other than in the case of confessions and evidence obtained from the accused after the crime, there is no discretion to exclude evidence unless its quality was or might have been affected by the way in which it was obtained (at 178-179).

53 *R v Khan* [1996] 3 All ER 289.

should be excluded, despite its inherent reliability, if it is obtained in violation of powers granted to law enforcement officers.[54]

6.2.3 Search and seizure of e-evidence with a warrant

Juxtaposed to the supposition of warrants as due process safeguards[55] is the theory of warrants as coercive instruments to obtain incriminating evidence through an exceptional intrusion into a person's privacy traditionally subscribed to by English judges. This somewhat more cautious view of the nature and purpose of warrants was the primary contributing factor to the absence of a general statutory power to search by warrant.[56]

Sections 15 and 16 of PACE equip law enforcement agencies with the power to obtain general search warrants. PACE also creates three categories of privileged material in respect of which law enforcement agencies[57] cannot obtain an ordinary search warrant. Access to material subject to legal privilege[58] cannot be obtained at all. For excluded and special procedure[59] material, law enforcement officers normally have to follow the procedures set out in Schedule 1 of PACE. There are two methods which may be used to gain access to excluded and special procedure material under Schedule 1 of PACE: a circuit judge may either make an order for production or access,[60] or she may issue a search warrant.

In order to assess the extent to which warrants serve to safeguard legitimate expectations of privacy, certain aspects of the warrant process are considered in more detail below. The first issue is the sufficiency of information provided by the applicant to the issuer of the warrant. Linked to this, but a distinct issue in itself, is the question of whether the required judicial scrutiny provides a real control upon the exercise of search powers. Proof of reasonable grounds to believe not only that a serious offence has been committed, but also that there will be evidence regarding the offence on the premises to be searched, may be necessary to comply with the derogation from the right to privacy contained in article 8(2) of the European Convention of Human Rights. Finally, certain aspects relevant to conceptualising an *e*-evidence search strategy are considered, including the role of the computer in the commission of the crime, the knock-and-announce rule, the need for multiple warrants and the search and sift provisions. There are no provisions in English law allowing for a surreptitious search or a

---

54 Sharpe *Search and Surveillance* 13. See footnote 31 of paragraph 5.2.2 above for a reference to the position regarding the exclusion of such "fruits of the poisonous tree".

55 As underscored in the United States. See paragraph 5.2.1 above in respect of the position in the United States.

56 As opposed to offence-specific search warrants, as pointed out in paragraph 6.2.1 above. See also Sharpe *Search and Surveillance* 47.

57 Other officials having the power to obtain search warrants are not limited by section 9(2) of PACE, as this provision applies only to the police.

58 Legally privileged material is defined in paragraph 6.3.2.1 below.

59 Excluded material and special procedure material are defined below in paragraphs 6.3.2.2 and 6.3.2.3 respectively.

60 Schedule 1 production orders are discussed in paragraph 6.3.3.1 below.

delayed notification of the execution of a search as *per* the sneak and peek provisions of the Unites States.[61]

The two different types of search warrants created by PACE are examined below.

6.2.3.1 Search warrant types

6.2.3.1.1 General search warrants in terms of PACE

Sections 15 and16 of PACE contain general provisions which apply to all warrants to enter and search premises,[62] under any enactment.[63] The requirements of sections 15 and 16 should be applied stringently[64] and an entry or search which fails to comply with them is unlawful.[65] The sections impose requirements at each of the application, issue, execution and return stages of obtaining and using a warrant. They provide, *inter alia*, that all search warrants must be executed within one month of their issue,[66] that only one entry may be made under each warrant[67] and that reasonable force may be used to gain entry.[68] Entry and search under a warrant must be at a reasonable hour, unless the purpose of the search may be frustrated.[69]

Section 19 of PACE contains general provisions relating to the seizure of items by a law enforcement officer who is lawfully on the premises, whether by virtue of a warrant, statutory power or the consent of the occupier.[70] Apart from the restriction relating to legal privilege, section 19 empowers a law enforcement officer to seize anything, including excluded or special procedure material, which she has reasonable grounds for believing has been obtained in consequence of the commission of an offence, or is evidence in relation to an offence she is

---

61 See paragraph 5.2.3.4.4 above for a reference to the sneak and peek provisions in the legislative framework of the United States.

62 Premises are defined in section 23 of PACE to include any place and include any vehicle, vessel, aircraft or hovercraft; any offshore installation; any renewable energy installation and any tent or moveable structure.

63 The limitations on the scope of these provisions are important as they only apply to warrants issued to constables (including specialist constables such as those employed by the British Transport Police) and not to other officials. The provisions have, however, also been extended to Customs and Excise officers and officers enforcing the Food and Environment Protection Act of 1985. See Stone *The Law of Entry, Search, and Seizure* 105. As far as the police are concerned, sections 15 and 16 apply only to warrants for both enter and search. A warrant simply to enter and inspect or an arrest warrant used to legitimise entry are not covered by these provisions. See section 17(1)(a) of PACE.

64 In *Kent Pharmaceutical Ltd v Director of the Serious Fraud Office* [2002] EWHC 3023, the stringency of sections 15 and 16 of PACE was recognised. The Court ruled that sections 15 and 16 are sufficiently stringent that if the exercise of a search power is compliant with them, there is no scope for an HRA argument based on article 8 of the European Convention of Human Rights. The Court noted that in drawing up the legislation contained in PACE in the terms that it has, Parliament gave statutory effect to the same principles which article 8 is designed to protect.

65 Section 15(1) of PACE. Those powers of entry which do not depend on a warrant or which depend on a warrant permitting, for example, inspection, rather than search, will be subject only to section 19 and not section 15 and 16 of PACE. See Stone *The Law of Entry, Search, and Seizure* 180.

66 Section 16(3) of PACE.

67 Section 15(5) of PACE.

68 Section 117 of PACE. Where any provision of PACE gives law enforcement officers the power to perform a certain act and does not make that power dependent upon the consent of the person affected by it, reasonable force may be used in the exercise of the power. Reasonable force may accordingly be used, *inter alia*, to search an arrestee both upon arrest and at the police station (sections 32 and 54 of PACE – see paragraphs 6.2.4.1.1 and 6.2.4.1.2 below), to make an intimate search (section 55 of PACE – see paragraph 6.2.4.1.2 below) and to enter and search an arrestee's premises (section 18 of PACE – see paragraph 6.2.4.1.1. below).

69 Section 16(4) of PACE.

70 Section 19(1) of PACE. Paragraphs 5.1 and 5.2 of the PACE Code of Practice B state that a search by consent should normally only take place on the basis of written permission and after giving the occupier full information as to the purposes of the search. Consensual warrantless searches are discussed in paragraph 6.2.4.1.6 below.

investigating or any other offence.[71] The offence need not be a serious one, nor need the article to be seized be in the possession of someone suspected of being implicated in the offence,[72] but the law enforcement officer must have reasonable grounds for believing that the seizure is necessary to prevent the concealment, loss, alteration or destruction of the item. In addition, items obtained from the commission of an offence may be seized to prevent damage to them.[73]

The legal framework for searching and seizing *e*-evidence in a computing context largely mirrors the legal framework for traditional searches and seizures. However, sections 19(4) and 20 of PACE specifically address the seizure of computers and data contained therein. Section 19(4) exists in addition to any other power otherwise conferred[74] and provides that a law enforcement officer who is lawfully on any premises may require any information which is contained in a computer and is accessible from the premises to be produced in a portable, visible and legible form. The law enforcement officer must have reasonable grounds for believing that such information is evidence in relation to an offence or has been obtained in consequence of the commission of an offence. She may also require the information if she reasonably believes that it is necessary in order to prevent its being concealed, lost, tampered with or destroyed. The computer need not be situated on the premises entered, but must simply be accessible from them. Given the growth in electronic communications systems, this might mean a computer situated on the other side of the world. Section 20(2) of PACE extends a similar power to require the production of information held in a computer to any situation where a law enforcement officer, having entered premises in the exercise of a statutory power, has power of seizure under section 8 or 18 of, or paragraph 13 of Schedule 1 to PACE, or any other Act.[75] Neither the power under section 19(4) nor that under section 20 of PACE gives a power to seize as such. Once the information has been produced in the required form, it may only be taken away if this is justified by some other power.[76] Since the power under section 20 only arises where there is a power of seizure, it should be taken as being limited by the terms in which that power of seizure is granted.[77]

---

71 Section 19(2) and (3) of PACE.

72 *Ghani v Jones* [1970] 1 QB 693; [1969]3 All ER 1700.

73 Section 19(2)(b) of PACE.

74 Section 19(5) of PACE.

75 See also paragraph 7.6 of the PACE Code of Practice B. Similarly worded extended powers also exist in, for example, section 43(5)(aa) of the Gaming Act of 1968, which provides that where the law enforcement officer has reasonable cause to believe that information contained in an electronic form and accessible from the premises may be required as evidence, such an officer may require it to be produced in a form which is visible and legible, or from which it can readily be produced in a visible and legible form, and in which it can be taken away. Also, as regards pseudo-photographs that appear to be photographs portraying obscenity in respect of children, but which may actually have been created or adapted by the use of a computer program, the power of seizure extends to copies and to data stored on a computer disks or by other electronic means. See Stone *The Law of Entry, Search, and Seizure* 191.

76 Section 19(3) of PACE.

77 If a law enforcement officer is exercising a power of seizure under, for example, section 3 of the Obscene Publications Act of 1959, she should be limited to requiring the production of information which she has reasonable cause to believe constitutes an obscene article, or which is related to the trade or business carried on at the premises.

Stone[78] submits that printouts would satisfy the requirements of section 19(4), but that disks or tapes would not. He does not expand on this submission, but it presumably relates to the requirements of visibility, legibility and portability. Taking into consideration the wealth of investigative information embedded in a forensic image of the computer data,[79] disqualifying such images as a means of production would severely restrict investigative efforts. There is no apparent reason why forensic images could not be considered within the scope of application of sections 19(4) and 20 of PACE. The gist of these sections is that a law enforcement officer may require any electronic data to be produced in a specified form. It is unclear whether law enforcement officers may obtain such data themselves, but seemingly they are to rely on the co-operation of the holder of the data. If they must depend on the co-operation of the holder of the data, it may, of course, hamper the investigation if the data is in the possession of an accused or uncooperative witness. The accused's right against self-incrimination, which is considered an integral part of the right to a fair trial as enshrined in article 6 of the European Convention of Human Rights, may also come into play. The accused cannot be expected to assist in building the prosecution's case.

Section 21 of PACE directs the law enforcement officer in charge of an investigation to allow access to or to provide copies or photographs of things which have been seized.[80] There is no such duty where the officer has reasonable grounds to believe that to allow access to or to supply a photograph or copy of the item(s) would prejudice the investigation for which the item was seized, or the investigation of any other offence, or criminal proceedings brought as a result of such investigations.[81] A record of the grounds must be made when access is denied.[82] If there are no such grounds when the investigating officer receives a request for access from a person who had custody or control of the seized item immediately before it was seized, or from someone acting on her behalf, she must allow supervised access.[83] Similarly, if a person, who had custody or control of the seized item, requests a photograph or copy of a seized item, the officer must either allow supervised access to it for the purposes of photographing or copying it or must personally supply a photograph or copy within a reasonable time.[84] In addition to these duties, law enforcement has a general power to photograph or copy anything which it has the power to seize.[85]

---

78 Stone *The Law of Entry, Search, and Seizure* 122.

79 See paragraph 2.3.1. in respect of mining the "forensic gold" in search of electronic evidence.

80 Similar access and copying provisions are, for example, provided for in respect of material seized in terms of section 28I and paragraph 25D of Schedule 2 of the Immigration Act of 1971. Another example can be found in paragraphs 1 and 12 of Schedule 5 of the Terrorism Act of 2000, which renders the seized material subject to the access and copying provisions contained in sections 21 and 22 of PACE.

81 Section 21(8) of PACE and paragraphs 7.16 and 7.17 of the PACE Code of Practice B. If property is retained, the person who had custody or control of it immediately before the seizure must, on request, be provided with a list or description of the seized property within a reasonable period.

82 Paragraph 7.17 of the PACE Code of Practice B.

83 Section 21(3) of PACE.

84 Section 21(4), (5) and (6) of PACE.

85 Section 21(7) of PACE. Copies, though not originals, may apparently be provided to foreign law enforcement agencies for whose investigation the production of the material is required. See *R v Crown at Southwark ex parte Customs and Excise*

PACE does not require law enforcement officers to record information following a search, other than on the warrant itself, or for the purposes of fulfilling the obligation under section 21 of PACE to supply a record of what has been seized.[86]

Items seized by law enforcement officers under PACE are not the property of the police,[87] but remain the property of the persons from whom they have been seized.[88] Law enforcement officers may accordingly not hand over seized documents to any party that requests them for the purposes of civil proceedings. The powers to seize and retain are conferred for the better performance of public functions by public bodies and cannot be used to make information available to private individuals for their private purposes.[89] The general principle is that seized items may be retained for as long as is necessary in all the circumstances.[90] An item may specifically be retained for use as evidence in a trial, for forensic examination, to establish its lawful owner when there are reasonable grounds for believing that it has been stolen or obtained by the commission of an offence or for any other investigation in connection with an offence.[91] There is no right to retain items, however, where the warrant and search under which the items were seized are found to be unlawful.[92] Nothing may be retained for the above purposes if a photograph, copy or image would be sufficient.[93] An article may also be retained in order to establish its lawful owner where there are reasonable grounds for believing that it has been obtained in consequence of the commission of an offence.[94] If an item has been seized on the grounds that it might be used to cause physical injury, to damage property, to

---

Commissioners [1990] 1 QB 250; [1989] 3 All ER 673. Originals may only be sent where this has been specifically authorised by the Court, for example, under the Evidence (Proceedings in Other Jurisdictions) Act of 1975.

86 Paragraph 8.1 of the PACE Code of Practice B requires each sub-divisional police station to keep a search register. The officer in charge of a search must, on arrival at a police station, make, or have made, a record of the search, and this should be entered in the search register. The record should include the address of the premises searched, the names of the officers conducting the search and of any person on the premises (if known), whether force was used, and, if so, why, and a list of any damage caused and the circumstances. The record should also include the authority under which the search took place. If this was a warrant, or written consent, a copy should be attached to the record, or kept in a place identified in the record. If the authority was a statutory power of entry without warrant, the record should include information about the power. Finally, the record must include a list of articles seized, or a note of where such a list is kept. If any of the articles was not covered by a warrant, the reason for the seizure should be stated.

87 *Marcel v Commissioner of Police of the Metropolis* [1992] Ch 225; [1992] 1 All ER 72.

88 With the exception, of course, of stolen property. See *Webb v Chief Constable of Merseyside Police; Porter v Chief Constable of Merseyside Police* [2000] QB 427; [2000] 1 All ER 209 and *Costello v Chief Constable of Derbyshire Constabulary* [2000] QB 427; [2001] EWCA Civ 381.

89 *Marcel v Commissioner of Police of the Metropolis* [1992] Ch 225; [1992] 1 All ER 72, 81. The position will be different if documents were sought by means of a subpoena *duces tecum*. Since the true owner would be obliged to comply with such a subpoena, there is no reason why law enforcement should not be under a similar obligation, subject only to the true owner's having a right to challenge the subpoena or the production of the documents, on any grounds on which a subpoena can be challenged. Stone argues that there is no reason why the principles adopted by the Court of Appeal in the *Marcel* case should not extend to any items other than documents in law enforcement possession as a result of a seizure governed by PACE. See Stone *The Law of Entry, Search, and Seizure* 123.

90 Section 22(1) of PACE. In *Marcel v Commissioner of Police of the Metropolis* [1992] Ch 225; [1992] 1 All ER 72, 87, it was suggested that the seized items may be retained for as long as is necessary for carrying out the purpose for which the powers given by sections 19 and 20 of PACE have been conferred. Note 7G to the PACE Code of Practice B also provides that when material is seized under the powers of seizure conferred by PACE, the duty to retain it under the Code of Practice issued under the Criminal Investigations Act of 1996 is subject to the provisions on retention of seized material in section 22 of PACE.

91 Section 22(2)(a) of PACE.

92 *R v Chief Constable of Lancashire ex parte Parker and McGrath* [1993] 2 All ER 56.

93 Section 22(4) of PACE and paragraph 7.15 of the PACE Code of Practice B.

94 Section 22(2)(b) of PACE.

interfere with evidence or to assist in escape from police detention, it may only be retained while the person from whom it was seized is in custody and has not been released on bail.[95]

6.2.3.1.2 Search warrants for excluded and special procedure material

In order to gain access to excluded or special procedure material, law enforcement agencies normally lodge an application under Schedule 1 of PACE.[96] The issue of a warrant to search for excluded or special procedure material should be a last resort.[97] It is a prerequisite for the issue of a warrant that the circuit judge to whom the *ex parte* application is made should be satisfied that one of the two sets of access conditions in relation to production orders[98] has been fulfilled.[99]

The first set of access conditions entails, in short, that there must be reasonable grounds for believing that a serious arrestable offence has been committed and that, on specified premises, there is special procedure material which is likely to be relevant evidence of substantial value to the investigation. Access to such material must further be deemed to be in the public interest. In addition, the circuit judge issuing the search warrant must also be satisfied of the existence of one of the following further conditions. The first two of these are that it is not practicable to communicate with the person who has power to grant entry to the premises, or access to the material, as under section 8(3) of PACE.[100] Although generally it would be very difficult to argue that it was not practicable to communicate with a firm of solicitors where items relevant to the investigation of a third party were sought, the position might be different where the solicitors themselves were the subjects of the investigation.[101] In general, it is unusual for a warrant to be

---

95 Section 22(3) of PACE.

96 Section 9(1) of PACE. In terms of section 9(2) of PACE, this applies even where the material could previously have been obtained by a search warrant issued under some other statute. As regards search warrant powers included in legislation passed after PACE, the Act is silent. The position therefore seems to be that, if the later Act itself contains no limitation, law enforcement officers will be able to search for excluded, special procedure and even legally privileged material with an ordinary search warrant. Because of the serious implications of this for the policy behind the introduction of the Schedule 1 procedure, it would be best if Parliament always made specific reference to privileged material when enacting, or re-enacting, search warrant powers. See Stone *The Law of Entry, Search, and Seizure* 139.

97 See *R v Crown Court at Lewes ex parte Hill* [1991] 93 Cr App R 60 and *R v Crown Court at Southwark ex parte Bowles* [1998] 2 All ER 193; [1998] 2 Cr App R 187. The last resort requirement applicable to search warrants aimed at excluded or special procedure material is also confirmed by the additional non-statutory safeguards set out in paragraphs 6.14 and 6.15 of the PACE Code of Practice B. These safeguards are applicable to all searches under Schedule 1 of PACE and Schedule 5 of the Terrorism Act of 2000. The PACE Code of Practice B contains a number of additional provisions relating to the execution of warrants issued under Schedule 1. An officer should be appointed to take charge of the execution of the warrant. The officer in charge is enjoined to ensure that the search is conducted with discretion and with the least possible disruption of the business or other activities on the premises. Before searching the premises, the officer should ask for the material in question to be produced. The officer might also ask for indices to files on the premises to be produced and seek to inspect any files which an index seems to show might contain any of the material sought. Only if these procedures are refused, or ineffective, or for some other reason the officer thinks that a physical search of the premises is necessary, should one be carried out. A more extensive search of the premises may be made only if the person responsible for them refuses to produce the material sought, to allow access to the index or if it appears that the index is inaccurate or incomplete.

98 See paragraph 6.3.3.1 below for an exposition of the two sets of access conditions applicable to production orders in terms of Schedule 1 of PACE.

99 *R v Crown Court at Liverpool ex parte Wimpey plc* [1991] Crim LR 635 para 12.

100 Paragraphs 14(a) and (b) of Schedule 1 of PACE. See *R v Crown Court at Liverpool ex parte Wimpey plc* [1991] Crim LR 635.

101 The meaning of practicable in this context was considered by the Divisional Court in *R v Leeds Crown Court ex parte Switalski* [1991] Crim LR 559. A warrant had been issued to search the premises of a firm of solicitors suspected of having been involved in the commission of serious arrestable offences. The judge issuing the warrant had accepted that it was not practicable to communicate with the solicitors in these circumstances.

issued against a firm of solicitors.[102] The third condition relates to the nature of the information. This condition is fulfilled if the material is subject to a statutory restriction on disclosure.[103] The fourth possible condition is that service of notice to apply for an order under paragraph 4 of Schedule 1 to PACE may seriously prejudice the investigation.[104] This is obviously the widest of the conditions and needs close supervision by the issuing judge if it is not to lead to abuse. The responsibility for ensuring that the procedure in Schedule 1 of PACE is not abused lies with circuit judges and they must be scrupulous in discharging this responsibility.[105]

A judge may issue an all premises warrant[106] if she is satisfied that there are reasonable grounds for believing that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application, as well as those which are, in order to find the material in question, and that it is not reasonably practicable to specify all the premises which she occupies or controls and which might need to be searched.[107]

If the applicant relies on the second set of access conditions,[108] that is, that a search warrant would have been obtained in relation to the material but for PACE, there is an additional ground on which a warrant may be issued. This is where an order under paragraph 4 of Schedule 1 of PACE has not been complied with.[109] The warrant authorises a law enforcement officer to enter the premises and search them.[110] She may seize anything which the warrant authorises her to search for. A warrant issued under Schedule 1 of PACE also falls within the scope of its general provisions, as set out in sections 15 and 16.[111] Non-compliance with an order, however, does not justify the issue of a warrant where it is the first set of access conditions which is being relied on. This simply falls to be treated as contempt of court.[112]

---

102 This was the view of the Divisional Court in *R v Southampton Crown Court ex parte J and P* [1993] Crim LR 962, where it was held that the need for an *ex parte* application had not been made out. Here warrants to search solicitors' offices issued under paragraph 14 of Schedule 1 of PACE were quashed because they were too widely drawn; insufficient attention had been given to the issue of legal privilege; and the need for an *ex parte* application had not been made out. A similar view was taken in *R v Crown Court at Southwark ex parte Sorsky Defries* [1996] Crim LR 195, where the warrant was sought in relation to a firm of accountants.

103 For example, under section 11(2)(b) of PACE. The information must be likely to be disclosed in breach of this if the warrant is not issued. See paragraph 14(c) of Schedule 1 of PACE. This would apply, for example, to information covered by the Official Secrets Act of 1989. See Stone *The Law of Entry, Search, and Seizure* 146.

104 Paragraph 14(d) of Schedule 1 of PACE.

105 *R v Maidstone Crown Court ex parte Waitt* [1988] Crim LR 384. See also Stone *The Law of Entry, Search, and Seizure* 148.

106 An all premises warrant is a warrant to search all premises occupied or controlled by a person specified in paragraph 2(a)(ii) or 3(a) of Schedule 1 of PACE, including sets of premises as specified in the application. It is interesting to note that sections 26 to 30 of the newly introduced Terrorism Act of 2006 make specific provision for all premises warrants for England, Wales, Northern-Ireland and Scotland; the search, seizure and forfeiture of terrorist publications; the power to search vehicles under Schedule 7 to the Terrorism Act of 2000; and the extension of authorisations to stop and search.

107 Paragraphs 12 and 13 of Schedule 1 and paragraph 3.6 of the PACE Code of Practice B.

108 See paragraph 6.3.3.1 below for a discussion of the second set of access conditions, as set out in Schedule 1 of PACE.

109 Paragraph 12(b) of Schedule 1 of PACE.

110 Paragraph 12 of Schedule 1 of PACE.

111 *R v Central Criminal Court ex parte AJD Holdings* [1992] Crim LR 669.

112 Paragraph 15 of Schedule 1 of PACE.

Where an application for a search warrant is made under Schedule 1 of PACE, the application must also indicate why it is believed that service of the notice of application for a production order may seriously prejudice the investigation.[113]

6.2.3.2 Particularity and specificity

The application for a search warrant, made to a justice of the peace, magistrate or judge as required by the provision under which the warrant is being sought must be supported by written information.[114] The applicant has a duty to make the grounds clear on which the application is based and the enactment under which the warrant would be issued.[115] There is no need for the warrant to be specific as to any suspected offences which lead to the issue of the warrant or to state the grounds for suspicion, or even to say that the person issuing the warrant was satisfied that reasonable grounds existed. Whilst it may be desirable in some cases to specify the grounds for application, their absence does not invalidate the warrant.[116] A law enforcement officer who receives information which appears to justify an application for a warrant should check its accuracy as far as possible. The officer should be prepared to answer questions about the accuracy of the information and the reliability of the source from which it came.[117]

The officer should also try to establish the nature and location of the articles to be searched for and how it relates to the suspected crime under investigation.[118] In situations where the warrant is issued to search for subversive or obscene material, the borderline between criminality and a lawful titillation is not necessarily clear-cut and the courts are more likely to strike down imprecise wording.[119]

The application for the warrant must explain that there are no reasonable grounds to believe that the material to be sought is legally privileged, special procedure or excluded material.[120] The officer who makes the application must make reasonable enquiries to establish whether anything is known about the occupier and whether the premises have previously been searched and, if so, how recently.[121] The search warrant application must specify whether the warrant authorises entry and search of one set of premises. In relation to premises in multiple

---

113 Paragraph 3.7 of the PACE Code of Practice B. Applications for search warrants under paragraph 11 of Schedule 5 of the Terrorism Act of 2000 must also indicate why a production order would not be appropriate.

114 Section 15(3) of PACE.

115 Section 15(2) of PACE.

116 Stone *The Law of Entry, Search, and Seizure* 26.

117 The law enforcement officer should not have to disclose the identity of an informant, but information from an anonymous source should not be acted on without seeking corroboration. Section 15(4) of the Police and Criminal Evidence Act of 1984 and paragraph 3.1 of the PACE Code of Practice B. No application should be made without the authorisation of an officer of at least the rank of inspector, except in a case of urgency, when the senior officer on duty may give approval (paragraph 3.4(a) of the PACE Code of Practice B). Similarly, if there is reason to believe that a search might adversely affect relations between the police and the community, the local police community liaison officer should be consulted (paragraph 3.5 of the PACE Code of Practice B).

118 *R v Central Criminal Court ex parte AJD Holdings* [1992] Crim LR 669.

119 In *Darbo v DPP* [1992] Crim LR 56, it was held that "sexually implicit" did not necessarily mean "obscene".

120 Paragraph 3.6(e) of the PACE Code of Practice B.

121 Paragraph 3.2 and 3.3 of the PACE Code of Practice B.

occupations, the application should make it clear which parts of the premises are to be covered by the warrant.[122] It must also be specified whether the application is for a warrant authorising entry and search on more than one occasion, the grounds for multiple entries and whether the desired number of entries authorised is unlimited or a specified maximum.[123]

If the application is under section 8 or paragraph 12 of Schedule 1 of PACE 1984, the warrant must also specify whether the warrant is directed at more than one set of premises or all premises occupied or controlled by a specified person.[124] Where, however, such a warrant is for a single warrant to enter and search more than one set of specified premises, the officer must specify each set of premises to be entered and searched. Where the single warrant is levelled at all premises occupied or controlled by a specified person, the officer must specify the following details:[125]

(a) as many sets of premises as the officer desires to enter and search as it is reasonably practicable to specify;

(b) the name of the person who is in occupation or control or those premises and any others which the officer desires to search;

(c) why it is necessary to search more premises than those which can be specified; and

(d) why it is not reasonably practicable to specify all the premises which law enforcement desires to enter and search.

A search warrant must contain a certain minimum of information.[126] It must specify the name of the person applying for it, the date of issue, the enactment under which it is issued and the premises to be searched. It must, as far as is practicable, identify the articles or persons to be sought.[127] The issuing justice, magistrate or judge should ensure that the material is clearly described, which implies a fairly high degree of specificity.[128] The specification of articles in the

---

122 See *R v South Western Magistrates' Court ex parte Cofie* [1997] 1 WLR 885.

123 Paragraph 3.6(db) of the PACE Code of Practice B.

124 Paragraph 3.6(b) of the PACE Code of Practice B.

125 Paragraph 3.6(da)(ii) of the PACE Code of Practice B.

126 Section 15(6) of PACE.

127 The requirement of facial validity, however, does not mean that every officer authorised to execute the search must be individually named, or that every single detail concerning the object of the search must be particularised. See *R v Hunt* 16 Cr App R (s) 87; [1994] Crim LR 747. Paragraph 4.4 of the PACE Code of Practice A and paragraph 2.9 of the PACE Code of Practice B provide that nothing in the Code requires the identity of officers, or anyone accompanying them during a search of premises, to be recorded or disclosed in the case of enquiries linked to the investigation of terrorism or if officers reasonably believe that recording or disclosing their names might put them in danger.

128 Paragraph 14.3 of the Judicial Studies Board *District Judge's (Magistrate's Court) Benchbook*, which is available on the Judicial Studies Board website: www.jsboard.co.uk/magistrates. In *R v South Western Magistrate's Court ex parte Cofie* [1997] 1 WLR 885 and *R v Atkinson* [1976] Crim LR 307, the Divisional Court granted judicial review of the issuance of a search warrant where the warrant gave the correct address of premises in multi-occupancy, but did not specify the actual flat to be searched.

warrant must match that in the information which formed the basis of the application.[129] The warrant may authorise other people to accompany the law enforcement officer executing the warrant and these should be identified as precisely as possible.[130] Where the police are accompanied by others, the police must remain in clear control of the operation.[131]

A search under a warrant may only be a search to the extent required for the purposes for which the warrant was issued.[132] A search must stop once everything specified in the warrant has been found or once the officer in charge is satisfied that what is being sought is not on the premises.[133] A warrant under section 8 of PACE may authorise entry to and search of premises on more than one occasion if, on the application, the justice of the peace is satisfied that it is necessary to authorise multiple entries in order to achieve the purpose for which the warrant was issued. No premises may be entered or searched on any subsequent occasions without the prior written authority of an officer of the rank of inspector who is not involved in the investigation. All other warrants authorise entry on one occasion only.[134] Where a warrant under section 8 or paragraph 12 of Schedule 1 of PACE authorises entry to and search of all premises occupied or controlled by a specified person, no premises which are not specified in the warrant may be entered and searched without the prior written authority of an officer of the rank of inspector who is not involved in the investigation.[135]

The officer executing a search warrant is required to make an endorsement on it stating whether the articles or persons sought were found and whether any articles other than those sought were seized.[136] There is no obligation on an officer to supply a receipt for what has been seized, unless she receives a request thereto from a person showing herself to be the occupier of the premises where the seizure occurred, or to have had possession or custody of the thing seized immediately before it was seized.[137]

An executed warrant, or a warrant which has not been executed before expiry, must be retained for 12 months from its return[138] and if during that period the occupier of the premises to which it relates asks to inspect it, she shall be allowed to do so.[139]

---

129 In *R v Central Criminal Court ex parte AJD Holdings* [1992] Crim LR 669, this was not the case and the warrant was held to be invalid, since it appeared to give the person exercising it a much wider scope to search and seize than would have been justified by the information.

130 Section 16(1) of PACE.

131 In *R v Reading Justices, Chief Constable of Avon and Somerset and Intervention Board for Agricultural Produce ex parte South West Meat Ltd* [1992] Crim LR 672, the police had been granted a warrant and searched premises in conjunction with officials from the Board of Agricultural Produce. These officials had apparently decided how the search should be conducted, what documents should be seized and where they should be taken. This was held to render the search and seizure unlawful and led to the award of substantial damages against the police and the Board of Agricultural Produce.

132 Section 16(8) of PACE.

133 Paragraphs 6.9A and 6.9B of the PACE Code of Practice B.

134 Paragraph 6.3A of the PACE Code of Practice B.

135 Paragraph 6.3B of the PACE Code of Practice B.

136 Section 19(6) of PACE.

137 Section 21(1) of PACE. The request may be made at the time of the search or later: no time limit is specified. The officer must provide a record of what was seized within a "reasonable time" of the request's being made (section 21(2) of PACE).

138 Section 16(11) of PACE.

6.2.3.3 Judicial supervision

Closely related to the question whether sufficiently specific information has been presented to a magistrate to enable a proper decision to be made is the adequacy of scrutiny accorded to a warrant application. The issuing authority must be satisfied that sufficient grounds exist for the issue of the warrant and may question the applicant to this end.[140] The issuer of a search warrant may not to be rushed into a decision and must be rigorous in ensuring that the relevant requirements are met, given the intrusive nature of the power granted. It is the duty of the issuer of the warrant, not the applicant, to ensure that the correct criteria are met.[141] A lack of magisterial scrutiny could preclude an assessment of probable cause.[142] It has been noted that applications involving the seizure of computer data need to be very carefully handled and that, both for the protection of the defendants and for the proper administration of justice, it is important that applications are made to those expert in the field of computer law. Forum shopping for tactical reasons with the aim of obtaining an advantage by putting the case before a judicial officer who is not a specialist in the field will not be tolerated.[143]

Some concern was noted that the magistracy and even judges, in Schedule 1 of PACE situations, may not be examining applications for search warrants as rigorously as they should.[144] Although it has been said that the appropriate judicial authority should herself be satisfied that the criteria for granting a warrant are satisfied and that it does not suffice for the person laying the information to say that they are,[145] it is often impossible to obtain an impartial account of the hearing and thus to challenge the issuance of a warrant effectively. The absence of extraneous grounds to quash a warrant works against those seeking to challenge what has occurred during the hearing of the *ex parte* application. One difficulty in determining the level of

---

139 Section 16(12) of PACE.

140 Useful guidance on the sort of questions that should be asked is to be found in the Judicial Studies Board *District Judge's (Magistrate's Court) Benchbook* available on the Judicial Studies Board website: www.jsboard.co.uk/magistrates. The checklist which appears in Appendix 2 to the *District Judge's (Magistrate's Court) Benchbook* is particularly useful both to those issuing warrants and to those applying for them. This is intended for district judges, but the approach outlined will be of use to all those entrusted with the power of issuing warrants. Although the applicant is, for example, not expected to identify informants, the issuer may wish to know whether the informant is known to the applicant, has been reliable in the past, has a criminal record and whether she knows the occupier. The issuer may also want to know whether it has been possible to make further enquiries to verify the information. See Stone *The Law of Entry, Search, and Seizure* 27.

141 See *R v Thames Magistrate's Court ex parte Hormz* [1983] 163 JP 19.

142 *R v Reading Justices, Chief Constable of Avon and Somerset and Intervention Board for Agricultural Produce ex parte South West Meat Ltd* [1992] Crim LR 672.

143 Anon 2002 *Informa UK Ltd Intellectual Property Newsletter* 1.

144 A few reported cases show that the rubber-stamping of applications does occur. In *R v Reading Justices, Chief Constable of Avon and Somerset and Intervention Board for Agricultural Produce ex parte South West Meat Ltd.* [1992] Crim LR 672, the Divisional Court considered that the facial errors in and generality of the warrant raised questions as to how closely the justices had enquired into it. The previous cooperative relationship between the Intervention Board and the subject of the application and the lack of specificity on the face of the warrant produced external evidence of rubber-stamping. Similarly, in *R v Southwark Crown Court and HM Customs and Excise ex parte Sorsky Defries* [1996] Crim LR 195, a circuit judge considered an application on behalf of Customs and Excise for a search warrant directed at a firm of accountants concerning money laundering activities that had taken place in the United States. The search was pursuant to a request from authorities in the United States under the Criminal Justice (International Cooperation) Act of 1990 and PACE section 9 and Schedule 1. The judge was not told of the particular jurisdictional and other issues involved in the case and he granted the application within a couple of minutes. The Divisional Court stated that it was clear that the judge could not in fact have been satisfied of those matters of which he was obliged to be satisfied before issuing a warrant. See also Sharpe *Search and Surveillance* 50.

145 *R v Crown Court at Lewes ex parte Hill* [1991] 93 Cr App Rep 60.

scrutiny accorded to applications under section 8 of PACE is that they are heard *ex parte*. The keeping of notes by the justices' clerk, although it is frequently endorsed as good practice, is not mandatory.[146]

Effective monitoring of compliance with the rhetoric of careful supervision is frustrated by claims of public interest immunity. It creates difficulties for those who seek to challenge the basis of a search, whether it is a physical search for tangible evidence, or whether it is an electronic search for intangible evidence. The problem is that law enforcers frequently work on the basis of a tip-off or on the basis of undercover observation and are unwilling to reveal preliminary sources of information.[147]

The English two-tier statutory scheme for warrants[148] provides an acceptance of the fact that whilst the most sensitive and intrusive searches require the scrutiny of a professional lawyer, applications to search for other evidence may be heard by the magistracy. The non-consensual search for and seizure of evidence other than legally privileged evidence, excluded and special procedure confidential material, has, under section 8 of the Police and Criminal Justice Act, been placed in the hands of justices of the peace who are usually not legally qualified.[149] The question of the detachment and independence of the judicial officer considering the application for a search warrant is not one that has, to date, much vexed the English court, but the absence of jurisprudence on this matter may be short-lived.[150] The decisions that come from the European Court of Human Rights demonstrate that article 8 not only requires legal certainty in the application of search procedures, but also (at least where evidence from that search is later relied on by the prosecution)[151] the scrutiny of an independent judge.[152]

---

146 See for example *R v Chief Constable Warwickshire Constabulary ex parte Fitzpatrick* [1998] 1 All ER 65; [1998] Crim LR 290.

147 Public interest immunity includes the concept of informer privilege provided for in the United States legislative framework. In England, however, the concept of public interest immunity goes well beyond the protection of informers. Paragraph 6.12 of the Code under the Criminal Procedure and Investigations Act of 1996 specifies a long list of sensitive material that need not be disclosed unless the Court so orders. The list includes general categories such as material given in confidence; but it also specifies, more particularly, material upon the strength of which search warrants were obtained. Added to this is any material that might reveal the identity of informants, undercover officers, the location of surveillance operations and techniques or methods used in police investigations. A judge will only order the disclosure of sensitive material when the disputed material may prove the defendant's innocence or avoid a miscarriage of justice (*R v Keane* [1994] 2 All ER 478; [1995] Crim LR 225). In the case of *R v Turner* [1995] 2 Cr App R 94, the increased tendency of defendants to allege that they had been set up or had acted under duress was deprecated. The Court ruled that actual compliance with the PACE Code of Practice B may only be tested in court in those cases where a defendant can show a reasonable possibility that information about the informant will bear upon the issues (at 98). It can be assumed that, in England, the maintenance of informer privilege will not be found to violate the HRA. Article 6 of the European Convention on the Protection of Human Rights and Fundamental Freedoms grants the right to a fair trial. However, the European Court of Human Rights has recognised that the right of the defendant to receive a fair trial, as per article 6 of the European Convention of Human Rights, must be balanced against the interests of society (*Kostovski v The Netherlands* (1989) 12 EHRR 434 at paragraph 44). The European Court of Human Rights has failed to uphold claims by English defendants who have submitted that there was an unfair trial because of non-disclosure of information relating to informants. See, for example, *Jasper v UK* App. No. 27052/95; *Fitt v UK* App No 29777/96 and *Rowe and Davis v UK* App No 28901/95. In *R v Baker* [1996] Crim LR 55, the defendant alleged that there had been no real informant, as alleged by the police, and that, after an improper warrant had been obtained, drugs were planted on him. See generally Sharpe *Search and Surveillance* 56.

148 See the exposition of the two different types of search warrant in paragraphs 6.2.3.1.1 and 6.2.3.1.2 above,

149 In England, stipendiary magistrates are professional lawyers, but the vast majority of justices are lay justices with no legal qualifications. Sharpe *Search and Surveillance* 50 and 70.

150 Sharpe *Search and Surveillance* 53.

151 See *Preston v UK* [1997] 6 EHRLR 695. Information obtained through telephone tapping is not admissible against an accused when obtained under a warrant issued by the Secretary of State.

6.2.3.4 Reasonable grounds

Probable cause is a fluid concept, turning on the assessment of probabilities in particular factual contexts. It is not readily reduced to a neat set of legal rules and it undoubtedly comes in many shapes and sizes.[153]

There are three situations related to powers of entry, search and seizure where the question may arise whether someone involved in the exercise of a power has reasonable grounds for action:[154]

(a) where a warrant is issued, the justice or judge issuing the warrant generally has to be satisfied that the person who seeks the warrant has reasonable grounds to support the request for it to be issued;

(b) a person executing a warrant, having gained entry to premises under it, may be required to have reasonable grounds for suspicion before taking further action, such as arresting a person, or seizing property, found on the premises;

(c) where a law enforcement officer takes action under a power which does not require a warrant (again there is generally a requirement that reasonable grounds for suspicion exist before the action is taken).

In all three situations above it seems to be settled law that the question of whether or not there are reasonable grounds is an objective one.[155] The test is whether a reasonable man, assumed to know the law and possessed of the information possessed by the defendant, would believe that there was a reasonable and probable cause for the action involved.[156] What constitutes reasonable grounds has been accepted to be a question of law. Whether such grounds do exist is a question of fact. It should therefore be possible to decide, within fairly broad limits, what amounts to reasonable grounds and what factors the person making the decision on the spot is entitled to take into account in reaching a decision.[157]

The amount of information required to qualify a reasonable suspicion, in respect of the truth of a certain fact, as based on reasonable grounds, is obviously limited. It is not a question of

---

152 *Klass v Federal Republic of Germany* (1978) 2 EHRR 214; 5029/71 [1978] ECHR 4 at paragraph 55; *Cremieux v France* (1993) 16 EHRR 357.

153 Sharpe *Search and Surveillance* 59.

154 Stone *The Law of Entry, Search and Seizure* 20.

155 This approach was applied in the context of entry, search and seizure powers by the House of Lords in *R v Internal Revenue Commissioners ex parte Rossminister* [1980] AC 952; [1979] 3 All ER 385, 70 Cr App Rep 159, 1000 (Lord Wilberforce), 1011 (Lord Diplock), 1025 (Lord Scarman). See Stone *The Law of Entry, Search and Seizure* 21.

156 *Dallison v Caffrey* [1965] 1 QB 348; [1984] 2 All ER 610, 371.

157 Paragraphs 2.2-2.11 of the PACE Code of Practice A, dealing with statutory powers of stop and search, also contain some useful guidance as to the kind of factors which are relevant to establishing reasonable grounds.

whether there are grounds to support a belief that the fact is true, but that the fact may be true. There is clear authority that nothing in the nature of a *prima facie* case is required.[158] Factors which would not be admissible in evidence in establishing a *prima facie* case, such as the suspect's known character and previous convictions, may be taken into account in establishing the existence of reasonable grounds for suspicion.[159] Some basis capable of evaluation by an objective third person must be shown.[160] The courts are unwilling to accept hunches as reasonable grounds for suspicion.[161]

At the crux of determinations of reasonability is the requirement that a legally protected search must not be so lacking in *indicia* of probable cause as to render official belief in its existence entirely unreasonable. If there is apparent insufficiency of probable cause, then the search is an unreasonable one. If an individual has given reasonable grounds to law enforcement officers to search for evidence of crime, then she cannot complain of a privacy violation, since there is no right to secrete evidence of offending. This principle is implicit in the Constitution of the United States and explicit in article 8(2) of the European Convention on Human Rights. Article 8(2) allows derogation from the right to privacy where a public authority acts in accordance with the law and the derogation is necessary in a democratic society for the prevention of disorder or crime. An unreasonable search is not a necessary one and, whilst probable cause does not separate the guilty from the innocent with any precision, it goes a long way toward doing so.[162]

A requirement of reasonable grounds for suspicion predicates that all search powers under PACE itself preclude an unreasonable search.[163] Whilst apparent probable cause is an essential component of a warrant application, it may only be established by an initial investigation that itself complies with article 8 of the European Convention on Human Rights.[164]

---

158 *Dumbell v Roberts* [1944] 1 All ER 326.

159 *McArdle v Egan* [1933] All ER Rep 611, 150 LT 412, 413 and *Shaabin Bin Hussein v Chong Fook Kam on Appeal from the Federal Court of Malaysia* [1970] AC 942.

160 This may be no more than that information is received from a reliable informant. See *McArdle v Egan* [1933] All ER Rep 611, 150 LT 412, 413.

161 Stone *The Law of Entry, Search and Seizure* 22. In *O'Hara v United Kingdom* (2002) 34 EHRR 32, the European Court of Human Rights confirmed that the approach taken by the House of Lords on this issue in *O'Hara v Chief Constable of the Royal Ulster Constabulary* [1997] 1 All ER 129; [1997] 1 Cr App Rep 447 is in line with the requirements of article 5 of the European Convention of Human Rights. Facts which raise a reasonable suspicion on which an arrest must be based need not be on the same level as those necessary to justify a conviction, or even the bringing of a charge which comes at the next stage of the process of criminal investigation (at 36). Although it is likely that the principles to be derived from these arrest cases would apply in a similar way in relation to entry, search and seizure, there are few authorities on this area. In *Reynolds v Commissioner of Police for the Metropolis* [1985] QB 881; [1984] 3 All ER 649, 80 Cr App Rep 125, the Court of Appeal had to consider another case where large quantities of documents had been removed, this time by the police. The view was taken that the police had to have reasonable cause for suspicion as regards each file, book, bundle or separate document, but need not go through each file or bundle examining individual sheets (at 890). The powers of the police in dealing with quantities of documents, etc, have been extended by the search and sift powers contained in Part 2 of the Criminal Justice and Police Act of 2001. See paragraph 6.2.3.5.3. below.

162 Sharpe *Search and Surveillance* 58.

163 Searches may be made other than on reasonable grounds in respect of individuals and vehicles under, for example, the Prevention of Terrorism (Temporary Provisions) Act of 1989 sections 13A (inserted by the Criminal Justice and Public Order Act of 1994 section 81) and 13B (inserted by the Prevention of Terrorism (Additional Powers) Act of 1996 section 1). Sharpe *Search and Surveillance* 15.

164 Sharpe *Search and Surveillance* 61.

Section 8 of PACE 1984 provides that a magistrate may issue a warrant authorising a police officer to enter and search premises if there are reasonable grounds for believing that[165]

(a) a serious arrestable offence has been committed;

(b) there is material on the premises specified in the application which is likely to be both of substantial value to the investigation of the offence and ultimately admissible as evidence, should there be a prosecution;

(c) the material is likely to be relevant evidence;

(d) the material does not consist of or include legally privileged items, excluded material or special procedure material; and

(e) it is not practicable to communicate with any person entitled to grant entry to the premises and/or access to the evidence; entry to the premises will not be granted unless a warrant is produced; or the purpose of a search may be frustrated or seriously prejudiced unless a law enforcement officer arriving at the premises can secure immediate entry to them.[166]

6.2.3.5 In search of an e-evidence strategy

6.2.3.5.1 Knock and announce

If, at the time the warrant is to be executed, the occupier[167] is present, the law enforcement officer must identify herself to the occupier. This should be done before entry, unless there are reasonable grounds to believe that to alert the occupier, or another person entitled to grant access, would frustrate the object of the search or endanger the officer concerned or any other person.[168] However, the officer should at the very earliest, after entry and before search, announce her identity, produce her authority and, at the first reasonable opportunity, give the occupier a copy of the search warrant.[169] Where a warrant has other documents attached, such as a schedule listing the items sought, the occupier is entitled to see the original or copies certified by the issuing judge of justice.[170]

---

165 Section 8(1) of the Police and Criminal Evidence Act of 1984.

166 Section 8(3) of PACE. These conditions are those limiting the use of warrants to the last resort principle. These are fairly stringent threshold requirements and it seems that their very stringency deters law enforcement from seeking a warrant when a search can be effected consensually or under sections 18 or 32 of PACE. See Sharpe *Search and Surveillance* 50.

167 If the occupier is not present, section 16(6) of PACE provides that the officer has the same obligation as regards some other person who appears to be in charge of the premises. In terms of section 16(7) the officer must leave a copy of the warrant in a prominent place on the premises in the absence of any person appearing to the officer to be in charge of the premises.

168 Paragraphs 6.4 and 6.5 of the PACE Code of Practice B. This was confirmed by the Court of Appeal in *R v Longman* [1998] 1 WLR 619 where the Court held that the police were justified in not revealing their identity or purpose prior to entry.

169 *R v Longman* [1998] 1 WLR 619, 626 and section 16(5) of PACE.

170 *R v Chief Constable of Lancashire ex parte Parker and McGrath* [1993] 2 All ER 56.

Normally a search warrant should be executed at a reasonable hour, but a search may take place at an unreasonable hour if the purpose of the search might otherwise be frustrated.[171] Reasonableness is to be determined by the nature of the business or domestic and the identity of the occupants, if any.[172]

The officer in charge of the search must first try to communicate with the occupier, or any other person entitled to grant access to the premises, explain the authority under which entry is sought and ask the occupier to allow entry, unless:

(a) the search premises are unoccupied;

(b) the occupier and any other person entitled to grant access are absent; and

(c) there are reasonable grounds for believing that alerting the occupier or any other person entitled to grant access would frustrate the object of the search or endanger officers or other people.[173]

6.2.3.5.2 Multiple warrants

Section 20 of PACE provides that the computer to be searched need not be situated in the premises entered physically, but must simply be accessible from them. The logistically problematic requirement for multiple warrants for multiple jurisdictions is therefore largely countenanced.[174] The so-called all premises warrant is also helpful in this context.[175]

6.2.3.5.3 Search and sift

In terms of section 16(8) of PACE, the search itself must be proportional to the purpose for which the warrant was issued.[176] The search and sift provisions contained in sections 50 to 70 of the Criminal Justice and Police Act[177] add significantly to the powers of search and seizure, in that they empower law enforcement officers to seize property from premises or persons so as to sift or examine the property elsewhere. The extent or complexity of a search might call for the

---

171 Section 16(4) of PACE.

172 Stone *The Law of Entry, Search, and Seizure* 110.

173 Paragraph 6.4 of the PACE of Code of Practice B.

174 See paragraph 6.2.3.1.1 above for a discussion of section 20 of PACE.

175 All premises warrants are referred to in footnote 106 in paragraph 6.2.3.1.1. above.

176 In the case of *Reynolds and Anor v Commissioner of Police of the Metropolis* [1985] 1 QB 881; [1984] 3 All ER 649, 80 Cr App Rep 125, it was stated that those searching under section 8 of PACE were not empowered to remove items to sift through them to see whether they fell within the scope of the warrant. Where a large number of documents are being sought, the temporary seizure and removal of all documents on the premises, in order to permit the police to sort them elsewhere, would be objectionable. The removal of files, rather than specific pieces of paper within the files, might be justified, if law enforcement reasonably believes that each file contains the material sought. It should be hard to justify the legitimacy of such conduct where a search is conducted under section 8 of PACE, since it is almost inevitable that, where material of such volume and complexity is involved, there is likely to be special procedure, excluded or even legally privileged material contained therein. Where a large quantity of material was involved, it was conceded that it might be impracticable to make a complete and final check of the materials seized whilst on the premises. Any item that was later discovered to be subject to legal privilege must be returned, but it was thought that the search itself would not, thereby, be invalidated. See Sharpe *Search and Surveillance* 64.

177 As further supplemented by paragraphs 7.7 to 7.13 of the PACE Code of Practice B.

consideration by the officer in charge of the search, of the deployment of seize and sift powers.[178] These provisions are also intended to address the situation where in the course of a search, a law enforcement officer encounters a large quantity of documentary material, some of which is likely to be relevant to the investigation and some of which is protected material. It might well be difficult, if not impossible, to determine quickly and on the spot which of the material is liable to seizure and which not. Similar problems arise in relation to material which is stored electronically, as it may take time to go through the contents of a hard disk or similar storage device to determine the relevance thereof.[179]

Stone[180] points out two situations where the search and sift provisions are likely to prove particularly useful. In investigations of fraud it may be difficult to determine at first sight which documents are relevant to the investigation or where some of the material may need to be extracted from the hard drive of a computer.[181] In investigations into pornography, where material may have been downloaded from the Internet or where exchanges were made by email, the deconstruction of the hard drive of one or more computers may be necessary to track down relevant material. If law enforcement officers aim the search and sift provisions at these sorts of situations and resist the temptation to use them for fishing expeditions, they will probably be found proportionate to the legitimate objectives of law enforcement. They are not, therefore, in principle, likely to lead to a breach of article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, but they might do so if they are used without proper discrimination.[182]

Section 50(1) of the Criminal Justice and Police Act adds to the powers of a law enforcement officer already lawfully on premises and equipped with a power to search.[183] The search and sift power is thus linked to the authorisation to search and relates to material which the person has reasonable grounds to believe may be or may contain something for which she is authorised to search. The power does not extend to items which a law enforcement officer would be justified in seizing if she happens to come across them in the course of a search for something else.[184] One of two further conditions must then be satisfied for the extended power of seizure under section 50(1) to arise. These two conditions are that it is not reasonably practicable,[185] in all the circumstances, to determine either whether what has been found is

---

178 Paragraph 6.3 of the PACE Code of Practice B.

179 Stone *The Law of Entry, Search, and Seizure* 149.

180 Stone *The Law of Entry, Search and Seizure* 155.

181 Such as the tracking of "deleted" emails. See paragraph 2.3.1 above for a reference to electronic evidence.

182 Stone *The Law of Entry, Search and Seizure* 156.

183 The person must also have one of the powers of seizure listed in Schedule 1 of, or the power set out in, section 50(2) to the Criminal Justice and Police Act. Schedule 1 contains an extensive list of over 70 powers under a wide range of statutes, including all the powers under Parts 3 and 4 of PACE.

184 As is allowed by section 19 of PACE. In this respect, section 50(1) is narrower than the power under section 50(2) of the Criminal Justice and Police Act.

185 The test to determine what is reasonably practicable in relation to the search and sift powers under both section 50(1) and 50(2) is dealt with in section 50(3) of the Criminal Justice and Police Act, which lists the factors to be taken into account. These factors include the length of time it would take to carry out a determination or separation on site; the number of people

something that the officer is entitled to seize, or whether the extent to which what has been found contains something that the officer is entitled to seize. If the above conditions are satisfied, then the power of seizure includes the power to seize so much of what it has been found necessary to remove from the premises to enable law enforcement to be determine whether it does constitute or include something which is liable to seizure.[186]

The power under section 50(1) does not extend to items which are reasonably believed to be legally privileged. It simply gives law enforcement officers the power to be able to remove and examine material which was not thought to be legally privileged but which might or might not otherwise be within the terms of the search power.

The search and sift power under section 50(2) of the Criminal Justice and Police Act arises where in the course of a lawful search the officer comes across something which she would be entitled to seize,[187] but for its being comprised in something else that she has no power to seize. It must also not be reasonably practicable in all circumstances to separate the seizable property on the spot. The most obvious situation where this applies is where the item or items subject to seizure is or are stored electronically on the hard drive of a computer,[188] but it can apply wherever disaggregation of the seizable from the non-seizable is impractical.[189]

Section 50(2) does give a power to seize material thought to be legally privileged, since the ban on such seizure is specifically disapplied.[190] Where items subject to legal privilege have been seized, there is a basic duty to restore items which appear to be subject to legal privilege to the person from whom they were seized.[191] This duty does not exist, however, where the legally privileged material cannot reasonably and practicably be separated from other property which either there is no obligation to return,[192] or there is a power to retain.[193] This power to retain legally privileged material exists when it is reasonably believed that the property was obtained though the commission of an offence, or that it is evidence of an offence (in either case, to stop it from being concealed, lost, altered or destroyed). Similar provisions govern the position of seized excluded or special procedure material.[194]

---

that would be required for the purpose; whether the process would involve damage to the property; what apparatus or equipment would need to be used; and in the case of separation, whether such separation would be likely to prejudice the use of the separated seizable property for a purpose for which it is capable of being used.

186 Stone *The Law of Entry, Search, and Seizure* 155.

187 Section 50(5) of the Criminal Justice and Police Act stipulates that the power of seizure must be one of those listed in Part 2 of Schedule 1 to the Criminal Justice and Police Act.

188 Particularly where the law enforcement officer suspects that documents may have been deleted from the hard drive, but are still recoverable. See paragraph 2.3.1 above.

189 Stone *The Law of Entry, Search, and Seizure* 151.

190 Section 50(4) of the Criminal Justice and Police Act, with reference to section 19(6) of PACE.

191 Section 54(1) of the Criminal Justice and Police Act.

192 Under sections 54 or 55 of the Criminal Justice and Police Act, which deal with excluded or special procedure material.

193 Under section 56 of the Criminal Justice and Police Act.

194 Section 55 of the Criminal Justice and Police Act. This provision is similar to section 54 in relation to legally privileged material. Note that for the purpose of section 55 in relation to all powers of seizure other than those specified in section 56(2) of the Criminal Justice and Police Act (which includes section 8(2) of PACE), special procedure material means such material in the form of documents or records.

These search and sift powers are limited and require law enforcement officers to be careful that they exercise them only when it is essential to do so and they do not remove more material than is necessary. The impact on a person's business of the removal of large volumes of material must be borne in mind and the officers should consider taking copies rather than originals.[195] Throughout the provisions, seizure is taken to include taking a copy of,[196] and various powers to obtain hard copy of material held in electronic form are treated as powers of seizure.[197] Officers must carefully consider whether removing copies or images of relevant material or data would be a satisfactory alternative to removing the originals. When originals are taken, officers must be prepared to facilitate the provision of copies or images for the owners when reasonably practicable.[198]

Where the seizure powers under section 50 have been deployed, there is an obligation to give the occupier of the premises a written notice setting out what has been seized and under what power, and giving information about the procedures for challenging the seizure.[199] The notice should specify the name and address of the person to whom notice of an application to the appropriate judicial authority in respect of any of the seized property must be given, and to whom an application may be made to allow attendance at the initial examination of the property.[200] Where the occupier is absent, the notice should be given to any person who appears to be in charge of the premises, or, failing that, the notice must be attached in a prominent place on the premises.[201]

Once property has been seized under section 50, there is an obligation on the law enforcement officer in possession of the seized property to examine the material to see whether its retention is justifiable.[202] Legally privileged, excluded or special procedure material which cannot be retained must be returned as soon as reasonably practicable without waiting for the whole examination.[203] This examination must take place as soon as is reasonably practicable, taking into account the desirability of allowing anyone from whom the property was seized, or with an

---

195 Paragraph 7.7 of the PACE Code of Practice B.

196 Section 63(1) of the Criminal Justice and Police Act.

197 Section 63(2) of the Criminal Justice and Police Act. Examples include sections 19(4) and 20 of PACE.

198 Paragraph 7.7 of the PACE Code of Practice B. Note 7C of the PACE Code of Practice B provides that officers should consider reaching an agreement with owners and/or other interested parties on the procedures for examining a specific set of property, rather than awaiting the judicial authority's determination. Agreement can sometimes give a quicker and more satisfactory route for all concerned and minimise costs and legal complexities. In *R v Leeds Magistrate's Court ex parte Dumbleton* [1993] Crim LR 866, the Court noted with approval that arrangements might be made for sorting processes to be carried out through the medium of solicitors. In this case, however, the documents being sought would all bear a particular letterhead or signature and the identification of them was obviously within the competence of the law enforcement officers carrying out the search.

199 Section 52 of the Criminal Justice and Police Act.

200 Paragraph 7.12 of the PACE Code of Practice B.

201 Section 52(2) or (3) of the Criminal Justice and Police Act and paragraph 7.13 of the PACE Code of Practice B.

202 Section 53(2) of the Criminal Justice and Police Act.

203 Paragraph 7.9B of the PACE Code of Practice B. Paragraph 7.10 further provides that when a law enforcement officer involved in the investigation has reasonable grounds to believe that a person with a relevant interest in property seized under section 50 or 51 intends to make an application under section 59 for the return of any legally privileged, special procedure or excluded material, the officer in charge of the investigation should be informed as soon as practicable and the material seized should be kept secure in accordance with section 61 of the Criminal Justice and Police Act.

interest in it, the opportunity of being present or represented at the examination.[204] Notification of the name and address of the person to be contacted in order to exercise the power to be present at the examination must be included in the notice given to the occupiers or left on the premises.[205]

All reasonable steps should be taken to accommodate an interested person's request to be present, provided the request is reasonable and subject to the need to prevent harm to, interference with, or unreasonable delay to the investigatory process. If an examination proceeds in the absence of an interested person who asked to attend or their representative, the law enforcement officer who exercised the relevant seizure power must give that person a written notice of why the examination was carried out in those circumstances. If it is necessary for security reasons or to maintain confidentiality, officers may exclude interested persons from decryption or other processes which facilitate the examination, but do not form part of it.[206] Until the examination is complete, the property should be kept separate and secure from anything seized under any other power.[207] Securing involves making sure the property is not examined, copied, imaged or put to any other use except at the request, or with the consent, of the applicant or in accordance with the directions of the appropriate judicial authority.[208]

Retention is justified if the property resorts within section 53(3) of the Criminal Justice and Police Act.[209] The retention of any material seized by a law enforcement officer is allowed, provided that one of two conditions is fulfilled.[210] These two conditions are that there are reasonable grounds for believing that the property is either property obtained in consequence of the commission of an offence, or evidence in relation to any offence. In either case it must be

---

204 Section 53(2) and (4) of the Criminal Justice and Police Act and paragraph 7.8 of the PACE Code of Practice B.

205 Under section 52 of the Criminal Justice and Police Act.

206 Paragraph 7.8A of the PACE Code of Practice B. See also Note 7D of the PACE Code of Practice B, which provides that a relevant interest in specific material may depend on the nature of that material and the circumstances in which it is seized. Anyone with a reasonable claim to ownership of the material and anyone entrusted with its safekeeping by the owner should be considered. It is interesting to note that the UK's National High-Tech Crime Unit ascribed to a generally applicable confidentiality charter. Business organisations have welcomed plans by the UK's National High-Tech Crime Unit to give guarantees of confidentiality to businesses when they report hacking, virus attacks and other computer crimes. The unit's confidentiality charter follows long-running concerns that businesses are failing to report computer crimes because they fear that bad publicity will damage both their reputation and their share price. In practice, however, experience has shown that fear of business disruption has been a greater deterrent to companies reporting computer crime than concerns about confidentiality. Goodwin 2002 *Computer Weekly* 2.

207 Section 53(2)(d) of the Criminal Justice and Police Act and paragraph 7.8 of the PACE Code of Practice B.

208 Note 7F of the PACE Code of Practice B stipulates that the mechanics of securing property vary according to the circumstances. The placing of material in sealed bags or containers (commonly referred to as "bagging up") and strict subsequent control of access is the appropriate procedure in many cases.

209 Section 53(3) includes property for which the person seizing it had the power to search, but is not required to be returned as legally privileged; or the retention of the property is authorised by section 56 of the Criminal Justice and Police Act; or it is property that cannot reasonably practically be separated from property falling within one of the first two categories.

210 Set out in section 56(2) and (3) of the Criminal Justice and Police Act. Section 56(5) specifically includes property seized by a person who was on the premises, in the company of a law enforcement officer, under the authority of a warrant under section 448 of the Companies Act of 1985; section 441 of the Companies (Northern Ireland) Order of 1986; section 199 of the Financial Services Act of 1998 (c 60); section 43 of the Banking Act of 1987 (c 22) or section 44A of the Insurance Companies Act of 1982 (c 50). Section 57 provides that a range of provisions, such as section 22 of PACE, which authorise the retention of property shall apply in relation to property seized under section 50 of the Criminal Justice and Police Act as if the property had been seized under the power of seizure by reference to which the power under that section was exercised in relation to that property. The provisions of sections 53 to 56 of the Criminal Justice and Police Act can, however, be used to justify retention where this would not be authorised by the relevant provisions.

necessary for it to be retained in order to prevent its being concealed, lost, damaged, altered or destroyed.

Seized material may also be retained to facilitate the use in any investigation or proceedings of anything to which it is inextricably linked. Inextricably linked material is material which cannot reasonably practicably be separated from other linked material without prejudicing the use of that other material in any investigation or proceedings. It may, for example, not be possible to separate items of data held on computer disk without damaging their evidential integrity. Inextricably linked material must not be examined, imaged, copied or used for any other purpose other than for proving the source and/or integrity of the linked material.[211]

Material in respect of which there is no power to retain must be separated from the rest of the seized property and must be returned as soon as reasonably practicable after examination of all the seized property.[212] Material must be returned to the person from whom it was seized, except when it is clear that some other person has better rights to it.[213]

Section 59 provides a power to challenge the retention of property that has been seized under section 50, any of the powers under Part 1 of Schedule 1 of the Criminal Justice and Police Act, or any statutory power exercised by a law enforcement officer.[214] The power to challenge retention is given to anyone with a relevant interest, including the person from whom property was seized, a person with an interest in the property, or a person who had custody or control immediately prior to the seizure.[215] The procedure for challenge is by application to the appropriate judicial authority.[216] The possible grounds for challenge are that

(a) there was no power to make the seizure;

(b) the seized property is or contains legally privileged, special procedure or excluded material; and

(c) the property does not fall within the provisions of section 56 of the Criminal Justice and Police Act.[217]

---

211 See note 7H of the PACE Code of Practice B.

212 Paragraph 7.9 of the PACE Code of Practice B. In terms of paragraph 7.9A, delay is only warranted if very clear and compelling reasons exist, for example, the unavailability of the person to whom the material is to be returned and the need to agree to a convenient time to return a large volume of material.

213 Section 58 of the Criminal Justice and Police Act. Paragraph 7.9C of the PACE Code of Practice B. Requirements to secure and return property apply equally to all copies, images or other material created because of the seizure of the original property.

214 Section 59(1) and (10) of the Criminal Justice and Police Act.

215 Section 59(11) of the Criminal Justice and Police Act.

216 As defined in section 64 of the Criminal Justice and Police Act. It will generally be a Crown Court judge, but, in relation or a power of seizure under section 448(3) of the Companies Act of 1985 or section 28(2) of the Competition Act of 1998, the application must be made to the High Court.

217 Section 59(3) of the Criminal Justice and Police Act.

The judicial authority is given extensive powers under section 59 to order the retention or return of some or all of the property or may give directions for the further examination or separation of any or all of it.[218] There are complex provisions dealing with the situation where the return of the property would be likely to lead to the immediate issue of a warrant for its seizure or an order for its production[219] or where the return of some parts of the material would result in such a warrant or order, but other parts would not.[220]

Failure to comply with the order of a Crown Court judge is to be treated as contempt of court.[221] Where an application is made under section 59 on the basis that the property is or includes legally privileged, special procedure, or excluded material, it generally imposes a duty on the investigating authority to secure the property.[222] This prevents its being examined, copied or put to any other use, other than with the consent of the applicant or the judicial authority.[223]

6.2.4 Search and seizure of e-evidence without a warrant

Section 17(5) of PACE stipulates that, with the exception of powers relating to breaches of the peace, all rules of common law under which a law enforcement officer has a power to enter premises without a warrant are abolished. Section 17 is essentially only concerned with powers of entry to arrest.[224] The common law power to enter and search premises following an arrest[225] survived the enactment of PACE, although it was effectively replaced by sections 18 and 19. The common law power to carry out a personal search[226] has also been superseded by section 32 of Police and Criminal Evidence Act.[227] Apart from the power to enter and search following an arrest, there were very few other powers of entry without warrant under the common law.[228]

In addition to searches incident to arrest, the following warrantless search doctrines are considered below: inventory searches, stop searches, exigent circumstances searches and plain view searches.

---

218 Section 59(5) of the Criminal Justice and Police Act.

219 The judge may authorize continued detention in terms of section 59(6) and (7) of the Criminal Justice and Police Act.

220 The judge may authorise the retention of all the material if the two parts cannot reasonably be separated. See section 59(8) of the Criminal Justice and Police Act.

221 Section 59(9) of the Criminal Justice and Police Act. Where the judicial authority is the High Court, failure to comply in any case constitutes contempt.

222 Pending the determination of the application. See sections 60 and 61 of the Criminal Justice and Police Act.

223 Section 61 of the Criminal Justice and Police Act. Note that there are exceptions to this in relation to inextricably linked property.

224 The precise scope of section 17 was considered by the House of Lords in *R (on the Application of Rottman) v Commissioner of Police for the Metropolis* [2002] UKHL 20; [2002] 2 All ER 865; [2002] 2 WLR 1315.

225 As recognised in, for example, *Ghani v Jones* [1970] 1 QB 693; [1969] 3 All ER 1700, CA.

226 The operation of the common law power to carry out a personal search in respect of persons detained by law enforcement following arrest can be seen in, for example, *Lindley v Rutter* [1981] QB 128 and *Brazil v Chief Constable of Surrey* [1983] 3 All ER 537, 77 Cr App Rep 237.

227 Stone *The Law of Entry, Search, and Seizure* 241.

228 Stone refers to two powers as illustrated in *Handcock v Baker* [1800] 2 Bos & P260 and *Thomas v Sawkins* [1935] 2 KB 249, both of which could be said to have been concerned with breaches of the peace. The first power has been given statutory form as far as the police is concerned by section 17(1)(g) of PACE. The latter power allows for a justified entry of premises on the basis of a reasonable anticipation of a fight or some other violent behaviour, as was the justification of the entries in *Lamb v Director of Public Prosecutions* [1990] Crim LR 58, 154 JP 381 and *McLeod v Commissioner of Police of the Metropolis* [1994] 4 All ER 553. See Stone *The Law of Entry, Search, and Seizure* 104.

6.2.4.1 Warrantless search and seizure doctrines

6.2.4.1.1 Searches incident to arrest

Very often the exercise of a law enforcement power of entry also involves carrying out a personal search of those found on the premises. Conversely, at times conducting a personal search provides the basis for seeking entry to premises. At least four different categories of personal search can be distilled from PACE, and the question of which category may be used in any particular situation depends primarily on the nature of the offence being investigated and the place where the search takes place. The four main categories of search are a superficial or basic search,[229] a non-public search,[230] a strip search[231] and an intimate search.[232] The two general powers of personal search[233] provided by PACE are searches immediately following arrest and searches during detention in police custody.[234] These two powers are considered below.[235]

Section 17 of PACE provides, *inter alia*, that a law enforcement officer may enter and search premises in order to execute a warrant for arrest or to make an arrest without a warrant for an arrestable offence. Provided that the law enforcement officer has reasonable grounds for

---

229 Stone argues that the word "superficial" is used in the sense of external or surface and not in the sense of cursory. See Stone *The Law of Entry, Search, and Seizure* 245. The word is used in paragraph 3.5 of the PACE Code of Practice A. There is in general no power to require a person to remove any clothing in public other than an outer coat, jacket or gloves. See also section 2(9) and 32(4) of PACE. The officer is permitted to do a rub-down search and feel for concealed items, to put her hand inside the pockets of the outer clothing or to feel round the inside of collars, socks and shoes, if reasonably necessary in the circumstances. It is assumed that this type of search also extends to the search of articles in the possession of the suspect, so that the officer may, for example, search a bag which was being carried.

230 This terminology is not used by the PACE Code of Practice A, but it is made clear that if a law enforcement officer wishes to conduct a search which goes beyond a superficial search, it must take place out of public view (see paragraph 3.6 of the PACE Code of Practice A). A search which goes beyond a superficial search may fall into the category of a strip search (as in the example given in paragraph 3.6 of the PACE Code of Practice A of a person who is asked to remove a T-shirt). A search which requires the removal of shoes, socks or headgear, although not a strip search, may also not take place in public.

231 A strip search is defined as one which involves the removal of more than outer clothing. Paragraph 11 of Annexure A to the PACE Code of Practice C sets out the procedures which should be followed in the conduct of strip searches. Although, as the name implies, a strip search may involve the removal of all clothing, this should be done in a way which does not mean that the person is at any time completely undressed. A strip search allows the visual inspection of bodily orifices.

232 The definition of an intimate search is contained in section 65 of PACE and means a search which consists of the physical examination of a person's body orifices other than the mouth. The exclusion of the mouth from the category of intimate searches was effected by section 59(1) of the Criminal Justice and Public Order Act of 1994. The conduct of such searches is regulated by section 55 of PACE and Annexure A to the PACE Code of Practice C.

233 These powers are general in the sense that their availability is not limited to a particular offence, although the manner in which they may be used may differ depending on the offence concerned. See Stone *The Law of Entry, Search, and Seizure* 254.

234 Paragraph 1.5 of the PACE Code of Practice A forbids, with one exception, searching persons with consent where there is no statutory power available. All searches, other than those falling within the exception, should take place on the basis of the relevant legal power and follow the provisions of the PACE Code of Practice A. The exception relates to the searching of those entering premises where consent to such a search is a condition of entry. This applies, for example, to routine security searches at airports or at the entrance to sports grounds. A personal search clearly has the potential to engage various articles of the European Convention of Human Rights and therefore to be open to challenge under the HRA. In particular, article 3 (inhuman or degrading treatment) and article 8 (respect for private life) may be relevant. The European Court of Human Rights has found, for example, that the regular and routine strip searching of a prisoner which included visual inspection of his rectum involved a breach of article 3 (*Lorse v The Netherlands* [2003] ECHR 59; (2003) 37 EHRR 3). In the United Kingdom, the House of Lords has held that there was no common law right of privacy which could be infringed by searching procedures (in this case visitors to a prison) even if those procedures went beyond what was laid down in regulations (*Wainwright v Home Ofiice* [2003] UKHL 53; [2003] 4 All ER 969). The statutory provision which gives law enforcement agencies a power of personal search will not generally specify the type of search which may be made, or place any limits on its extent. See Stone *The Law of Entry, Search, and Seizure* 243.

235 The power of a personal search during detention is discussed in paragraph 6.2.4.1.2 below.

believing that the person she is seeking is on the premises,[236] she may enter in order to execute an arrest. The premises searched could be the arrestee's own home, but that is not necessarily so.[237] This power to search is limited in the sense that the officer may only do whatever is reasonably required to ascertain whether her quarry is on the premises and she is not entitled to search for evidence.[238] Also, in relation to premises consisting of two or more separate dwellings, the power to enter and search are limited to any parts of the premises which are used in common by the occupiers of two or more dwellings and any dwelling in which the law enforcement officer has reasonable grounds for believing that the person whom she is seeking may be. An exception to this limitation is the power to enter and search premises for the purpose of saving life or limb, or preventing serious damage to property. There is also no requirement of reasonable belief here, so, presumably, all that is required is for the law enforcement officer's purpose genuinely to fall within the scope of section 17 of PACE.[239]

The powers to search premises after an arrest are found in sections 18 and 32 of PACE.[240] Section 32 arises where a person has been arrested anywhere other than at a police station. The arrest does not have to be for an arrestable offence within the definition contained in section 24 of PACE.[241] Where a law enforcement officer has reasonable grounds for believing that a person may present a danger to herself or to others, the officer may arrest the person.[242] The purpose of this search is clarified by an indication of the items which may be seized as a result of the search. Items that may be seized include anything which the officer has reasonable grounds for believing that the person might use to cause physical injury to herself or to another.[243] A law enforcement officer who arrests a suspect may also search such a suspect if the officer has reasonable grounds to suspect that the suspect has anything which might either be used to escape or might be evidence of an offence, even it that is not necessarily the offence for which the arrest was made.[244] The search should not extend beyond what is

---

236 Section 17(2)(a) of PACE.

237 For many years, law enforcement assumed that, if they arrested a person away from her home, they had the same right to search the arrested person's home as if she had been arrested there. This was confirmed in *Jeffrey v Black* [1978] 1 QB 490; [1978] 1 All ER 555, subject to the important qualification that the property which law enforcement hoped to find as a result of the search had to have some connection with the matter for which the arrestee had been detained. The facts of *Jeffrey v Black* provide a good example of when authorisation for a search would not be justified. Cannabis was found in the arrested person's lodgings when officers searched it without his consent and following his arrest for stealing a sandwich from a public house. The Divisional Court held that the search was unlawful because the officers could not have had a reason to suppose that it would yield evidence relating either to the theft for which the accused was under arrest or even to other offences of dishonesty. Precisely the same reasoning would apply under both sections 18 and 32 of PACE. The reasoning in *Jeffrey v Black* was doubted in *McLorie v Oxford* [1982] QB 1290, a case which suggested that, unless the arrest happened to take place at the arrestee's home, there was no power to search it against her will and without a warrant. Section 18 of PACE, broadly speaking, restores the position to what it was before *McLorie v Oxford*. See Stone *The Law of Entry, Search, and Seizure* 132.

238 Sprack *A Practical Approach to Criminal Procedure* 51.

239 Section 17(1)(g) of PACE. Stone *The Law of Entry, Search, and Seizure* 135.

240 Section 18 of PACE is directed at premises occupied or controlled by a person who has been arrested for an arrestable offence and is discussed in more detail below.

241 An arrest for a non-arrestable offence on the basis that the general arrest conditions, set out in section 25 of PACE, are satisfied, will potentially give rise to a right to search, as will an arrest under a specific power contained in a statute other than PACE. See footnote 28 in paragraph 6.2.1 above for examples of such specific statutory powers.

242 Section 32(1) of PACE.

243 Section 32(8) of PACE..

244 Section 32(2)(a) and (5) of PACE. In *R v Beckford* [1992] 94 Cr App R 43, the Court of Appeal accepted that, although the power of entry under section 32 is limited to seeking evidence of the offence for which the arrest has been made, it also

reasonably required to discover whether the arrestee has anything on her which might be so seized.[245] If, in making a search under either section 17 or 32, the officer discovers evidence of other offences, the officer may seize that too.[246]

There is a limitation on the extent of a body search.[247] The only type of personal search which may be carried out in public is a superficial search or a search of the arrested person's mouth.[248] If, however, the person can be removed from public view, there is, in theory, no limit to the type of search which can be used.[249] The degree of intrusion into personal autonomy is therefore limited and, traditionally, this has been a significant factor in upholding the reasonableness of warrantless searches.[250]

Section 32(7) is specifically aimed at a situation where the premises on which the arrest occurs consist of two or more separate dwellings. It limits the power to search to the dwelling in which the arrest took place or which the arrested person left immediately prior to her arrest and any parts of the premises which the occupiers of that dwelling use in common with the occupiers of other dwellings.[251] There is no time limit on the exercise of the power under section 32(2)(b), but it is designed principally to allow a search immediately after an arrest.[252]

Whereas section 32 of PACE is concerned with searches of the premises where an arrest occurred, section 18 applies to any premises occupied or controlled[253] by a person who has been arrested for an arrestable offence.[254] Supervision of the exercise of the power of search under section 18 is given to officers of the rank of inspector or above. Such an officer must authorise the search in writing. Section 18 authorises the search of premises, if the law

---

empowers law enforcement officers to enter premises which the suspect is known to have been in shortly before the arrest in order to search for evidence which might support or confirm the allegations against the suspect.

245 Section 32(3) of PACE.

246 Section 19 of PACE. See the discussion under the plain view doctrine in paragraph 6.2.4.1.5 below.

247 Section 32(4) of PACE.

248 Section 32(4) of PACE.

249 Where, for example, the arrested person is suspected of having concealed a stolen article, or drugs, inside her underwear, a strip search may be justified.

250 However, it should be remembered that, under section 19, an officer may seize anything that she has reasonable grounds to believe is evidence of or the fruits of an offence in order to prevent its destruction or alteration, except legally privileged material. Thus, once lawfully on premises under section 32, an officer may seize evidence of unrelated offending, so long as the search is limited to that reasonably required to discover items falling within the section (section 32(3) – this argument applies equally to the wider search power under section 18). Further, the section applies in respect of any offence, not simply an arrestable one. See Sharpe *Search and Surveillance* 35.

251 In *R v Beckford* [1992] 94 Cr App R 43, 49, the Court of Appeal held that, where premises consist of several separate flats, law enforcement is entitled to use their knowledge of the purposes for which one of the flats has been used in the past (i.e. dealing with drugs) to form an assumption as to which flat a person arrested (for possession of drugs) outside the building had just left.

252 In *R v Badham* [1987] Crim LR 202, a Crown Court refused to regard an attempted entry some four hours after an arrest as lawful under section 32. Although no time limit was given, this was an immediate power, and it would be wrong to have an open-ended right to go back to premises where an arrest had occurred. It is surely right that, in view of the width of this power, it should be used sparingly, and not as a means of circumventing the protective provisions attaching to searches under warrant. See Stone *The Law of Entry, Search, and Seizure* 128.

253 The concept of control is not defined, but it is likely that it would extend to the manager of premises and might even include security personnel such as a night watchman. See Sharpe *Search and Surveillance* 35.

254 The definition of an arrestable offence is contained in section 24 and Schedule 1 to PACE and the term denotes an offence for which an arrest may be made without a warrant. This rather cumbersome list was significantly extended by the Criminal Justice and Public Order Act of 1994 and the Offensive Weapons Act of 1996 and has been regularly added to subsequently. Examples of arrestable offences include, for example, offences for which the sentence is fixed by law (such as murder); offences for which a person over 21 may be sentenced on first conviction to five years' imprisonment; offences that can be tried either way under section 14(1) of the Wireless Telegraphy Act of 1949 and various other statutory specific offences.

enforcement officer has reasonable grounds for believing that there is evidence[255] on such premises that relates to the offence for which the person has been arrested, or any other arrestable offence connected with or similar to that offence.[256] Section 18 does not specifically require the authorising officer to be satisfied of the reasonable grounds for the applicant's belief.

As with section 32, the power may be used to search for excluded or special procedure material without using the Schedule 1 procedure.[257] The proportionality principle is applicable to these searches by virtue of section 18(3), which limits the power to search to the extent reasonably required to discover the evidence that the law enforcement officer believes to be there.[258]

Section 18 of Police and Criminal Evidence Act adds certain additional safeguards for the arrestee. The section enables an officer of at least the rank of inspector to give written authorisation for any premises occupied or controlled by a person under arrest for an arrestable offence to be searched by the investigating officers. In addition to a search of the arrestee's home, a search of her shop or other business premises might be authorised.[259] Authorisation may only be given if the inspector reasonably suspects that there is evidence on the premises relating either to the offence in respect of which the arrest was made, or to another connected or similar arrestable offence. Having authorised a search, the inspector should note her reasons and the nature of the evidence sought in the arrestee's custody record.

The only situation in which a section 18 search may be made without prior authorisation is when the arresting officer decides that it is appropriate to delay taking the arrestee to the station so that they can go together to the premises in question, with a view to carrying out the search in the arrestee's presence.[260] The officer should then inform the inspector of what has occurred as soon as practicable.[261]

6.2.4.1.2 Inventory searches

Searches of arrestees when brought to the police station are dealt with in section 54 of PACE. One of the custody officer's initial duties in respect of an arrestee brought to the police station is

---

255 Other than legally privileged items and not necessarily "relevant" evidence – see the discussion under the plain view exception in footnote 6.2.4.1.5 below.

256 Section 18(1) of PACE. The precise scope of the words "connected with or similar to that offence" awaits judicial interpretation. Stone argues that this would cover the situation where law enforcers are searching for evidence related to the theft of a car used in a robbery for which someone has been arrested, since the offences could be connected. Another example is where someone has been arrested for a burglary, and law enforcers wish to search for evidence of earlier burglaries which the arrestee may also have committed, since the offences here would be similar. Stone *The Law of Entry, Search, and Seizure* 132. In *Jeffrey v Black* [1978] QB 490; [1978] 1 All ER 555, it was held that the flat of a person arrested for stealing a sandwich may not be searched for drugs. See the reference to this case in footnote 237 in paragraph 6.2.4.1.1 above.

257 Stone *The Law of Entry, Search, and Seizure* 132.

258 Section 18(3) of PACE.

259 In *R v Badham* [1987] Crim LR 202, the Crown Court judge ruled that the authorisation should be in the form of an independent document which the officer could take with her to the premises to be searched.

260 Section 30(10) of PACE.

261 Sprack *A Practical Approach to Criminal Procedure* 52.

to record what the arrestee has with her. A search would normally be authorised to ascertain this. The extent of the search is in the custody officer's discretion. It may extend to a strip search, in which case the search must be carried out by an officer of the same sex.[262]

A strip search is not necessarily an intimate search (an intimate search is a search which consists of the physical examination of a person's body orifices other than the mouth[263]). Such searches should be subject to strict controls, because they might be used to humiliate or intimidate the subject. If inexpertly carried out, they could also cause physical harm. Although the custody officer is entitled to order a strip search to ascertain what an arrestee has with her, the officer may not sanction an intimate search.[264] Intimate searches must be authorised by an officer of at least the rank of inspector, but only if the officer reasonably believes that an arrestee in detention at the station has concealed on her either anything which she could and might use to cause physical injury to herself or others while in police detention or at court, or a Class A drug[265] which, prior to her arrest, she had in her possession for purposes of supply or illegal exportation. The search should not be authorised if the object of the search might be found by other means.[266]

6.2.4.1.3 Stop searches

Sections 1 to 3 of PACE provide law enforcement with a general power to detain a member of the public, without arresting her, for the purposes of carrying out a search of her person.[267] Although PACE Code of Practice A indicates that it governs the power to search a person without first arresting her, past law enforcement practice in the use of similar powers has been to stop and search where officers' suspicions about the proposed subject are too vague to amount to reasonable grounds for an arrest. The object of the search is to dispel or confirm

---

262 Nobody of the opposite sex (other than a doctor or nurse) may be present, nor may anybody whose presence is unnecessary be present. Annexure A to the PACE Code of Practice C defines a strip search as one involving more than the removal of outer clothing. See Sprack *A Practical Approach to Criminal Procedure* 51.

263 Section 65 and Code C, annexure A paragraph 1. See also footnotes 231 and 232 of paragraph 6.2.4.1.1 above for definitions of intimate and strip searches respectively.

264 Section 54(7) of PACE. Section 55 of PACE deals with intimate searches.

265 Class A drugs are the hard drugs such as cocaine, heroin et cetera. Cannabis is not considered a hard drug. If it is believed that the detainee might have a hard drug concealed on her body but that she is simply a user, as opposed to a supplier or exporter, of the drug, an intimate search should not be authorised.

266 For example, waiting for it to be passed through the natural bodily functions. This guideline may also become relevant in a scenario where authentication is established by means of biometrics.

267 Examples of specific stop and search powers include the following: stop and search of vehicles and pedestrians in terms of sections 43 and 44 of the Terrorism Act of 2000; stop and search for purposes of port and border controls under Schedule 7 of the Terrorism Act of 2000; stop and search in terms of the Poaching Prevention Act of 1862, section 6 of the Public Stores Act of 1875, section 47 of the Firearms Act of 1968, section 23 of the Misuse of Drugs Act of 1971, section 19 of the Wildlife and Countryside Act of 1981, section 27 of the Aviation Security Act of 1982, section 7 of the Sporting Events (Control of Alcohol, etc) Act of 1985, section 4 of the Crossbows Act of 1987, section 12 of the Deer Act of 1991, section 11 of the Protection of Badgers Act of 1992, section 60 of the Criminal Justice and Public Order Act of 1994. The latter section introduced a law enforcement power to stop vehicles or pedestrians and search for offensive weapons or dangerous instruments. Once such authority has been issued, it gives a law enforcement officer the right to make such a search as she sees fit, whether or not she has any reasonable grounds for suspecting that the person or vehicle is carrying weapons or articles of that kind. This is in stark contrast to the exercise of the power under section 1 of PACE, which is restricted to cases where the officer has reasonable grounds for suspecting that she will find stolen property or prohibited articles.

those vague suspicions. In the latter event, an arrest will no doubt follow.[268] A police officer may search a person or vehicle[269] if the officer has reasonable grounds[270] for suspecting that she will find stolen or prohibited articles.[271] Prohibited articles include offensive weapons and articles made or intended by the person carrying them for use in connection with burglary, theft, taking vehicles or obtaining property by deception or criminal damage.[272] The power to stop and search may be exercised only in a place to which members of the public have access.[273] The period for which a person may be detained is that necessary to carry out the search either at the place where the person was stopped or nearby.[274]

The most that the law enforcement officer carrying out the search can require the suspect to do in public is to remove an outer coat, jacket or gloves.[275] However, there is nothing to stop the officer from taking the person to a nearby van or police station, where a more thorough

---

268 Paragraph 1.4 of the PACE Code of Practice A. Sections 1 to 3 of PACE are among its most controversial provisions due to the room for abuse, as is acknowledged in the guidance given in the Stop and Search Code of Practice A of PACE. See, for example, paragraph 1.1. of the Code of Practice A that states that the powers are to be employed responsibly and without "unlawful discrimination" (for example, on grounds of race). See Sprack *A Practical Approach to Criminal Procedure* 45 and Sharpe *Search and Surveillance* 25 and 30, where reference is made to studies that revealed that there was an apparent racial bias in the selection of persons subject to stop and searches. It has been found that, overall, black people are five times more likely to be stopped than whites. Supervising officers should therefore consider whether there is any evidence that officers are exercising their discretion on the basis of stereotyped images of certain persons or grounds, particularly accruable to racial or ethnic bias. The procedural safeguards contained in sections 2 and 3 are stated to apply to all statutory powers to search persons and vehicles prior to arrest.

269 The permitted extent of a vehicle search is not set out in the PACE Code of Practice A. The general power to stop a vehicle derives from section 163(1) of the Road Traffic Act of 1988. This provides that a person driving a motor vehicle on a road must stop on being requested to do so by a law enforcement officer in uniform, but there is no attendant search power. The section is primarily aimed at facilitating requests to produce documents and details of identity following accidents and traffic violations. Section 23(2) of the Misuse of Drugs Act of 1971 provides similar powers to stop a vehicle on reasonable grounds that drugs may be found therein. All searches effected under PACE must be predicated by reasonable grounds to suspect that prohibited or stolen articles will be in the vehicle. Should a vehicle have been stopped under section 163 of the Road Traffic Act of 1988, it may be difficult for an officer to argue that it is reasonable to search the baggage in a car simply because the driver turns out to be disqualified from driving or to be driving without insurance. Sharpe opines that even if it could be argued, on the particular facts, that driving without required permits gives reasonable grounds to suspect that weapons of offence, stolen items or drugs may be present in the vehicle, an extreme measure such as ripping open upholstery or dismantling body work would probably be excessive and parallel to an intrusive or strip search of the person (Sharpe *Search and Surveillance* 25). Certain public protection searches are predicated on reasonable grounds for belief in respect of the factual situation that triggers the exercise of the power. This applies to the conduct of road checks under section 4 of PACE. The authorising officer must have reasonable grounds to believe that a serious arrestable offence has been, or is about to be, committed and that the person sought in connection with that offence is, or is about to be, in the locality in which vehicles would be stopped if the road check were authorised. Alternatively, there must be reasonable grounds to suspect that a person unlawfully at large is, or is about to be, in the locality. A road check permits an officer to stop all vehicles in the locality during the period of the power, or to stop vehicles selected by any criterion (section 4(2) of PACE). Section 4(1) of PACE provides that the purpose of the search is to ascertain whether a vehicle is carrying a person as described above, or a witness to a serious arrestable offence. See Sharpe *Search and Surveillance* 31.

270 Paragraph 2 of the PACE Code of Practice A gives guidance on what amounts to reasonable suspicion justifying a stop and search. The main point is that there must be a concrete basis in fact for the suspicion, as opposed to a mere hunch or instinct. Such a basis may be found in the nature of the property which the member of the public is seen or thought to be carrying, coupled with facts such as the time and place and her general behaviour. But reasonable suspicion can never be supported on the basis of personal factors alone without reliable supporting intelligence or information or some specific behaviour by the person concerned. For example, a person's race, age, appearance, or the fact that the person is known to have a previous conviction, cannot be used alone or in combination with each other as the reason for searching that person. Reasonable suspicion cannot be based on generalizations or stereotypical images of certain groups or categories of people as more likely to be involved in criminal activity. See also the discussion of reasonable grounds in paragraph 6.2.3.4 above.

271 Sections 1(2) and (3) of PACE. Prohibited articles are made, or adapted, or intended to use in the course of or in connection with specified offences, such as burglary and theft.

272 Section 1(7) to (9) of PACE.

273 Section 1(1) of PACE. Broadly speaking, this means any public place; any place to which the public, or a section thereof, have access by permission whether with or without payment and any place to which members of the public do in fact have regular access, even though they might not be entitled to go there. Within the last-mentioned category are car-parks, forecourts, the common parts of blocks of flats and even private yards or gardens adjoining the road. However, a person may not be stopped and searched in her own garden or yard; nor may somebody who is there by her permission. But, if a stranger jumps over the garden fence to hide behind a hedge, law enforcement has power to search her where she is. See Sprack *A Practical Approach to Criminal Procedure* 45.

274 Section 2(8) of PACE.

275 Section 2(9)(a) of PACE.

examination can take place, out of the public view.[276] Reasonable force may be used both for the purposes of detaining the person to be searched and then for actually searching her, but it should be employed as a last resort where the person is not willing to cooperate.[277] Every effort should be made to spare the person embarrassment and not to extend the search beyond what is strictly necessary. Before commencing the search, the officer must tell the person the officer's name and the name of the police station to which the officer is attached; the object of the proposed search; the grounds on which it is being made and the right of the person to have a copy of the record of the search.[278] If the officer is not in uniform, the officer must produce her warrant card.[279] Although the officer may also ask some preliminary questions, the person is not obliged to answer, nor is the officer entitled to detain her for the purpose of asking questions. However, if answers are forthcoming, they may dispel the suspicions which led to the original decision to stop and thus avoid the need for a search.[280]

Although a vehicle may be stopped in order to search it, this may only be done by a law enforcement officer in uniform.[281] Where an unattended vehicle is searched, a notice must be left on it, stating what has happened and giving information about the officer's contact details that would have been given to the driver in person had the driver been there.[282]

Law enforcement agencies are required to make adequate records as to the execution of the stop and search powers. The record must be made on the spot or as soon as is practicable after carrying out the search.[283]

6.2.4.1.4 Exigent circumstances

The power of law enforcement in the circumstances where implied consent is created by necessity now exists under section 17(1)(e) of PACE and is limited to saving life or limb or preventing serious damage to property. Generally, the results of searches and seizures on these bases are likely to be beneficial to the owner, and so disputes are unlikely. It is unlikely that the occupier is going to bring an action for trespass against a person who has entered the property with the sole purpose of preventing a crime being committed against the occupier or the occupier's family or property. To the extent that the power is based on preventing crime, the

---

276 Paragraph 3.6 of the PACE Code of Practice A.
277 Paragraph 3.2 of the PACE Code of Practice A.
278 Section 2(2) and (3) of PACE.
279 Paragraph 3.9 of the PACE Code of Practice A.
280 Section 2(1) and paragraphs 2.9 and 2.10 of the PACE Code of Practice A. If, as a result of questioning before a search, or other circumstances which come to the attention of the officer, there cease to be reasonable grounds for suspecting that an article of a kind is being carried for which there is a power to stop and search, no search may take place. In the absence of any other lawful power to detain, the person is free to leave at will and must be informed of that right.
281 Section 2(9)(b) of PACE.
282 Section 2(6) of PACE. See Sprack *A Practical Approach to Criminal Procedure* 46.
283 The record must give the name of the officer concerned and, if known, that of the arrestee, otherwise a description of her. The object, grounds, date, time and place of the search are all to be specified, together with what was found and details of any injury to a person or damage to property apparently caused. The person that was arrested is entitled, on request made within 12 months, to a copy of the record (section 3(7) and (9) of PACE). That might assist her, for example, in suing law enforcement if the search appears to have been unjustified or in making a complaint about their conduct.

question of the lawfulness of a warrantless search is likely to arise only where it is the occupier of property who is committing the offence.[284]

Although section 18 of PACE permits a search on arrest, there is no element of exigency and it may be conducted at any time after arrest. This is a considerable extension of a warrantless search power that is usually linked to urgency or exigent circumstances. The power may be challenged under article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, since there is no requirement of judicial scrutiny even in those circumstances where it would be feasible to obtain a warrant.[285]

Section 32 of PACE, by contrast, provides a power of search that is clearly based upon immediacy. It permits search upon arrest at a place other than at a police station. An officer may search the arrested person if the officer has reasonable grounds for believing that that person may present a danger to herself, the officer or others. The officer may also search for anything that might be used to assist the arrestee to escape from lawful custody or which might be evidence relating to an offence.[286] Section 32(2)(b) allows an officer to enter and search any premises in which the arrestee was when she was arrested or immediately before she was arrested for evidence relating to the offence for which she has been arrested.[287]

The section 32(2)(b) power is apparently more circumscribed than section 18 in that the search is restricted by requirements of urgency and particularity. There is some uncertainty about the meaning of the requirements of urgency and particularity, since the Act specifies no time limits. The Court of Appeal refused to interpret the immediacy requirement as making a section 32 search available only when or very soon after a person has been arrested.[288] Uncertainty as to the actual scope and application of section 32 renders it as liable to challenge on the basis of a lack of judicial authorisation as section 18 of PACE.[289]

The development of warrantless search powers in the United States has been constrained by the reasonableness requirement of the Fourth Amendment.[290] Whilst recognising a right to search both a person lawfully arrested and the place where the arrest is made, this right is an

---

284 Stone *The Law of Entry, Search, and Seizure* 10.

285 To this extent the pre-PACE case of *Mclorie v Oxford* [1982] 1 QB 1290 rejected the proposal that all such searches should be by warrant, holding that there was no common law power to enter and search a dwelling house several hours after the arrest of an occupier.

286 Section 32(1) and 32(2)(a) of PACE.

287 Sharpe *Search and Surveillance* 35.

288 In *R v Badham* [1987] Crim LR 202, the Crown Court considered that a delay of three to four hours prevented the police from searching under section 32 and that a proper authorisation under section 18 should have been obtained. However, in *R v Heap* 13 October 1994; see also *R v Beckford* [1992] 94 Cr App R 43, the Court of Appeal refused to interpret the immediacy requirement as making a section 32 search only "available at or very soon after a person has been arrested". Relying on editorial criticism of the *Badham* case, the Court rejected the notion that the powers under these two sections had to be used sequentially.

289 Sharpe *Search and Surveillance* 35.

290 See the discussion in paragraph 5.2.3.3 above.

incident of the arrest. A clear discernment is made between those circumstances where there is an opportunity to obtain a warrant and those of urgency and hot pursuit. Thus, a search of an accused's premises several blocks from the scene of the arrest and after all the accused were in custody elsewhere has been found to violate the Fourth Amendment. Sharpe[291] submits that this approach contrasts noticeably with the judicial interpretation of the provisions of PACE discussed above.

6.2.4.1.5 Plain view

Even prior to the enactment of PACE, the law has evolved to allow for the seizure of material other than that specified in the warrant.[292] The seizure of items not specified in the warrant was not ruled out, but such seizure was limited to prohibited goods or evidence of a grave offence. To this extent, evidence found incidentally in the course of a lawful search should be admissible. The manner of the search was to be determinative. If the law enforcement officers did not search appropriately under the warrant and fulfil their recording obligations, they could not rely upon the fruits thereof.

Section 19 of PACE goes further than the recommendations of the Royal Commission on Criminal Procedure. Although the manner in which the search is conducted may be crucial in considering whether material has been lawfully seized, the fact that the property has no relationship either to the crime being investigated or to the subject of the search is irrelevant. Nor is it relevant that there are no reasonable grounds to believe that the property is evidence of a serious crime. Section 19(1) provides that a law enforcement officer who is lawfully on the premises has certain powers of seizure. There is no requirement that the officer must be on the premises in order to execute a search warrant. It may be that the officer has been invited onto the premises and is there by consent. Whatever the basis of the lawful entry, an officer has a virtually unlimited power to seize any item where she has reasonable grounds for believing that the item has been obtained in consequence of the commission of an offence, or that it is evidence in relation to an offence which she is investigating or any other offence.[293]

Stone[294] accordingly argues that it is unfortunate that section 19 of PACE uses the word "evidence" rather than the phrase "relevant evidence". In section 8(4) "relevant evidence" in

---

291 Sharpe *Search and Surveillance* 35.

292 *Ghani v Jones* [1970] 1 QB 693; [1969] 3 All ER 1700 created an extension of seizure powers in respect of any material that was believed to implicate the subject of the search in other offending. This judicial endorsement of serendipity was motivated by the need to assist law enforcement in their efforts to track down criminals (at 1703). There is some uncertainty, however, whether *Ghani v Jones* had the effect of authorising the seizure of any items found, regardless of the level of suspected offending. The term "goods that show the suspect to be implicated in some other crime", is qualified. The law enforcement officers must have reasonable grounds for believing that a serious offence has been committed and that it is of the first importance that offenders be caught and brought to justice. The second requisite is that the officers have reasonable grounds for believing that the article in question is either the fruit of the crime, an instrument of the crime or evidence of the crime. The first two requisites would indicate that unless serious crime is reasonably believed to have taken place, the property cannot be removed. See Sharpe *Search and Surveillance* 61.

293 Section 19(2) and (3) of PACE. Sharpe *Search and Surveillance* 61.

294 Stone *The Law of Entry, Search, and Seizure* 122.

relation to an offence is defined for the purposes of the Act as anything which would be admissible in evidence at a trial for that particular offence. It is to be hoped that the word "evidence" in section 19 will be interpreted in the same way as section 8(4), but there is clearly a danger that a court might be persuaded that the omission of the qualifying adjective "relevant" was deliberate and that the word "evidence" should be given a wider meaning, perhaps closer to its popular use, rather than the technical concept of admissible evidence.

Sharpe[295] refers two caveats to what she terms a general licence to take away any suspect evidence. The first is that the law enforcement officer must have reasonable grounds to believe that it is necessary to seize the evidence in order to prevent its concealment, loss, damage, alteration or destruction.[296] A question arises as to whether this requirement precludes the seizure of items that can be photographed or copied by an officer under section 21(5) of PACE. A law enforcement officer may, however, consider in the light of the best evidence rule that it is preferable to retain the original material, which could be destroyed or defaced if not removed immediately. A police officer might well not consider herself qualified to judge whether the rule has been effectively eradicated by section 27 of the Criminal Justice Act of 1988, which provides for the reception in evidence of certified copies of documents, or merely confined in its application.

Sections 19(4) and 20 of PACE also allow an officer to require information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away. There is no longer any special requirement concerning the admissibility of computer-generated evidence. The provisions of the Criminal Justice Act of 1988 with regard to the reception of hearsay evidence in documentary form would still apply to much of this material before it would be relied upon in court.[297] A law enforcement officer is therefore not always in a position to judge whether seized material will be usable evidence, even if she reasonably

---

295 Sharpe *Search and Surveillance* 72.

296 Sharpe notes that the word "damage" does not appear in section 19(3), but opines that it is probably an error in drafting. Sharpe *Search and Surveillance* 72.

297 Section 69 of PACE has now been repealed by the Youth Justice and Criminal Evidence Act of 1999 section 60 which removes the additional admissibility conditions previously attaching to computer evidence. However, unless the evidence resulted from the purely automated function of a computer and involved no human input, it would still need to fall within one of the documentary exceptions to the hearsay rule. Sharpe *Search and Surveillance* 73. See also *R v Shephard* [1993] AC 380; 1 All ER 225; 93 Cr App Rep 139 and *DPP v McKeown and Jones* [1997] 1 All ER 225. It is interesting to note that it has been argued that section 69 should not have faced abolition due to the considerable clarification of section 60 provided by the House of Lords in the *Shephard* and *McKeown* cases. The so-called common law presumption of regularity now fills the void left by section 69 and some uncertainty surrounds the exact operation of this presumption in relation to computers. It is therefore unclear whether the common law presumption will make the use of computer evidence in criminal proceedings any less onerous than its statutory predecessor, particularly for the accused. As a result of the abolition of section 69, questions regarding the reliability of computer printouts should be challenged on the basis of the weight to be attached to the evidence rather than its admissibility. The consideration of the reliability of computer evidence has firmly been placed in the hands of the trier of fact. Without necessarily doubting the competence of juries and other triers of fact to evaluate complex computer evidence, in order to avoid injustice, some guidance will be necessary if the weight to be attached to this intricate evidence is to be left squarely with the tribunal of fact. See Quinn 2001 *International Journal of Evidence and Proof* 187. It is interesting to note that a "document" is defined in section 118 of PACE to mean anything in which information of any description is recorded.

believes that the seized material will be concealed or destroyed if not immediately removed, and the taking of copies is no guarantee that the evidence will subsequently be admitted at trial.[298]

The second caveat is that, under section 19(6) of PACE, the law enforcement officer may not seize an item that she has reasonable grounds for believing is subject to legal privilege. Another curious feature of section 19(6) is that it does not exclude from seizure special procedure or excluded material. The commonality between these concepts is the confidential nature of the information contained in the material sought. Such material is precluded from seizure under magisterial warrant under section 8(1)(d) of PACE, but not from seizure by a police officer.[299]

The concerns expressed over the use of search powers affecting innocent individuals and organisations have been addressed by means of the special procedure provisions contained in Schedule 1 of PACE and sections 9 and 10 that exempt legally privileged material from search.[300]

The substantial limitations on search powers contained in PACE have a curious loophole. Section 19 of PACE allows a law enforcement officer who is lawfully in the premises to seize any material found thereon if she has reasonable grounds for believing that it consists of the fruits of a crime and that it is necessary to seize it to prevent its concealment or destruction.

The only restriction in section 19(6) of PACE relates to items that an officer has reasonable grounds to believe are subject to legal privilege. The section allows a law enforcement officer to seize material outside the scope of a warrant and does not limit the right of seizure to serious offences. Section 19(6) therefore legitimates general searches once an officer has entered the premises by means of a warrant or by consent. The section does not accord with the views of the Royal Commission that, though it is not realistic to expect an officer to ignore items found incidentally in the course of a legal search, officers should only be allowed to seize fortuitously obtained material that is evidence of a grave offence. In this respect, PACE arguably grants wider powers of search and seizure than existed under the common law.[301] The search and sift power in terms of section 50(1) of PACE does not extend to items which a law enforcement officer would be justified in seizing if she happened to come across in the course of a search for

---

298 Sharpe *Search and Surveillance* 63.

299 Sharpe *Search and Surveillance* 63.

300 See the discussions of legally protected, excluded and special procedure material in paragraph 6.3.2 below.

301 See *Chic Fashions (West Wales) Ltd v Jones* [1968] 2 QB 299; [1968] 1 All ER 229 and *Ghani v Jones* [1970] 1 QB 693; [1969] 3 All ER 1700. Despite some incursion into the specificity limitation (*Wikes v Wood* (1763) 19 How St Tri 1153, 98 ER 489 and above) the right of seizure was limited to related or serious offences. Compare *Arizona v Hicks* 480 US 321 (1987) for a more restrictive approach; but note that the doctrine of "plain view" may legitimate the seizure of items not specified in the warrant where an officer is lawfully on the premises, see *Washington v Chisman* 455 US 1 (1982). Sharpe *Search and Surveillance* 6.

something else, as is allowed by section 19 of PACE.[302] In this respect the section 50(1) power is narrower than the power under section 50(2).

A similar distinction is made in the plain view doctrine applicable in the United States, as that under PACE, between search powers (which are constrained by the Fourth Amendment) and a power of seizure.[303] Section 19(6) of PACE grants the equivalent of general warrant powers to officers operating at street level, and it is surely inevitable that a challenge will be made under the Human Rights Act.[304]

6.2.4.1.6 Consensual

Consent to search and/or seize may be created by words or conduct, or both. Problems arising in respect of express verbal consent usually pitch on the evidential level of what exactly was said. If law enforcement wishes to search premises, written consent should be obtained.[305] Before seeking consent, the officer in charge of the search must state the purpose of the proposed search and its extent. This information must be as specific as possible, particularly regarding the items or person being sought and the parts of the premises to be searched. The person concerned must be clearly informed that she is not obliged to give consent and that anything seized may be used in evidence. If, at the time, the person is not suspected of an offence, the officer must explain the abovementioned when stating the purpose of the search.[306]

Consent may be implied in the absence of any indications to the contrary. It is well established that there is an implied licence to pass through an unlocked garden gate and walk up to the front door of a house if a person has or reasonably thinks she has legitimate business with the occupier[307] or with a member of the occupier's household.[308] The question whether this implied consent would cover entry to the common parts of a block of flats, or of a house divided into flats, is more complex and depends on the facts of each individual case.[309]

---

302 As is allowed by section 19 of PACE.

303 See paragraph 5.2.4.1.4 above for a discussion of the plain view doctrine under the law of the United States.

304 Sharpe *Search and Surveillance* 65.

305 Paragraph 5.1 of the PACE Code of Practice B. Sprack *A Practical Approach to Criminal Procedure* 52/3. In *Faulkner v Willetts* [1982] RTR 159; [1983] Crim LR 453, DC, the appellant's wife, having opened the door to a law enforcement officer and being told the reason for his visit, thereupon opened the door fully and she walked into the house. The Divisional Court held that this could be construed as an invitation for the officer to follow.

306 Paragraph 5.1 of the PACE Code of Practice B.

307 *Robson v Hallet* [1967] 2 QB 939; [1967] 2 All ER 407, 51 Cr App Rep 307; *Lambert v Roberts* [1981] 2 All ER 15, 72 Cr App Rep 223; *Baily v Wilson* [1968] Crim LR 617.

308 Stone *The Law of Entry, Search, and Seizure* 9.

309 In *Knox v Anderton* (1983) 76 Cr App R 156; [1983] Crim LR 114, DC, the Divisional Court found that the staircases and landings of a block of flats in a council housing estate were, in the absence of any restriction of access, a public place for the purposes of the Prevention of Crime Act of 1953. The staircase and landings were open to the atmosphere. In *Heads v Chief Constable of Humberside Police* 12 May 1986, DC, the block of flats had a door which was habitually open during the day but locked at night. The common parts were considered a public place for the purposes of the Public Order Act of 1936 at any time when the door happened to be open, including times when it was usually locked. Stone suggests that there should only be implied consent where it is necessary to go to the front door of a particular flat in order to attract the individual occupier's attention (that is where there are no bell pushes or other devices for this purpose at the main entrance). See also Stone *The Law of Entry, Search, and Seizure* 9. In *Rukwira v Director of Public Prosecutions* 158 JP 65; [1993] Crim LR 882, the entry to a block of flats was controlled by an entry phone system. Once through this, however, an entrant could gain access to landings outside a number of individual flats. The Court referred to the common parts as a means of access to the living

Any consent may take several forms and may be withdrawn at any stage. If the hostility to the other's entry is made clear at a sufficiently early stage, of course, it may operate to prevent a licence arising at all.[310] The question of whether express or implied consent has been withdrawn is more difficult and is a question of fact alone.[311] The occupier is well advised to make her wish to withdraw consent perfectly clear.

The owner in possession always has the power to grant or withdraw consent. In the absence of the owner, a party wishing to enter empty property has to rely on implied licence of some kind or seek out the owner or another person controlling the means of entry. A landlord or other owner of unoccupied premises is regarded as having possession of them for the purposes of granting consent to enter.[312] If the owner exercises her power to admit others to the premises there is little the licensee can do about it. If, for example, the owner of a boarding house gives law enforcement officers the necessary permission to enter a room, the officers are lawful entrants under the licence granted by the occupier, despite any objections from the person who is paying for the room. Equally, if the entry takes place in the licensee's absence, she has no grounds for complaints against the entrants, though she may have against the owner. This depends on the terms of her licence.[313]

Where the owner is absent and the property is unlawfully occupied by a third party, such as in the case of squatters, there is authority for saying that *de facto* possession is sufficient to entitle the possessor to undisturbed possession of the property as against all but the true owner.[314] In effect, the squatter seems to be in much the same position as a licensee in lawful occupation. As such, the squatter has the right to prevent anyone from entering the property, other than the owner, those acting on her instructions or those relying on a statutory power or warrant to enter.[315]

Difficulties arise where several parties have an interest in the property. As to lawful third party possession in the absence of the owner, the principal question is whether the third party has a

---

accommodation. The facts of the case do not reveal, however, how the law enforcement officers gained access to the common parts. If they were admitted in the normal way via the entry phone, then there would clearly be express consent to use the landings. If they entered in some other way, any consent would have been implied. The case is thus inconclusive, but it does not in any way contradict the suggestion put forward above by Stone that there would not normally be an implied licence in this situation to proceed beyond the front door of the block, which is under the control of the entry phone.

310 Examples would include where the front gate is kept locked or a notice reading "This is private property: you are trespassing" is displayed, as was the case in *Lambert v Roberts* [1981] 2 All ER 15, 72 CR App Rep 233, 19. This notice was considered enough to withdraw the consent, without there being a specific request to leave the premises.

311 *Snook v Mannion* [1982] RTR 321; [1982] Crim LR 601, DC.

312 *Jewish Maternity Society's Trustees v Garfinkle* (1926) 95 LJKB 766.

313 Sharpe *Search and Surveillance* 15. Note, however, that as far as the police are concerned, paragraph 5A of the PACE Code of Practice B states that in a lodging house or similar accommodation, every reasonable effort should be made to obtain the consent of the tenant, lodger or occupier. A search should not be made solely on the basis of the landlord's consent unless the tenant, lodger or occupier is unavailable and the matter is urgent.

314 *Graham v Peat* (1801) 1 East 244; 102 ER 95; *Nicholls v Ely Beet Sugar Factory* [1931] 2 Ch 84; [1931] All ER Rep 154. In *Scarborough Borough Council v Adams and Adams* [1983] JPL 673; (1983) 47 P & CR 133, DC, it was held that squatters could be occupiers for the purposes of the Town and Country Planning Act of 1971.

315 Stone *The Law of Entry, Search, and Seizure* 15.

right of exclusive occupation. If she does, she has the right to admit or exclude people from the property and the landlord has no right to interfere, unless there is damage to the reversion. This is typically the case with a tenant under a lease. The extent of any implied licence to enter a building leased by a number of tenants is unclear. In the absence of authority and in the interests of certainty, it has been recommended that the tenant should be endowed with authority over the common parts, if not as a result of the tenancy agreement, then under an implied authority from the landlord.[316] Where property is jointly owned, consent granted by one owner is sufficient, even if the other owner objects.[317]

Where premises are in single ownership, though multiple occupation, the owner of premises may expressly or impliedly delegate authority to allow others onto the premises to others who are in lawful occupation, for example, members of her family.[318] I n some circumstances, the owner is able to override an invitation given by a person with a lesser interest in the property.[319] A subtenant is in the same position as a tenant, provided she has exclusive possession. The requirement of exclusive possession places people such as lodgers, guests at hotels and boarding houses and servants in a much weaker position. It is not suggested that, if a hotel guest invites a friend back to her room, that friend is automatically a trespasser. Unless the owner or her manager has let it be known that such behaviour is unacceptable, the guest is taken to have an implied authority to bring in the friend.[320]

An objective test is applied to ascertain whether the person letting another into premises has the required implied authority to do so. The question is whether it is reasonable in all circumstances for the entrant to assume that the person granting the consent has the authority to do so.[321]

---

316 This would provide a workable solution for all cases except the unusual one where there was a conflict between two tenants as to whether the police should stay or go. In that situation it is suggested that the most workable solution would be for the licence to remain effective provided that at least one tenant wishes it to do so. Stone *The Law of Entry, Search, and Seizure* 12.

317 In *Slade v Guscott* (1981) 72 Cr App R 302, the Court of Appeal remarked that if one of two owners of a house, by her conduct, indicates that it is permissible for someone to come to that house, the fact that the other owner says it is not and the fact that the other owner tells a person to go away, may not be sufficient to remove the inference that there is an implied licence allowing the person to go at any rate as far as the door.

318 *Robson v Hallet* [1967] 2 QB 939; [1967] 2 All ER 407, 51 Cr App Rep 307; *Lambert v Roberts* [1981] 2 All ER 15, 72 Cr App Rep 223; *Jones & Jones v Lloyd* [1981] Crim LR 637.

319 In *R v Jones R v Smith* [1976] 3 All ER 54, 63 Cr App Rep 47, the Court found no consent for the son of the owner to enter the premises with a friend for the purposes of stealing from them. The owner of the property, however, does not always have the last word on the termination of consent. In *R v Thornley* (1981) 72 Cr App R 302; [1981] Crim LR 637, the Court of Appeal considered a domestic dispute between the wife of the owner and her husband. The Court ruled that the husband had no power to revoke the consent issued by his wife until the law enforcement officers had completed the investigation which she had requested them to make. The question as to in which situations the owner's wishes could be overridden in this way causes difficulties. Stone remarks that the *Thornley* decision ought to be applied restrictively and a different basis for legitimising law enforcement presence ought to be considered (such as the statutory right to enter to save life or limb, to effect an arrest or the common law power to prevent a breach of the peace). Stone *The Law of Entry, Search, and Seizure* 13. See *McLeod v Commissioner of Police of the Metropolis* [1994] 4 All ER 553; *McLeod v The United Kingdom* 24755/94 [1998] ECHR 92; (1999) 27 EHRR 493.

320 Stone *The Law of Entry, Search, and Seizure* 13.

321 Paragraph 5.1 of the PACE Code of Practice B requires an officer to make any necessary inquiries to be satisfied that the person is in a position to give such consent.

Consent must be freely given. Where there is some doubt about the capacity of an individual to give informed consent, whether through mental handicap, disorder, or otherwise, that person should not be subjected to a voluntary search. If an officer acts in an improper manner, this vitiates consent. Consent is, in reality, likely to be no more than co-operation. Article 8 of the European Convention of Human Rights can be relied upon where it is alleged that informed consent has not been truly given and that there was no reasonable basis for the search. [322]

In the context of searches of the person, the cooperation of the person to be searched must be sought in every case, even if the person initially objects to the search. A forcible search may be made only if it has been established that the person is unwilling to cooperate or resists.[323] An officer must not search a person, even with her consent, where no power to search is applicable.[324] Interestingly, specific provision is made for when an officer makes an electronic record of the scope of the search and is unable to produce a copy of the form at the time. The officer is then required to explain how the person can obtain a full copy of the record of the stop or search and give the person a receipt which contains a unique reference number and guidance on how to obtain a full copy of the stop or search, the name of the officer who carried out the stop or search and the power used to stop and search her.[325]

6.3 *Production devices*

6.3.1 *Background*

In deference to the concerns of various groups of professional and business people, who felt that their relationship with clients would be jeopardised if they could be forced to surrender to law enforcement agencies material that had been entrusted to them in confidence, PACE was passed with complicated safeguards to protect three classes of material, namely legally privileged material, special procedure material and excluded material.[326] Access to special procedure and excluded material may normally be obtained by means of a production order issued in terms of Schedule 1 of PACE.[327]

---

322 Sharpe *Search and Surveillance* 20.

323 Paragraph 3.2 of the PACE Code of Practice A.

324 Paragraph 1.5 of the PACE Code of Practice A. The only exception, where an officer does not require a specific search power, applies to searches of persons entering sports grounds or other premises carried out with their consent given as a condition of entry.

325 Paragraph 4.10A of the PACE Code of Practice A.

326 Sprack *A Practical Approach to Criminal Procedure* 48.

327 A number of specific access or production devices also exist in English Law. An example can be found in paragraph 5 to Schedule 5 of the Terrorism Act of 2000, which allows for the application to a circuit judge for a production order in respect of excluded or special procedure material. The order will direct the person who appears to the judge to be in possession of the material to produce it to a law enforcement officer within a specified period, to give the constable access to it within such a period, or to state to the best of her knowledge or belief the location of the material, if it is not in and will not come into her possession within such a period. Where the order is to give access to the material, the order may also direct any person entitled to grant entry to premises where the material is situated to allow an officer to enter for the purposes of access to it. If the order relates to material which is expected to come into existence, or to become available to the person specified, within 28 days of its issue, the order will require the person to notify a named constable as soon as the material comes into existence, or becomes available in terms of paragraph 7 of Schedule 5. Material held on a computer must be produced in a form which is visible and legible and if the order is for production rather than access, in a form in which it can be taken away

Chapter II of Part I of the Regulation of Investigatory Powers Act provides a legislative framework to cover the requisition, provision and handling of communications data.[328] The framework clarifies the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, reflecting the requirements of article 8 of the European Convention of Human Rights.[329] Access to communications data may be obtained by means of authorisations and notices issued in terms of section 22 of RIPA. Section 49 of RIPA also specifically introduces a power to require the disclosure of protected data.[330] Since RIPA has come into force, various supporting regulations have also been enacted in the form of statutory instruments.[331] The Data Protection Act,[332] which establishes a separate statutory

---

(paragraph 8(2)). Material produced will be subject to the access and copying provisions of sections 21 and 22 of PACE. Failure to comply with a production order under paragraph 5 will mean that a circuit judge may, on application by a constable, issue a warrant to search for the material in terms of paragraph 12 of Schedule 5. In addition, a warrant may be issued if the judge is satisfied that there are reasonable grounds for believing that the conditions for the issue of an order under paragraph 5 have been met, but that it is not practicable to communicate with the person entitled to produce the material, or it is not practicable to communicate with any person entitled to grant entry to the relevant premises, or access to the material, or that the investigation might be seriously prejudiced if a law enforcement officer could not obtain immediate access to the material. Other examples include section 157 of the Extradition Act of 2003, which provides for the issue of a production order by a circuit judge, requiring the person in possession of the required material to produce or give access to it; section 2 of the Criminal Justice Act of 1988 empowers the Director of the Serious Fraud Office to demand the production of information relevant to an investigation under her auspices. Interestingly, section 55 of the Drug Trafficking Act of 1994, which directs a person in possession of sought after material either to produce it to a law enforcement officer or to give an officer access to it, does not include a power of search, but simply allows a law enforcement officer to take possession of the material specified in the order. Whilst these specific production devices do not resort within the research parameters of this thesis, the general powers of production in terms of Schedule 1 of PACE and the production devices aimed at communications data are explored. The Inland Revenue Services are also empowered with an array of production orders. Examples include production orders in terms of section 20BA and Schedule 1AA of the Taxes Management Act of 1970 added by the Finance Act of 2000. Where information reasonably believed to be evidence is held in an electronic form, and is accessible from the premises being searched, the power of seizure include the power to require information to be reproduced in a form in which it is visible, legible and can be taken away (section 20C(3A)). The seize and sift provisions of section 50 of the Criminal Justice and Police Act of 2001 apply to section 20C of the Taxes Management Act of 1970, so that items may be removed for examination to see whether they constitute relevant evidence. It had in any case been held that it was legitimate under section 20C to seize an entire computer, even though its hard disk might contain irrelevant material, because the computer itself was a "thing" falling under section 20C(3)(b). See *R (On Application of H) v Inland Revenue Commissioners* [2002] EWHC 2164 (Admin). See also *R (on application of Paul Da Costa & Co) v Thames Magistrate's Court* [2002] EWHC 40 (Admin); [2002] BTC 5605, where, in considering powers of search in relation to VAT, it was held that it was permissible to take an image of an entire hard disk, without examining the contents in detail. Section 118D of the Customs and Excise Management Act of 1979 provide a procedure for an officer to obtain an order from a justice of the peace, giving access to recorded information. In respect of information stored in electronic form, a provision similar to section 19(4) of PACE is also provided, to the effect of such information to be produced in a visible and legible form and if the officer wishes, in a form in which it can be removed.

328 It is only relevant to communications data held by a communications service provider and not to personal contact details or records of communications held by an employer or other person. If such data is relevant to an investigation, it could be obtained using the traditional means. See "Evidence That May Assist in Your Investigation" found on the Internet http://www.hse.gov.uk/enforce/enforcementguide/investigation/physical/evidence.htm 2.

329 See the UK Home Office "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 156.

330 See the UK Home Office "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 12.

331 JISC Legal Information Service (2002) "E-Security Encryption and the Law – Overview" found on the Internet http://www.jisclegal.ac.uk/esecurity/escurity.htm 3.

332 Of 1998. The Data Protection Act was designed to implement the EC Data Protection Directive 95/46. EC Directive 2002/58EC translates the principles set out in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, into specific rules for the electronic communications sector. Articles 5, 6 and 9 of Directive 2002/58/EC define the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when it is no longer needed for the purposes of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value added services. Article 15(1) of Directive 2002/58/EC sets out the conditions under which member states may restrict the scope of the right and obligations provided for in articles 5, 6, 8(1)(2)(3) and (4), and article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, in other words to safeguard national security defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems. Article 15(1) does not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks.

regime governing the processing of personal data,[333] must also be borne in mind. Law enforcement agencies may accordingly garner information from commercial bodies such as telephone companies and utility companies, or from public bodies such as local health authorities.[334] The only restrictions on the acquisition of this information are the restrictions contained in PACE concerning special procedure and excluded material. Data protection in the European Union is regulated under Directive 94/46/EC and Directive 2002/58/EC.[335]

6.3.2 *Information categories*

6.3.2.1 Legally privileged material

Generally power of seizure in terms of section 19 of PACE power of seizure is slightly wider than the power under the common law, but in one respect it is more restricted. Items which a law enforcement officer has reasonable grounds for suspecting to be subject to legal privilege may never be seized, whatever the basis of the law enforcement officer's presence.[336] Presumably reasonable grounds require more than a mere statement by the owner that the items are subject to legal privilege and the officer may well be entitled to inspect the documents to a limited extent in order to ascertain their character.[337] In any case, law enforcement also have available the power of seizure conferred by section 50 of the Criminal Justice and Police Act 2001, which empowers the removal of items for more detailed inspection.

Legally privileged information is defined in section 10 of PACE. Privilege attaches essentially to any communication[338] between a professional legal advisor and her client, made in connection

---

333 Data controllers have a duty to comply with eight data protection principles in respect of personal data, namely: personal data must be fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; not kept for longer than necessary; processed in accordance with the data subject's rights; and kept secure. See Blanpain *The Impact of the Internet and New Technologies on the Workplace* 196. Under section 7(1)(a) of the Data Protection Act, there is a presumptive right of access to personal data. An individual is entitled to "be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller". This presumptive right is, however, subject to, *inter alia*, the exemptions provided for in sections 28 and 29 of the Data Protection Act. Section 28 deals with exemptions "required for the purpose of safeguarding national security". Section 29 deals with data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature.

334 Sharpe *Search and Surveillance* 220.

335 Privacy International "Silenced – Europe Profile" found on the Internet http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-103799 3-6.

336 Section 19(6) of PACE. This seems more restrictive than the approach to this issue adopted by Swanwick J in *Frank Truman Export Ltd v Metropolitan Police Commissioner* [1977] QB 952; [1977] 3 All ER 431, 64 Cr App Rep 248, since items which are evidence of an offence may still be protected by the privilege.

337 *AM & S Europe Ltd v Commission of the European Communities* [1983] QB 878.

338 Such communications will typically be documents. Stone opines that there is no reason why communications should not include letters, emails, faxes, telefaxes, other typed, printed, or handwritten communications, recordings of conversations or telephone calls or copies and transcripts thereof. See Stone *The Law of Entry, Search, and Seizure* 115. Non-documentary evidence may also be the subject of legal privilege. In *R v R* [1994] 4 All ER 260; [1995] 1 Cr App Rep 183, 265, the defendant provided a blood sample for scientific analysis to his general practitioner, on advice of his solicitors. The scientist who carried out the analysis was subpoenaed by the prosecution and her evidence admitted. The Court of Appeal held that the blood sample fell within section 10(1)(c) of PACE as a legally privileged item, made for the purposes of legal proceedings, and should not have been admitted. A similar view was taken in *R v Davies (Keith)* [2002] EWCA Crim 85 in respect of the opinion of a psychiatrist whom the defence had instructed but not called. See also Pattenden 2000 *International Journal of Evidence and Proof* 213-245 for an examination of two areas of uncertainty of litigation privilege that have not attracted the attention that they deserve: the extent to which the opinion of an expert and evidence connected with such an opinion are protected by litigation privilege and the rationale for litigation privilege.

with the giving of legal advice;[339] communications between a legal advisor or a client and a third party made in contemplation of legal proceedings and items enclosed with such communications.[340]

Items held with the purpose of furthering a criminal purpose cannot enjoy legal privilege.[341] Where the police seek material which is *prima facie* covered by legal privilege, it is rare for the judge to issue a blanket order granting a search warrant in respect of wide categories of documents held by a firm of solicitors.[342]

Even if the legal privilege is lost, it does not mean that the material sought is not protected by confidentiality, as such material may nonetheless be held in confidence under an express or implied undertaking and thus be special procedure material.[343] Material cannot be regarded as special procedure material where the material sought is criminal in itself.

---

339 Straightforward records of transactions, such as conveyancing documents, are not covered in this study, as these documents are not related to the giving of legal advice or legal proceedings. See *R v Crown Court at Inner London Sessions ex parte Baines & Baines (a firm)* [1988] 1 QB 579; [1987] 3 All ER 1025, 57 Cr App Rep 111 and *R v Central Criminal Court, ex parte Francis & Francis (a firm)* [1988] 1 All ER 677, 87 Cr App Rep 104, 679.

340 When an application under section 9 of PACE is made against a solicitor, the notice of application will invariably refer to the files of named clients. The right to privilege belongs to the client, not to the solicitor. If a client is not prepared to give instructions to oppose or to provide the solicitor with reasonable sums on account, the solicitor is under no obligation to oppose the application. Hiley 1987 *Law Society's Guardian Gazette* 3090.

341 The scope of this limitation on legal privilege where the solicitor is in possession of material relevant to the investigation of a third party has been considered in two conflicting decisions, leaving the scope of application of section 10 of PACE uncertain. In *R v Crown Court at Snaresbrook ex parte DPP* [1988] 1 All ER 315, where the item in question was a legal aid application in the possession of the local law society, the Divisional Court ruled that the intention in section 10(2) of PACE must be the intention of the person holding the material. A different view was taken in *Francis & Francis (a firm) v Central Criminal Court* [1988] 3 All ER 775, 88 Cr App Rep 213, where the items sought were correspondence and attendance notes held by a firm of solicitors relating to property transactions undertaken by one of their clients. The funds for these transactions were suspected to be provided by one of the client's relatives out of the proceeds of drug trafficking. The House of Lords upheld the Divisional Court's view that, although the solicitors holding the information had no criminal intention, the purposes of the client's relative were sufficient to bring section 10(2) of PACE into operation. Communications criminal in themselves or intended to further any criminal purpose are not privileged. Stone argues that this decision has a severely limiting effect on legal privilege in that in any case where law enforcement is searching for items which constitute evidence of an offence, they will normally be able to show that someone has a criminal purpose in relation to those items. The danger is that section 10 could be rendered redundant, which cannot have been Parliament's intention. The precise scope of section 10 is uncertain. Stone *The Law of Entry, Search, and Seizure* 116. It should, however, be remembered that even if legal privilege is lost, material held by a solicitor on behalf of a client will almost certainly constitute either excluded or special procedure material and thus have some protection from seizure.

342 In certain circumstances, however, such a blanket order may be proper, as in *Leeds v Crown Court ex parte Switalski* [1991] Crim LR 559, where the Divisional Court upheld the circuit judge in the granting of such a blanket order. The firms in question were subjects of an enquiry into fraud on the legal aid fund and conspiracy to pervert the course of justice. In *R v Southampton Crown Court ex parte J and P* [1993] Crim LR 962, the Divisional Court emphasized the need, even where solicitors themselves are under investigation, to be cautious in this area. The judge to whom an application for an order or warrant granting access to a solicitor's files was made should seek the fullest possible information with a view to excluding from any order or warrant any material which could be said to be protected by section 10 of PACE (at 964). In *R v Leeds Magistrate's Court ex parte Dumbleton* [1993] Crim LR 866, the applicant, a solicitor, was suspected of having forged documents to try to indicate that the debtor company had an interest in certain assets. The Court held that the forged material could not be said to be legally privileged, because the protection afforded to documents made in connection with legal proceedings under section 10 of PACE only applied to documents lawfully made and could not apply to forgeries. The forged documents were also not special procedure material, as forged documents could not be said to have been produced in the course of the profession of a solicitor. A criminal can therefore not gain protection from search by depositing forged documents with her solicitor. In *R v Justice of the Peace for Peterborough ex parte Hicks* [1978] 1 All ER 225, it was held that the solicitor cannot assert a greater authority than the client herself possesses in respect of the seizure of such forged documents.

343 *R v Guildhall Magistrate's Court ex parte Primlaks Holdings Co. (Panama) Inc* [1990] 1 QB 261. See, for example, also *R v Maidstone Crown Court ex parte Rogers* [1999] 1 WLR 832, where the record of time of attendance of a client has been held as special procedure material, but not subject to legal professional privilege.

6.3.2.2 Excluded material

Excluded material is narrowly defined in section 11 of PACE. There are three types of excluded material, namely personal records, human tissue or tissue fluid[344] and journalistic material. Journalistic material must consist of documents or records and must be material acquired or created for the purposes of journalism. It must also be in the possession of a person who acquired or created it for the purposes of journalism if it is to attract protection.[345] Journalistic material must have been held in confidence continuously, by one or more persons, ever since it was first acquired or created for the purposes of journalism, to be considered excluded material.[346]

For personal records to qualify as excluded material, they must be held in confidence by a person who acquired or created them in the course of a trade, business, profession or other occupation or for the purposes of a paid or unpaid office.[347] Records are held in confidence if they are subject to an express or implied undertaking to that effect, or to a statutory restriction or obligation of secrecy.[348] Personal records means records concerning a living or dead individual from which she may be identified. Such personal records must relate to the person's physical or mental health, spiritual counselling or advice given or to be given to her, or counselling or assistance given or to be given to her, for the purposes of her personal welfare. Such information may be divulged by a voluntary organisation, or an individual who, because of her office or occupation, has responsibilities for the person's welfare, or who is responsible for supervising the person under a court order.

Typical examples of such excluded material would be medical records, records of spiritual counselling, some educational records and files kept on their clients by social workers, probation officers, members of the clergy and voluntary organisations.

---

344 In terms of section 11(1)(b) such human tissue or tissue fluid must have been taken for the purposes of diagnosis or medical treatment and must be held in confidence.

345 Section 13(2) of PACE. Stone argues that the reporter who deposits her journalistic material with a friend for safekeeping may thus achieve the opposite of her aim. Stone *The Law of Entry, Search, and Seizure* 119.

346 An example would be a document covered by the Official Secrets Act of 1989 which had been leaked by a civil servant to a journalist. Stone *The Law of Entry, Search and Seizure* 119. In *British Steel Corporation v Granada Television Ltd* [1981] AC 1096, 1171, the concept of journalistic immunity , prohibiting the right to compel disclosure of sources, was rejected as placing journalists in a favoured position as compared with priest-confessors, doctors, bankers and other recipients of confidential information. Section 10 of the Contempt of Court Act 1981 attempted to address the disquiet caused by this apparent rejection of confidentiality. It provides that no person may be required to disclose the source of information contained in a publication for which she is responsible unless such disclosure is necessary in the interests of justice, national security or for the prevention of disorder or crime. In *Goodwin v The United Kingdom* 17488/90 [1996] ECHR 16; (1996) EHRR 123, the Court ruled that these three exceptions are not to be given a wide interpretation.

347 Section 11(1)(a) of PACE.

348 See section 11(2) of PACE. An example of a statutory obligation of secrecy can be found under the Official Secrets Act of 1989.

6.3.2.3 Special procedure material

Special procedure material is defined in section 14 of PACE. This is a wider category than excluded material, covering anything that a person acquired in the course of her trade, business or employment and which she holds subject to an express or implied undertaking or statutory obligation to keep confidential.[349] This category also covers all journalistic material which is not excluded material acquired and continuously held in confidence.

Material acquired by an employee from her employer in the course of her employment or by a company from an associated company,[350] is only special procedure material if it was such material immediately before its acquisition.[351] The special procedure status can accordingly not be gained for otherwise unprotected material simply by extracting an undertaking of confidentiality from an employee to whom it is transferred. Material created by an employee in the course of employment is also only special procedure material if it would have been that if the employer had created it.[352]

Examples of special procedure material include business records held by banks, building societies, clubs, local societies, voluntary groups, youth associations; photographs held by newspapers; and conveyancing documents in the possession of a solicitor.[353]

6.3.2.4 Communications data

Communications data essentially includes information relating to the use of a communications service but excludes the contents of the communication itself.[354] Communications data[355] is defined in section 21(4) of RIPA as any of the following

(a) any traffic data comprised in or attached to a communication, whether by the sender or otherwise, for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted;[356]

---

349 Section 14(1) and (2) of PACE.

350 In terms of section 14(6) of PACE, a company will resort into the category of an associated company if it would be so treated for the purposes of the Income and Corporation Taxes Act of 1970.

351 Section 14(3) of PACE.

352 Section 14(4) and (5) of PACE.

353 Stone *The Law of Entry, Search, and Seizure* 120.

354 See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 160.

355 Related communications data has a corresponding meaning and is defined in section 20 of the Regulation of Investigatory Powers Act (RIPA). Related communications data, in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunications system, means so much of any communications data (as defined in paragraph 6.3.2.4 above and within the meaning accrued to it in Chapter 2 of RIPA) as is obtained by, or in connection with, the interception and relates to the communication or to the sender or recipient, or intended recipient, of the communication.

356 This definition of traffic data also resounds in section 2(5) of RIPA. Section 2(5) excludes from the definition of interception in section 2(2) of RIPA any conduct which relates only to the traffic data comprised in or attached to a communication (expanded on in section 2(9), which is similar to section 21(6) of RIPA), or which relates only to so much of the content of the

(b) any information which includes none of the contents of a communication, apart from any information falling within the definition of traffic data as detailed in paragraph (a) above and is about the use made by any person of either any postal service or telecommunications service, or in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunications system; and

(c) any information not falling within paragraphs (a) or (b) that is held or obtained, in relation to persons to whom she provides the service, by a person providing a postal service or telecommunications service.

6.3.2.5 Traffic data

Traffic data is defined in section 21(6) of RIPA to mean the following in relation to any communication: [357]

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from whom or which the communication is or may be transmitted,[358]

(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;[359]

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting, in whole or in part, the transmission of any communication;[360] and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication.[361]

The tailpiece of section 21(6) of RIPA provides that this definition of traffic data includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored. This definition of traffic data puts beyond doubt that in

---

communication as is necessary in order to identify this traffic data. Traffic data is further circumscribed in section 21(6) of RIPA. See paragraph 6.3.2.5 below.

357 For the purposes of section 21(6) of RIPA. This definition of traffic data is precisely the same as the definition provided in section 2(9) of RIPA.

358 This is described as subscriber information in the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 33. These explanatory notes have been prepared by the Home Office in order to assist in understanding RIPA and have not been endorsed by Parliament.

359 This is described as routing information in the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 33.

360 To be read with section 21(7), in much the same way as section 2(9)(c) is to be read with section 2(10), which operates on section 2(5), as explained in the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 33. It addresses what is commonly referred to as "dial through fraud" and covers, for example, data entered by a user seeking to arrange for a telephone call to be accepted and routed by a telecommunications system.

361 This encapsulates the data which is found at the beginning of each packet in a packet switched network which indicates which communications data attaches to which communication. See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 33.

relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic may identify a server but not a website or page.[362]

References in relation to traffic data comprising signals for the actuation of an apparatus to a telecommunication system (by means of which a communication is being or may be transmitted) include references to any telecommunication system in which that apparatus is comprised. References to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.[363] An interesting analogy is found in section 21(7) that defines data, in relation to a postal item,[364] to mean anything written on the outside of the item.

6.3.2.6 Protected data

Section 56(1) of RIPA defines protected information as any electronic data which, without the key to the data cannot or cannot readily be accessed or put into an intelligible form. The intelligibility of data includes references to its being in the condition in which it was before an encryption[365] or similar process was applied to it to the data being restored to that condition.[366] A key, in relation to electronic data, means any key, code, password, algorithm or other data the use of which, with or without keys, allows access to the electronic data or facilitates putting the data into an intelligible form.

6.3.3 Different production devices

6.3.3.1 Production order in terms of Schedule 1 to PACE

The process is initiated by a law enforcement officer[367] applying to a circuit judge for a production order. The application hearing is *inter partes*[368] and notice of the application must be given to the person from whom access is sought.[369] A person on whom a notice is served is

---

362 See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 34.

363 Section 21(7) of RIPA , which is precisely the same as section 2(10). Sections 10(b) and 21(7)(b) ensure that the references to data being attached to a communication in section 2(5) include data which may not be transmitted simultaneously with the contents of that communication such as the calling line identifier (the data which identifies the number of the person making a telephone call). See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 35.

364 A postal item is defined in section 21(7) to mean any letter, postcard or other such thing in writing that may be used by the sender for imparting information to the recipient, or any packet or parcel.

365 See Chapter 2 re encryption. See also Bharvada 2002 *International Review of Law, Computers & Technology* for an overview of the use of electronic signature, biometrics and public key infrastructures in the United Kingdom.

366 This definition of intelligibility is the same as the one provided in section 15(3) of the Electronic Communications Act 2000.

367 Paragraph 3.4 of the PACE Code B requires that an application for a search warrant or production order must be supported by a signed written authority from an officer of the rank of inspector or above. An application under Schedule 5 of the Terrorism Act of 2000 for a production order, search warrant or an order requiring an explanation of material seized or produced under such a warrant or production order must be supported by a signed written authority from an officer of the rank of superintendent or above.

368 Paragraph 7 of Schedule 1 to PACE.

369 In accordance with paragraphs 8, 9 and 10 of Schedule 1 of PACE. In *R v Crown Court at Leicester ex parte DPP* [1987] 3 All ER 654, 86 Cr App Rep 254, it was held that the person under investigation did not need to be notified where information relating to her was sought from her bank. This approach was approved in *Barclays Bank plc v Taylor; Trustee Savings Bank of Wales and border Counties v Taylor* [1989] 3 All ER 563; [1989] 1 WLR 1066, where it was held that the bank in such a

forbidden to conceal, destroy, alter, or dispose of the material to which the application relates without the leave of a judge, or the written permission of a law enforcement officer.[370] The obligation to preserve the material continues until the application is dismissed or abandoned, or there has been compliance with an order made as a result of the application. The sanction for breaking the obligation to preserve the material is unclear, but it would presumably be dealt with as contempt of court.[371]

The application notice should provide a description of all that is sought to be produced or discovered and be sufficient to enable the person on whom the notice is served to comply with the obligation not to interfere with the material subject to it.[372] If law enforcement officers fear that giving notice may lead to the disappearance of such items, they should seek a warrant *ex parte*.[373] In addition, the notice ought to indicate the general nature of the offence or offences under investigation and the address of the premises where the material is alleged to be.[374] In some circumstances it may be acceptable for the required information to be given orally, but then the written notice should then identify the person to whom the information has been given.[375]

At the *inter partes* hearing, the judge must be satisfied that one of the two sets of access conditions (contained in paragraphs 2 and 3 of Schedule1 to PACE) has been satisfied. It is important that the judge is presented with sufficient material to make this decision.[376]

The second set of access conditions[377] applies where law enforcement agencies are able to obtain a search warrant under some other Act, but for section 9(2) of PACE. The judge must be

---

situation was under no obligation to notify its customers of what was happening. The Divisional Court in *R v Crown Court at Lewes ex parte Hill* [1991] 93 Cr App R 60 took the view that the same principles applied whether the person about whom the information was sought was simply under investigation, or had been charged (at 67). The Court, however, stated that although an accused person has no statutory right to be given notice or to be heard, it may sometimes be helpful to hear what such a person might wish to say before she decides whether to make an order or not. Sharpe opines that it is likely that the practice of notifying the holder of the information, rather than the suspect, will be challenged under article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms. See Sharpe *Search and Surveillance* 84. However, in *Klass v Federal Republic of Germany* (1978) 2 EHRR 214, 5029/71 [1978] ECHR 4, the European Court of Human Rights accepted that it was not feasible in all cases to notify a suspect affected by surveillance activities, even after the cessation of such surveillance. Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms would permit non-notification where it was necessary for the protection of the democratic society as a whole. Whether the procedure for obtaining a production order would satisfy this proportionality principle depends on the facts of the particular case.

370 Paragraph 11 of Schedule 1 of PACE.

371 *R v Adegbesan* [1986] 3 All ER 113, 117.

372 *R v Adegbesan* [1986] 3 All ER 113, 117.

373 In terms of paragraphs 12 -14 of Schedule 1 to PACE. See also the discussion of this type of search warrant in paragraph 6.2.3.1.2 above.

374 Stone *The Law of Entry, Search, and Seizure* 140.

375 *R v Manchester Crown Court ex parte Taylor* [1988] Crim LR 386, DC.

376 In particular, in situations where the person from whom the material is sought is not concerned to oppose the application there is an obligation on the applicant to make sure that everything, including material adverse to the application, is before the judge. An example may be the case in relation to records held by a bank. See *R v Crown Court at Lewes ex parte Hill* [1991] 93 Cr App Rep 60, 69. In *R v Central Criminal Court ex parte Bright* [2001] 2 All ER 244, the Court of Appeal held that since the judge acts as the safeguard between law enforcement and the person from whom the material is sought, it is essential that the judge should be personally satisfied that the statutory requirements have been established. In *R v Acton Crown Court ex parte Layton* [1993] Crim LR 458, it was emphasized that law enforcement must be open-handed and set out all the material in their hands, whether it assisted in the application under Schedule 1 of PACE or militated against it.

377 As set out in paragraph 3 of Schedule 1 of PACE.

satisfied that there are reasonable grounds for believing that excluded or special procedure material is on the premises specified, or on premises occupied or controlled by the person specified in the application[378] and that the issue of such a warrant would be appropriate. It is only under this set of access conditions that an order relating to excluded material may be made.[379]

The alternative first set of access conditions[380] to some extent follows the provisions of section 8(1) which apply to ordinary search warrants under PACE.[381] There must be reasonable grounds for believing that a serious arrestable offence[382] has been committed and that, on specified premises, there is special procedure material which is likely to be relevant evidence of substantial value to the investigation.[383] The judge must give serious attention to these issues.[384] In addition, the judge must be satisfied that other methods of obtaining the material have been tried without success, or have not been tried because it appeared that they were bound to fail.[385] The power to make an order should be regarded as substantially the last resort and so only used where absolutely necessary.[386] Finally, the judge must be satisfied that it is in the public interest that the material(s) are produced or access to it is given.[387] In deciding what is in the public interest, the judge should take into account the benefit likely to accrue to the investigation if the material is obtained and to the circumstances under which the person in possession of the material holds it.[388]

If, at the *inter partes* hearing of the application, the judge is satisfied that one of the sets of access conditions is satisfied, she may order the person who has possession of the material either to produce it to law enforcement or to give a law enforcement officer access to it, within seven days.[389] If the material consists of information held in any electronic form, it must be produced in a form in which it can be taken away and in which it is visible and legible or from

---

378 Including all such premises on which there are reasonable grounds for believing that there is excluded or special procedure material as it is reasonably practicable to specify. Paragraph 3(a) of Schedule 1 of PACE.

379 *R v Central Criminal Court ex parte Brown* The Times, 7 September 1992. Stone *The Law of Entry, Search, and Seizure* 141.

380 As set out in paragraph 2 of Schedule 1 of PACE.

381 See paragraph 6.2.3.1.1 above for a discussion of section 8 of PACE.

382 See footnote 30 and paragraph 6.2.1 above for a description of serious arrestable offences.

383 Paragraph 2(a) of Schedule 1 of PACE.

384 In *R v Crown Court at Southwark and HM Customs and Excise, ex parte Sorsky Defries* [1996] Crim LR 195,it was felt that the judge could not have been satisfied of the relevant matters, as he took only 15 minutes to come to a decision.

385 Paragraph 2(b) of Schedule 1 of PACE. This may include attempting alternative legal procedures, such as by making applications under the Bankers' Books Evidence Act of 1879 in relation to bank accounts, or giving the person whom the information concerns the opportunity to consent to its disclosure. Stone *The Law of Entry, Search and Seizure* 142.

386 *R v Crown Court at Lewes ex parte Hill* [1991] 93 Cr App Rep 60, 71.

387 Paragraph 2(c) of Schedule 1 of PACE.

388 The implied judicial discretion embedded in the public interest condition should not be used capriciously. Stone opines that it is difficult to imagine many circumstances where a judge is willing to hold that it is contrary to the public interest to allow the police access to relevant evidence which may be of substantial value to the investigation of a serious arrestable offence. See Stone *The Law of Entry, Search, and Seizure* 143-146 for a critical discussion of this issue in the context of case law. The issue of public interest was considered in *R v Bristol Crown Court ex parte Bristol Press and Picture Agency* (1986) 85 Cr App Rep 190; *Senior v Holdsworth ex parte Independent Television News Ltd* [1976] 1 QB 23; *R v Crown Court at Northampton ex parte DPP* (1991) 93 Cr App Rep 376; *R v Central Criminal Court ex parte Bright* [2001] 2 All ER 244. See also Sharpe *Search and Surveillance* 87-88. It is becoming increasingly difficult to maintain an official secrecy regime in these times of human rights, freedom of information and whisteblowing. See in this regard CASE NOTE R v Central Criminal Court ex parte Bright, Alton and Rusbridger "Divisional Court – PACE Special Procedure Production Orders, the Official Secrets Act of 1989 and the Public Interest in Disclosure" 2001 *Journal of Criminal Law* 4-6.

389 Paragraph 4 of Schedule 1 of PACE. The order may itself specify a longer period.

which it can readily be produced in a visible and legible form.[390] Anything produced in response to an order must be dealt with in accordance with the provisions of sections 21 and 22 of PACE pertaining to access, copying and retention.[391] Failure to comply with an order is to be dealt with by the judge as if it were contempt of the Crown Court.[392] Once an order has been made, the issuing judge has no jurisdiction to vary it. The correct procedure to challenge a court order is judicial review.[393]

Whilst difficulties over the seizure of legally privileged material usually arise in the context of application made under Schedule 1 of PACE, but the seizure of documents under a section 8 warrant has been subject to challenge on the basis that legal privilege may have applied.[394] Judicial review of the warrant is granted on the basis that even where there was doubt about the existence of the privilege, the matter should have been considered by a circuit judge. Even where there is only a *prima facie* claim of privilege, law enforcement officers should rather proceed under Schedule 1 of PACE. If it is inappropriate for a justice to consider the scope of legal privilege, it is surely even more inappropriate for a police officer at the scene of the seizure to do so.[395]

6.3.3.2 Authorisations and notices for communications data in terms of RIPA

Chapter II of RIPA provides a legislative framework to cover the requisition, provision and handling of communications data. It clarifies the duties and responsibilities placed upon each party involved in these processes and create a system of safeguards, reflecting the requirements of article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms.[396]

The strict test of necessity must be met before any communications data is obtained in terms of sections 21 to 25 of RIPA.[397] The assessment of necessity is one made by a person designated by order of the Secretary of State.[398] The designated person must not only consider the communications data to be necessary, but must also apply a proportionality test as to the conduct involved in obtaining the communications data.[399] Obtaining communications data is necessary if it is necessary in the interests of national security, the economic well-being of

---

390 Section 19(4) and paragraph 5 of Schedule 1 of PACE.
391 Paragraph 6 of Schedule 1 of PACE. See paragraph 6.2.3.1.1.above for a discussion of sections 21 and 22 of PACE.
392 Paragraph 15 of Schedule 1 of PACE.
393 See *R v Crown Court at Liverpool ex parte Wimpey plc* [1991] Crim LR 635.
394 See *R v Guildhall Magistrate's Court ex parte Primlacks Holdings Co. (Panama) Inc.* [1990] 1 QB 261.
395 Sharpe *Search and Surveillance* 64.
396 See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 156. Section 21(1) of RIPA distinguishes between interception of communications in the course of their transmission, which is activity excluded from this part of the Act, and conduct involving the obtaining of or disclosure of communications data, which is activity covered by this part of the Act. This is in line with the requirement that interception and monitoring must be discerned from search and seizure and other methods to obtain data, as explained in paragraph 2.4 above.
397 Section 22(1) of RIPA).
398 Section 25(2) of RIPA.
399 Section 22(5) of RIPA.

England (and the whole of the United Kingdom) or public safety. It is also deemed necessary for the purposes of preventing crime or detecting crime, preventing disorder, protecting public health and assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department. Communications data may also be obtained for the purpose, in an emergency, of preventing death and/or mitigating injury or any damage to a person's physical or mental health.[400] The Secretary of State has the discretion to issue an order in which any other purpose is specified as necessary for the purposes of obtaining communications data.[401]

There are essentially two ways in which communications data may be obtained. Firstly, section 22(3) of RIPA provides a means for a designated person to authorise someone within the same relevant public authority[402] to provide the legal basis upon which the public authority may itself collect the communications data.[403]

Section 22(4) of RIPA provides the second way in which communications data may be obtained by allowing a designated person to serve a notice upon the holder of the data, requiring the holder to comply with the terms of the notice. A communications service provider in receipt of a section 22(4) notice must comply with the notice as soon as reasonably practicable if the provision of the data is reasonably practicable.[404] If a communications service provider fails to provide the required communications data, the Secretary of State may take civil proceedings against the provider. This may result in the issue, *inter alia*, of an injunction which would have the effect of compelling the provision of data.[405]

Authorisations and notices must be granted in writing or, if not in writing, in a manner that produces a record of their having been granted. They must specify the office, rank, or position held by the person granting them. They must describe the conduct authorised and/or the communications data to be obtained or disclosed and must detail the grounds upon which this is deemed necessary.[406] A notice must also specify the manner in which any disclosure required by it is to be made.

---

400 With the exception of section 22(2)(g), these are the same as the purposes for which directed surveillance and the use of a cover human intelligence source may be permitted by sections 28 and 29 of RIPA. See section 22(2) of RIPA.

401 A draft of such an order must have been laid before Parliament and approved by a resolution of each House before the Secretary of State may make an order under section 22(2)(h).

402 Section 25(1) defines a relevant public authority as any of the following: a police force, the National Criminal Intelligence Service, the National Crime Squad, the Commissioners of Customs and Excise, the Commissioners of Inland Revenue, any of the intelligence services and any other public authority specified as such by an order made by the Secretary of State. Under section 25(3), the Secretary of State may place restrictions on who may act under these provisions and in what circumstances.

403 Where, for example, a private telecommunications operator was technically unable to collect certain communications data, section 22(3) would provide the authority to allow an investigating body to collect the data themselves. See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 156.

404 Section 22(6) and 22(7) of RIPA.

405 Section 22(8) of RIPA.

406 The format which authorisations and notices must take is explained in sections 23(1) and (2), respectively.

Disclosure may only be required of data in the possession of or obtained by the communications service provider during the authorisation period of authorisations and notices, which is set at one month.[407] An authorisation or notice may be renewed at any time during the month, by following the same procedure as in obtaining a fresh authorisation or notice.[408] The period for which a renewed authorisation or notice is extant begins at the point at which the notice or authorisation it is renewing expires.[409]

The person to whom the data may be disclosed is restricted to the person giving the notice or another specified person who must be from the same relevant public authority.[410] As soon as it is clear that the reasons for which a notice was granted are no longer valid, such a notice must be cancelled.[411]

The Secretary of State must ensure that payment arrangements are made in order to compensate holders of communications data for the costs involved in complying with notices issued under chapter II of RIPA, albeit made out of money provided by Parliament.[412]

The Regulation of Investigatory Powers (Communications Data) Order 2003[413] is of particular importance and came into force on 5 January 2004.[414] This order specifies additional public authorities for purposes of section 25(1) of RIPA. It also specifies which individuals within those authorities, and the public authorities already listed in the act, are entitled to acquire communications data. It also places restrictions on the grounds allowing for the acquisition of communications data and the types of communications data that may be acquired.[415]

6.3.3.3 Notices for protected data in terms of RIPA

Sections 49 to 56 of RIPA facilitate the disclosure of protected data.[416] Properly authorised members of law enforcement, security and intelligence agencies are empowered to serve

---

407 Section 23(4) of RIPA..
408 Section 23(5) and (6) of RIPA.
409 Section 23(7) of RIPA.
410 Section 23(3) of RIPA.
411 Section 23(8) of RIPA specifically incorporates the necessity and proportionality tests.
412 Section 24 of RIPA.
413 SI 2003 No 3172.
414 HSE Enforcement Guide (England & Wales) (2006) "Evidence That May Assist in Your Investigation" found on the Internet http://www.hse.gov.uk/enforce/enforcementguide/investigation/physical/evidence.htm 2.
415 See the "Explanatory Note to the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003 No 3172)" 1.
416 The first consultation on this subject was undertaken by the previous administration in March 1997. A broader consultation "Building Confidence in Electronic Commerce: A Consultation Document" was launched on 5 March 1999 (URN 99/642). Finally, provisions very similar to those put forward in this Consultation Document were published as Part III of the draft Electronic Communications Bill issued for consultation on 23 July 1999. See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 12. In June 2006, the United Kingdom government finally decided to activate Part III of RIPA. The provisions of Part III have not yet been implemented because the development and adoption of encryption and other information protection technologies has been slower than was anticipated when the Act was passed. The Home Office has therefore now released a public consultation on a draft statutory Code of Practice for the implementation of RIPA Part III (replies are required by 30 August 2006). The government is also proposing an increase in the maximum penalty for not disclosing encryption keys when required to do so under RIPA. Where a notice to provide encryption keys is given for reasons of national security, the penalty for non-

notices on individuals or bodies requiring the disclosure of protected information which they lawfully hold, or are likely to hold, in an intelligible form.

The information to which the power to service notices applies is limited by the definition of the various means by which the protected information in question has been, or is likely to be, lawfully obtained. This could, for example, be:

(a) material seized under a search and seizure warrant in terms of PACE 1984;

(b) material that was lawfully obtained under an authorisation in terms of section 22(3) or a notice in terms of section 22(4) of RIPA; or

(c) material which has lawfully come into the possession of a law enforcement officer but not by use of statutory functions, for example, where the material has been voluntarily handed over.[417]

The effect of Schedule 2 of RIPA[418] is to set authorisation levels for permission to serve a notice under section 49. The level of authority required varies depending on the power under which the protected information was, or is likely to be, lawfully obtained. In England, the general rule is that a circuit judge must grant a person the appropriate permission to give section 49 notices in relation to any protected information.[419] One exception to the general rule include cases where a search warrant issued by a person holding judicial office or the Secretary of State[420] contains the relevant authority's permission in relation to that protected information. Another exception is where written permission is granted by the relevant authority for the giving of such notices in relation to protected information obtained under a search warrant, after the issue of the warrant.[421] Only a person who is entitled to exercise the power conferred by the warrant[422] is capable of getting the appropriate permission to grant section 49 notices in relation to protected information obtained, or to be obtained, under a warrant issued by a person holding judicial office.[423]

---

compliance is to rise to five years (in other cases the penalty will remain unchanged – see section 53 of RIPA). See Linx Public Affairs "Home Office to Demand Encryption Keys, At Last" found on the Internet http://publicaffairs.linx.net/news/?cat=37 1-4.

417 Section 49(1) of RIPA. Other examples would be where the material has been intercepted by means of any statutory power to intercept communications or where the material was lawfully obtained by law enforcement as a result of having been provided or disclosed in pursuance of any statutory duty, whether or not one arising as a result of a request for information, other than under a warrant (for example, under the Customs and Excise Management Act of 1979).

418 As introduced by section 49(11) of RIPA.

419 Paragraph 1(1) to Schedule 2 of RIPA. Paragraph 2 is aimed at data obtained under a warrant; paragraph 3 is directed at data obtained by the intelligence services under statute but without a warrant; paragraph 4 deals with data obtained under statute by other persons but without a warrant; paragraph 5 addresses data obtained without the exercise of statutory powers; paragraph 6 provides the general requirements relating to the appropriate permission; paragraph 7 details the duration of permission and paragraph 8 sets out the formalities for permission granted by the Secretary of State. Some of these provisions are referred to in relation to production, preservation and search and seizure devices.

420 In terms of paragraph 8 of Schedule 2 of RIPA, permission shall not be granted by the Secretary of State except under her hand or in an urgent case in which the Secretary of State has expressly authorised the grant of permission, under the hand of a senior official.

421 Paragraphs 2(1) and (2) of Schedule 2 of RIPA.

422 Or is of the description of persons on whom the power conferred by the warrant is conferred.

423 Paragraph 2(4) of Schedule 2 of RIPA. Paragraph 2(8) provides that references in paragraph 2 of Schedule 2 of RIPA to a person holding judicial office are references to, *inter alia*, any judge of the Crown Court or of the High Court of the Judiciary,

Persons with the appropriate permission in terms of Schedule 2 of RIPA may serve a notice imposing a disclosure requirement in respect of the protected information in question, provided there are reasonable grounds for believing[424]

(a) that the key[425] to the relevant protected information is in the possession of the person on whom the notice is being served;

(b) that serving a notice imposing a disclosure requirement is necessary in the interests of national security or the economic well-being of England (and the whole of the United Kingdom) or for the purposes of preventing or detecting crime[426] or for securing the effective exercise or proper performance of any statutory power or duty of a public authority;

(c) that imposing a disclosure requirement is proportionate to what is sought to be achieved by its imposition; and

(d) that an intelligible version of the relevant protected information cannot be obtained by any other reasonably practicable means.

A notice imposing a disclosure requirement in respect of any protected information must be given in writing or must be given in a manner that produces a record of its having been given. It must describe the protected information to which the notice relates, set out the disclosure that is required by the notice and the form and manner in which the disclosure is to be made. It must specify the following: the necessity grounds[427] by reference to which the notice is given; the office, rank, or position held both by the person giving it and the person granted permission for the giving of the notice, and the time by which the notice is to be complied with.[428]

If it appears that more than one person is in possession of the key to any protected information and any one of those persons is in possession of the key in her capacity as an officer or employee of the organisation, notices must be served on a senior officer[429] within a corporate

---

any justice of the peace and any person holding any such judicial office as entitles her to exercise the jurisdiction of a judge of the Crown Court or of a justice of the peace.

424 Section 49(2) of RIPA.

425 Section 56(1) defines a key, in relation to any electronic data, to mean any key, code, password, algorithm, or other data the use of which, with or without other keys, allows access to the electronic data or facilitates the putting of the data into an intelligible form. This definition resounds in the definition of a key provided in section 14(3) of the Electronic Communications Act of 2000. References to a person's having information, including a key to protected information, in her possession include references to the following: its being in the possession of a person who is under her control so far as that information is concerned; to her having an immediate right of access to it, or an immediate right to have it transmitted or otherwise supplied to her; and to its being, or being contained in, anything which she or a person under her control is entitled, in exercise of any statutory power and without otherwise taking possession of it, to detain, inspect or search.

426 Section 49(3) of RIPA.

427 See paragraph (b) above.

428 Section 49(4) of RIPA.

429 Section 49(10) of RIPA defines a senior officer, in relation to a body corporate, as a director, manager, secretary or other similar officer of the body corporate. Director in relation to a body corporate whose affairs are managed by its members means a member of the body corporate, for this purpose. Section 49(6) requires that the notice be served on a partner or a senior employee of a firm.

body or firm.[430] An exception is provided for in cases where special circumstances to the case would defeat the purposes for which a notice is given.[431]

The making of a disclosure by a recipient of a notice must be to the person giving the notice or such other person as may be specified in, or otherwise identified by, the notice.[432] A key which is used solely for the purpose of generating electronic signatures[433] does not have to be disclosed in response to a notice.[434]

The effect of serving a notice imposing a disclosure requirement varies. Where a person, at the time a notice is served,[435] is in possession of the relevant protected information and a means of accessing it and of disclosing it in an intelligible form,[436] the effect of imposing a disclosure requirement is that the recipient of a notice may use any key in her possession to access the information or to put it into intelligible form. Alternatively, the person must facilitate disclosure in accordance with the terms of the notice.[437] A person who is required to disclose information in an intelligible form may instead opt to disclose a relevant key if she so prefers.[438] Where a notice is served on a person who does not have the relevant protected information in her possession; or cannot access the information without the use of a key which is not in her possession; or the notice contains a direction that a key must be disclosed,[439] that person must disclose any key to the information that is in her possession at a relevant time.[440]

RIPA does not prohibit a person giving a section 49 notice also to give the recipient access to the protected information, in order to allow her to produce plain text rather than disclose a key.[441] A person, who is served with a notice to disclose every key to the relevant protected

---

430 Sections 49(5) and (6) of RIPA.

431 An example would be where the senior officer is a suspect in a criminal investigation. Section 49(7) of RIPA.

432 Section 49(8) of RIPA.

433 An electronic signature is defined in section 56(1) as anything in electronic form which is incorporated into, or otherwise logically associated with any electronic communication or other electronic data; is generated by the signatory or other source of the communication or data and is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both. Section 56(4)(a) stipulates that references to the authenticity of any communication or data are references to any one or more of the following: whether the communication or data comes from a particular person or other source; whether it is accurately timed and dated or whether it is intended to have legal effect. Section 56(4)(b) states that references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data. These definitions of authenticity and integrity are the same as the definitions provided thereof in section 15(2) of the Electronic Communications Act of 2000.

434 Section 49(9) of RIPA.

435 A reference to a relevant time, in relation to a disclosure requirement imposed by a section 49 notice, is defined in section 50(10) to mean the time of the giving of the notice or any subsequent time before the time by which the requirement falls to be complied with.

436 This means that they have the password, in the case of material protected by a password; or the decryption key in the case of encrypted material; or both, in the case of material protected in both ways. See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 265.

437 Section 50(1) of RIPA.

438 Section 50(2) of RIPA.

439 As to which, see section 51 of RIPA.

440 Section 50(3) of RIPA. This duty is qualified by sections 50(4) to (6) of RIPA. The effect of sections 50(4) and (5) is that where a person served with a notice is entitled or obliged to disclose a key, they need only provide those keys which are sufficient to access the relevant information and to put it into intelligible form. And section 50(6) further provides that such a person may choose which keys to provide, so long as they suffice to access the information and render it intelligible.

441 See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 268.

information that is in her possession need only provide those keys which suffice to access the information and render it intelligible, and that she may choose which keys to provide to achieve the same end.[442] Where a person served with a notice no longer possesses a key to the relevant protected information, she is to disclose all information that is in her possession which could facilitate the discovery of the key.[443]

If a key is required to be disclosed rather than the disclosure of protected information in an intelligible form, extra requirements are to be met. A notice may not contain a statement that it can be complied with only by disclosing a key unless a direction to this effect has been given by the person giving permission for the notice to be served.[444] A police direction that a key must be disclosed must be given expressly by the chief officer of police.[445] A person may only give a direction requiring the disclosure of a key if she believes that there are special circumstances to the case making this necessary and that giving such a direction is proportionate to the outcome sought.[446] In deciding whether it is proportionate to require that a key be disclosed, consideration must be given to the type of other information also protected by the key in question and also to the potential adverse impact on a business that might result from requiring that a key be disclosed.[447] Any direction to disclose a key given internally by the police must be notified within seven days to the Chief Surveillance Commissioner.[448]

Payment arrangements must be made in order to compensate persons who are required to disclose information following service of a notice under section 49.[449]

A person served with a notice is guilty of an offence if she knowingly fails to comply with the disclosure requirement contained in that notice.[450] If it is shown that a person was in possession of a key to any protected information at any time before a section 49 notice is given, that person is taken to have continued to be in possession of that key at all subsequent times. If it is, however, shown that the key was not in a person's possession after the notice was given and before the time by which the person was required to disclose it, the person is not considered to have been in possession of the key at all subsequent times.[451] If doubt is raised as to whether the person still had the key when the notice was given, she is not held liable for

---

442 Section 50(5), (6) and (7) of RIPA.
443 Section 50(8) of RIPA.
444 Section 51(1) of RIPA.
445 Sections 51(2) and (3) of RIPA. Similar requirements are set for directions by customs and excise and Her Majesty's forces.
446 Section 51(4) of RIPA.
447 Section 51(5) of RIPA.
448 Sections 51(6) and (7) of RIPA. Similar requirements are set for directions by customs and excise and Her Majesty's forces.
449 Section 52 of RIPA.
450 Section 53(1) of RIPA. Section 53(5) of RIPA specifies the maximum sentence for the offence of failing to comply with a notice. As regards financial penalties, there is no upper limit to fines set in the Crown Court on conviction on indictment, although the term of imprisonment that could be imposed is set at two years. On summary conviction in a Magistrate's Court the maximum fine is £5 000 and the imprisonment term is fixed at a maximum of six months. See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 284.
451 Section 52(2) of RIPA.

the disclosure.[452] A person who shows that it was not practicable to comply with the disclosure requirement placed upon her before the time she was required to do so, but that she did make the required disclosure as soon as was reasonably practicable, will not be held liable.[453]

Where the recipient of a notice that explicitly contains a secrecy requirement, or a person that becomes aware of it tips off another person that a notice has been served, or reveals its contents, such a person is guilty of an offence.[454] The rationale behind this is to preserve, where necessary, the covert nature of an investigation. The inclusion of a secrecy requirement in a notice must be authorised by the person who is giving permission for such a notice to be served.[455] The imposition of such a requirement is restricted to instances where the maintenance of the effectiveness of any investigation or investigatory techniques is at stake. It may also be imposed in the interests of the safety and well-being of any person.[456]

Various statutory defences may be levelled against a tipping-off charge. Where the tipping-off occurs entirely as a result of software designed to give an automatic warning that a key has been compromised and where, in addition, the defendant is unable to stop this from taking place after receiving the notice, she is not held liable.[457] Liability is also ruled out where a disclosure is made to or by a professional legal adviser as part of advice, concerning the effect of the provisions of this part of RIPA, given to a client or her representative or where a disclosure was made by a legal adviser in connection with any proceedings before a court or tribunal.[458] This statutory defence is not available where a professional legal adviser tips off a client with a view to furthering any criminal purpose.[459]

Disclosures are lawful if confined to a relevant Commissioner[460] or persons authorised by such a Commissioner. Persons are also deemed lawfully authorised for disclosure purposes if authorised by:

(a) the terms of the disclosure notice;

(b) by the person who gave the notice or by someone on her behalf; or

---

452 Sections 52(3) of RIPA.

453 Section 53(4) of RIPA.

454 Section 54(4) of RIPA specifies the maximum sentence for the tipping-off offence. On conviction in the Crown Court, the maximum term of imprisonment is five years, and six months in the Magistrate's Court. The financial penalties are the same as for the offence set out in section 53 of RIPA. See footnote 451 above.

455 Or where such a person herself has permission to serve a notice, for example, a superintendent in certain cases. Section 54(2) of RIPA. See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm paragraph 287.

456 Section 54(3) of RIPA.

457 Section 54(5) of RIPA.

458 Section 54(6) and (7) of RIPA.

459 Section 54(8) of RIPA.

460 Section 54(11) of RIPA provides that relevant Commissioner, for purposes of section 54, means the Interception of Communications Commissioner, the Intelligence Services Commissioner or any Surveillance Commissioner of Assistant Surveillance Commissioner.

(c) by a person who is in lawful possession of the protected data to which the notice relates, as described in section 49 of RIPA.[461]

The effect of this provision is to ensure that, for example, persons within an organisation may be informed about a notice in order to give effect to it by accessing a key or plain text of the protected data, without this falling foul of the tipping-off offence.[462] A person told about a notice, but not about the fact that there was a requirement for secrecy, may also avail herself of a statutory defence.[463]

Certain safeguard requirements apply to all those who may have responsibility for organisations that handle material provided in response to a section 49 notice.[464] An onus rests on such responsible persons to ensure that

(a) any keys disclosed are used only for a purpose for which the key(s) may be required;

(b) the uses to which the keys are put are reasonable;

(c) the use and any retention of the keys are proportionate;

(d) that the keys are stored in a secure manner; and

(e) that the keys are destroyed as soon as they are no longer needed.[465]

The keys are to be shared with the minimum number of people possible.[466] A civil liability is imposed in instances where seized keys are compromised by a failure of these safeguards.[467]

The provisions in respect of cryptography contained in the Electronic Communications Act[468] must be considered in the context of the provision of or access to protected data.

---

461 Section 54(9) of RIPA.

462 See the "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.|uk/acts/en2000/2000en23.htm paragraph 294.

463 Section 54(10) of RIPA.

464 These persons include the Secretary of State in respect of the security and intelligence agencies, every other Minister of the Crown in charge of a government department, every chief officer of police, the Commissioners of Customs and Excise and every person whose officers or employees include persons with duties that involve the giving of section 49 notices. See section 55(1) of RIPA.

465 Section 55(2) of RIPA.

466 Section 55(3) of RIPA.

467 Section 55(4) of RIPA. This civil liability is aimed both at persons who fail to ensure that adequate arrangements are in place for the protection of keys, as well as at persons who contravene these arrangements and so compromise a key. Section 55(5) of RIPA limits the persons who may bring an action to persons who have made a disclosure in pursuance of a section 49 notice or those persons whose protected information or key has been disclosed by some other person in pursuance of a notice. Section 55(6) of RIPA stipulates that information is considered to belong to a person if she has any right that would be infringed by an unauthorised disclosure of the information. A key is considered to belong to a person if it is a key to information that belongs to her or she has any right that would be infringed by an unauthorised disclosure of the key.

468 Of 2000. Sections 1 to 6 deal with cryptography service providers and establish a register of approved cryptography service providers. Section 4(2)(d) provides for the disclosure of information obtained under or by virtue of the provisions of Part 1 of the Electronic Communications Act of 2000 and which relates to the private affairs of any individual or to any particular business without consent, in connection with the investigation of any criminal offence or for the purposes of any criminal proceedings. Section 7 deals with electronic signature and related certificates. Section 14 contains a prohibition on key escrow requirements. It stipulates that no power is conferred on any Minister of the Crown by conditions of approval under

6.4 *Preservation and partial disclosure devices*

No specific provision has been made in the criminal[469] procedural law framework of England for preservation and partial disclosure mechanisms. The traditional measures of search and seizure and production set out above[470] must accordingly be utilised to accomplish the expedited preservation of stored computer data and the expedited preservation and partial disclosure of traffic data.

With regard to the expedited preservation of traffic data, the retention requirements applicable to certain categories of communications data need to be considered. The retention of communications data is closely associated with the provision and accessing thereof. Data that has been retained is, by default, preserved. The opportunity for law enforcement agencies to obtain data is of less value than it might be if the communications companies have no obligation to retain data.[471]

The retention of communications data in England is currently addressed by the current Code of Practice for Voluntary Retention of Communications Data, issued by the Home Secretary in

---

Part I or by any regulations or order under the Electronic Communications Act of 2000, to impose a requirement on any person to deposit a key for electronic data with another person. This shall not prohibit the imposition of an order under section 8 regarding a requirement to deposit a key for electronic data with the intended recipient of electronic communications comprising the data. Alternatively, a requirement is allowed for arrangements to be made, in cases where a key for data is not deposited with another person, which otherwise secure that the loss of a key, or its becoming unusable, does not have the effect that the information contained in a record kept in pursuance of any provision made by or under any enactment or subordinate legislation becomes inaccessible or incapable of being put into an intelligible form.

469 Technological developments in the area of communications fed the amazing growth in the mid-1970s of an order, sometimes called a "civil search warrant", which could be sought, without notice to the other party, sometimes even before a writ had been issued. This growth continued into the 1990s with the increase in the availability and use of computer software, which has become a profitable source of illegitimate copying in many parts of the world. These so-called "warrants" were in fact orders issued by the High Court (most often the Chancery Division), without notice, under the authority of Order 29 of the Rules of the Supreme Court, combined with the inherent jurisdiction of the Court to make orders of this type in order to preserve evidence. They were originally known as "Anton Pillar-orders", after the plaintiffs in the first case of this type to receive the seal of approval of the Court of Appeal (*Pillar KG v Manufacturing Processes* [1976] 1 Ch 55, 60). The three essential preconditions for making the order are, firstly, that there must be an extremely strong *prima facie* case. Secondly, the dangers to the applicant, potential or actual, must be very serious. There must, lastly, be clear evidence that the respondents have in their possession incriminating documents or things and that there is a real possibility that they may destroy such material before any with notice application can be made. Since the search order is at the extremity of the court's powers, it should only be used where there is no alternative way of ensuring that justice is done to the applicant. See Stone *The Law of Entry, Search, and Seizure* 542. Search orders of this type are now governed by section 7 of the Civil Procedure Act of 1997 and Part 25 of the Civil Procedure Rules, together with its associated Practice Direction. The order sought in this case is not a search warrant, as it only authorises entry and inspection by permission of the defendants. It does, however, order the defendant's to give permission, lest they be found guilty of contempt of court. Once the enforcement of the order became backed up by the threat of contempt proceedings, the differences between the order and a search warrant exercised by a law enforcement officer, backed up by the threat of criminal proceedings for obstruction were perhaps a little subtle. The execution of a civil search order, relying on the permission of the respondent before it can be put into effect, ought to be a peaceful affair. In some cases, however, the applicant fears trouble, and inform the local police with a view to obtaining, if possible, the presence of a uniformed officer at the premises when the order is served, to forestall any breach of the peace. This was described as normal practice in *Columbia Picture Industries v Robinson* [1986] 3 All ER 338, 353. The law enforcement officer remains outside the premises unless a breach of the peace occurs (although the officer does have the power to enter if there is a reasonable anticipation of a breach of the peace – see *McLeod v Commissioner of Police of the Metropolis* [1994] 4 All ER 553)). The search order must not be carried out at the same time as a police search warrant as the simultaneous execution is considered unfortunate. If the police are to be involved in more than a supervisory role when a civil search order is executed, the applicant must inform the judge issuing the order. Such involvement should be avoided altogether, if possible. See Stone *The Law of Entry, Search, and Seizure* 562. See footnote 565 in paragraph 5.6 above for a reference to the Anton Pillar Order in the South African legislative context.

470 In paragraphs 6.2 and 6.3 respectively.

471 Bristows 2002 *Computer Law & Security Report* 205.

2003 under authority of the Anti-Terrorism, Crime and Security Act.[472] The Code prescribes a range of maximum retention periods for communications and traffic data. Subscriber information and telephony data are to be retained for a maximum of 12 months; short message service (SMS),[473] enhanced messaging service (EMS),[474] multimedia messaging service (MMS)[475] data, email data and Internet Service Provider data for a maximum of six months and web activity data for a maximum of four days.[476]

The European Union has also now accepted the European Union Data Retention Directive. The European Union Data Retention Directive provides, *inter alia*, for the mandatory retention of data for a period between six and 24 months, although member states may extend the retention period. European Union countries have until August 2007 to implement the directive, which was initially proposed after the Madrid bombings in 2004.[477] The legislation is being championed by England, as the change in law was proposed during its presidency of the European Union in the wake of the bombings of 7 July 2005 in London.[478] This new European Union Data Retention Directive is intended to harmonise the laws of the member states in respect of the processing

---

472 Of 2003. This Act therefore did not directly introduce the process of data retention in the United Kingdom, but it set in place the mechanisms for issuing a consultation on a proposed Code that would be voted on, after consultation, some time later. See Whitley and Hosein 2005 *Telecommunications Policy* 861. Some industry stakeholders have, however, argued that while the United Kingdom government appears more than willing to follow the United States approach to combating international terrorism, it should be persuaded to follow the United States model of data preservation (see paragraph 5.4.1 above) rather than the European approach of data retention. See, for example, Sharpe and Russell 2003 *Privacy and Data Protection* 11-17. Clayton opines that the voluntary code means traffic data is often kept on a "best efforts" basis, meaning that "a disk failure holding a day's logs is just a matter of regret, back-ups are not taken, and many ISPs keep far less traffic data than the six months recommended in the voluntary code for email traffic data." See Mathieson 2005 *Computer Fraud & Security* 2.

473 SMS is a service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use the Global System for Mobile (GSM) communication. SMS is similar to paging. However, SMS messages do not required the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. An SMS gateway is a web site that allows users to enter a SMS message to someone within the cell served by that gateway or that acts as an international gateway for users with roaming capability. See Mobile Computing Definitions "Short Message Service" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci213660,00.html 1.

474 EMS is an adaptation of SMS that allows users to send and receive ring tones and operator logos, as well as combinations of simple media to and from EMS-compliant handsets. EMS works on all Global System for Mobile (GSM) communications networks. See Mobile Computing Definitions "Enhanced Messaging Service" found on the Internet http://searchmobile computing.techtarget.com/sDefinition/0,290660,sid40_gci785459,... 1.

475 MMS is a communications technology developed by 3GPP (Third Generation Partnership Project) that allows users to exchange multimedia communications between capable mobile phones and other devices. MMS is also an extension to SMS. MMS defines a way to send and receive, almost instantaneously, wireless messages that include images, audio and video clips in addition to text. When the technology has been fully developed, it will support the transmission of streaming video. Common current applications of MMS messages is picture messaging (the use of camera phones to take photos for immediate delivery to a mobile recipient), animations and graphic presentations of stock quotes, sports news and weather reports. See Mobile Computing Definitions "Multimedia Messaging Service" found on the Internet http://searchmobile computing.techtarget.com/sDefinition/0,290660,sid40_gci943702,... 1.

476 See Room 2004 *New Law Journal* 951.

477 The current European Union Data Retention Directive is by no means a new invention. See Quintessenz (2006) "EU Data Retention – Doqu/Base" found on the Internet http://www.quintessenz.at/cgi-bin/index?id=000100002986 1. The Directive has drawn fire from privacy advocates who believe the directive is a threat to human rights. Adopting this directive would cause an irreversible shift in civil liberties within the European Union. It will adversely affect consumer rights throughout Europe and it will generate an unprecedented obstacle to the global competitiveness of European industry. Telecommunications companies and ISP's expressed concerns about the financial impact of the parliament's decision as the new law will drastically increase companies' storage costs. c/Net News.com (2006) "EU Data Retention Directive Gets Final Nod" found on the Internet http://news.com.com/2100-7348_3-60423032.html 1.

478 c/Net News.com (2006) "Europe Passes Tough New Data Retention Laws" found on the Internet http://news.com.com/Europe+passes+though+new+data+retention+laws/2100-7350_3- 1. It is also interesting to note that the United Kingdom has indicated that it plans to use the UK's presidency of the European Union to push through stronger initiatives for *e*-government and *e*-business. It aims to improve regulation affecting communications across the European Union by "reducing, harmonising and collaborating across all aspects." See Anon 2005 *Accountancymagazine.com* 73.

and retention of communications data for the purposes of investigations, detection and prosecution of serious crime.[479]

Several European Union member states have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection and prosecution of crime and criminal offences. The provisions of the various national legislations vary considerably. The legal and technical differences between national provisions concerning the retention of data for the purposes of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications. Service providers are faced with different requirements regarding the types of traffic data to be retained, as well as the conditions and the periods of retention.

The Declaration on combating Terrorism adopted by the European Council on 25 March 2004 instructed the European Council to examine measures for establishing rules on the retention of communications traffic data by service providers. Common measures related to the retention of electronic communications traffic data at a European level were called for. The retention of data has proven to be a necessary and effective investigative tool for law enforcement in investigations in several member states and in particular into serious cases such as organised crime and terrorism. It is considered necessary to ensure the availability of retained data to law enforcement for a certain length of time. The adoption of an instrument on the retention of data is therefore a necessary measure in accordance with the requirements of article 8 of the European Convention on Human Rights.

The European Union Data Retention Directive is aimed at harmonising the following elements:

(a) the types of data to be retained;

(b) the length of time for which the data should be retained; and

(c) the purposes for which the data may be supplied to competent authorities.

The European Union Data Retention Directive also provides for an obligation on Internet service providers to retain the data in such a way that they can co-operate with the competent authorities without undue delay, whilst leaving it to member states to determine which authorities are competent under national legislation. Finally, the European Union Data Retention Directive also provides for the principal reimbursement of the additional cost incurred by the network and service providers to comply with the obligations imposed on them as a

---

479 Bramwell 2006 *Privacy and Data Protection* 11.

consequence of this Directive. This is an essential element to ensure that there is no market distortion through the application of different national cost reimbursement schemes.

The categories of data to be retained, as detailed in article 4 of the European Union Data Retention Directive, are data necessary to identify the source;[480] destination;[481] date, time and duration of a communication;[482] the type of communication;[483] the communication device or what purports to be the communication device;[484] and the location of mobile communication equipment.[485] This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to content data. Retention of data should be done in a way that avoids a situation where data is retained more than once. Generating or processing data, when supplying the communications services concerned refers to data which is accessible. In particular, when retaining data related to Internet email and Internet telephony, the scope may be limited to the providers' own services or the network providers' own services.

Member states must ensure that these categories of data are retained for periods no less than six months and a maximum of two years from the date of the communication.[486] Content is specifically excluded from the operation of the European Union Directive.[487] Access to data must be provided in accordance with national legislation.[488] Minimum data security principles are prescribed in respect of data retained in accordance with the present Directive.[489]

---

480 Concerning fixed network telephony and mobile telephony, this refers to the calling telephone number and the name and address of the subscriber or registered user; concerning Internet access, Internet email and Internet telephony this refers to the user ID's allocated, the user ID and telephone number allocated to any communications entering the public telephone network; the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication. See article 4(1)(a) of the European Data Retention Directive.

481 Concerning fixed network telephony and mobile telephony this refers to the numbers dialled (the called telephone number or numbers) and in cases involving supplementary services such as fall forwarding or call transfer, the number or numbers to which the call is routed and the names and addresses of the subscriber or registered users. Concerning Internet email and Internet telephony, this refers to the user ID or telephone number of the intended recipient of an Internet telephony call and the names and addresses of the subscribers or registered users and the user ID of the intended recipient of the communication. See article 4(1)(b) of the European Data Retention Directive.

482 Concerning fixed network telephony and mobile telephony, this means the date and time of the start and end of the communication. Concerning Internet access, Internet email and Internet telephony this refers to the date and time of the log-in and log-off of the Internet Access service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet Access Service provider to a communication and the user ID Or the subscriber or registered user; and the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service based on a certain time zone. See article 4(c) of the European Data Retention Directive.

483 Concerning fixed network telephony and mobile telephony this refers to the telephone service used and concerning Internet email and Internet telephony the Internet service used. See article 4(1)(d) of the European Union Data Retention Directive.

484 Concerning fixed network telephony this refers to the calling and called telephone numbers and concerning mobile telephony this refers to the calling and called telephone numbers, the IMSI (International Mobile Subscriber Identity) and the IMEI (International Mobile Equipment Identity) of the calling party and of the called party. In the case of prepaid anonymous services, it refers to the date and time of the initial activation of the service and the location label (Cell ID) from which the activation was made. Concerning Internet access, Internet email and Internet telephony this refers to the calling telephone number for dial-up access and the digital subscriber line (DSL) or other end point of the originator of the communication. See article 4(1)(e) of the European Data Retention Directive.

485 This refers to the location label (Cell ID) at the start of the communication and to data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data is retained.

486 Article 7 of the European Data Retention Directive.

487 See articles 1 and 4(2) of the European Union Data Retention Directive.

488 Article 3(bis) of the European Union Data Retention Directive.

489 Article 7(bis) of the European Union Data Retention Directive.

The European Union general Directive 95/46/EC and the specific requirements of Directive 2002/58/EC for the processing of personal data and the protection of privacy in an electronic communication medium provide that traffic data[490] must be erased or made anonymous when it is not needed for the purposes of the transmission or necessary for billing purposes. Prior to the Data Retention Directive, article 15 of Directive 2002/58/EC provided European Union member states with a data retention measure for a limited period of time if it is a "necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". It also states that the retention of data must be in accordance with the European Convention on Human Rights.

Mandatory blanket retention of data result in the data of all users' are being kept irrespective of whether they are suspected of committing a crime and this may be in conflict with the protection of human rights.[491] However, human rights such as the freedom of expression and privacy are not absolute and may be infringed if justifiable.

The mandatory retention of traffic data for a fixed length of time imposes huge and even infeasible obligations on the Internet Service Provider.[492] The difficulty with introducing a mandatory general retention of traffic data is that not only the "fingerprints" of an extremely small minority of a population are being kept, namely those of suspected criminals, but also those of a whole population to whom no suspicion is attached. At the very least, the emerging regulations on the mandatory general retention of traffic data create an unpredictable legal framework and should be the subject of a more refined legal debate.[493]

6.5 Brouter[494] to chapter 7

The main objective of this study is to consider whether the South African search and seizure, production and preservation mechanisms, when directed at electronic evidence, need to be augmented and/or aligned in accordance with those set out in the Cybercrime Convention. In serving this objective, this chapter was firstly aimed at providing an overview of the different domestic search and seizure, production and preservation procedural mechanisms available in

---

490 Article 2 of the E-Privacy Directive 2002/58/EC defines "traffic data" as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

491 Goemans and Dumortier *Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and Online Anonymity"* 167.

492 Goemans and Dumortier *Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and Online Anonymity"* 166.

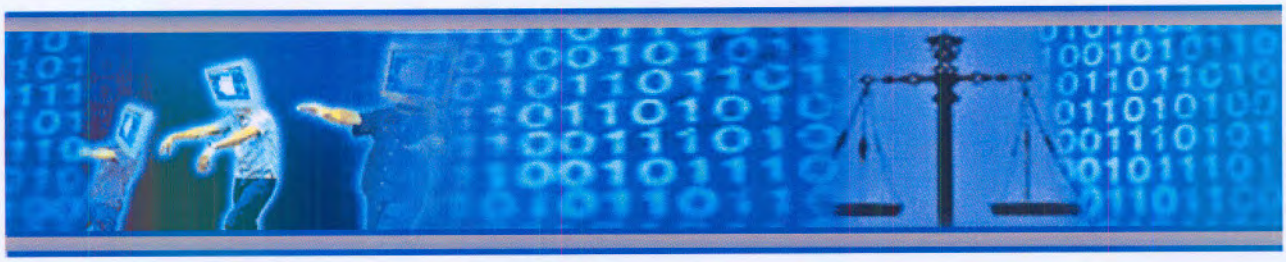
493 Goemans and Dumortier *Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and Online Anonymity"* 167.

494 Some of the most important findings that can be extracted from the snapshots provided of the different catalogues of search and seizure, production and preservation mechanisms available in the legislative frameworks of England are referred to in chapter 7.

the English legislative framework. Secondly, this exposition sought to illustrate the application of the equivalent English domestic search and seizure, production and preservation mechanisms, when directed at electronic evidence. Precedents regarding the application of these equivalent mechanisms in England are considered instructive for the South African context.

The rationale for this chapter was essentially to enable a contextually comparative troubleshooting utility in respect of the application of these procedural mechanisms to electronic evidence in South Africa. It is therefore not considered an objective in itself to juxtapose the devices proposed in the Cybercrime Convention to those available within the current English catalogue of search and seizure, production and preservation mechanisms. The findings relevant for the primary objectives of this research are pointed out in chapter 7.

CHAPTER 7:
SEARCH HITS, CURSORS AND SHUT-DOWN



7.1 SEARCH ENGINE QUERY 381

7.2 SEARCH HITS 382

7.2.1 A technical contextualisation 382
7.2.1.1 Computer data 383
7.2.1.2 Electronic evidence 383
7.2.1.3 Computer forensics and anti-forensics 384
7.2.1.4 Evidence collection mechanisms 384
7.2.1.5 Surfing the Third Wave 386
7.2.2 Search and seizure, production and preservation @ the Cybercrime Convention 387
7.2.2.1 Domestic search and seizure, production and preservation devices 387
7.2.2.2 Transborder search and seizure, production and preservation devices 391
7.2.2.3 Declarations 395
7.2.2.4 Reservations 396
7.2.3 South African search and seizure, production and preservation mechanisms compared to the mechanisms proposed by the Cybercrime Convention 397
7.2.3.1 Domestic search and seizure, production and preservation devices 397
7.2.3.2 Transborder search and seizure, production and preservation devices 408
7.2.3.3 Declarations 416
7.2.3.4 Reservations 416
7.2.4 Search and seizure, production and preservation troubleshooting @ the United States and England 417
7.2.4.1 Right to privacy 418
7.2.4.2 Unconstitutionally obtained evidence 419
7.2.4.3 Domestic search and seizure devices 420
7.2.4.4 Domestic production devices 424
7.2.4.5 Domestic data preservation devices 426

7.3 CURSORS 427

7.4 SHUTDOWN 431

7.1 Search engine query[1]

Today criminals are becoming increasingly involved in computing activity and connectivity, and it seems that the criminal justice field just cannot keep pace. In order to meet the challenges of computer-related crime, the bottom line is that even technophobes must be become part of the Third Wave, not least law enforcement practitioners. Being comfortable with the technology that underpins the Information Age is a non-negotiable skill for those who have to investigate twenty-first century crimes and crime scenes

> As long as we live in a world where a 17th Century philosophy of sovereignty is reinforced with an 18th Century judicial model, defended by a 19th Century concept of law enforcement that is still trying to come to terms with 20th Century technology, the 21st Century will belong to transnational criminals.[2]

An understanding of the technicalities involved in the collection of electronic evidence begins with knowing that you know not. This notion, coupled with the aspiration to remain relevant and meaningful in the Third Wave, poses a severe challenge to protagonists of the legal process. In order to assist law enforcement practitioners to meet some of these challenges, chapter two of this study attempted to acquaint the reader with the exceedingly complex technologies involved in computers and networks, to provide a technical contextualisation of the research parameters and to clarify terminology typical of the collection of electronic evidence.[3]

At present, the Cybercrime Convention is the only existing internationally agreed upon benchmark for, *inter alia*, the procedural powers aimed at the collection of electronic evidence. The main objective of this study was to consider whether the South African search and seizure, production and preservation mechanisms, when directed at electronic evidence, need to be augmented and/or aligned in accordance with the mechanisms set out in the Cybercrime Convention.

---

1 A search engine is a software program that searches for data based on some criterion and that gathers and reports information that contains or is related to specified terms. Search engines can differ dramatically in the way that they find and index relevant material and the way that they conduct a search based on the user's query. A search engine is a program designed to help find information stored on, for example, the WWW or a personal computer. The search engine allows a user to ask for content meeting specific criteria, on the basis of which it then retrieves a list of references that match those criteria. Although a search engine is technically the software and algorithms used to perform a search, the term has become synonymous with the web site itself (the Google search site is, for example, commonly called the Google search engine). The very first tool used for searching on the Internet was called "Archie" and was created in 1990. Others include Gopher, Veronica, Jughead, Wandex, Aliweb, WebCrawler, Lycos, Excite, Infoseek, Inktomi, Northern Light, Altavista, Yahoo! Search, MSN Search. See Answers.com "Search engine" found on the Internet http://www.answers.com/topic/search-engine 2-7. In this context, it briefly reiterates the main objective of this thesis (as stated in paragraph 1.2 above).

2 Geoffrey Robinson quoted in Jones 2001 *Computer Fraud and Security* 6.

3 The principal findings that can be extracted from this contextualisation are listed in paragraph 7.2.1 below.

This objective was served by first providing[4] an exposition of the requirements, scope and conditions and safeguards of the domestic and transborder search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention.[5] This exposition constitutes the yardstick against which to measure South Africa's compliance with the requirements in respect of search and seizure, production and preservation proposed in the Cybercrime Convention.

Next, the requirements, scope and conditions and safeguards of the domestic and transborder search and seizure, production and preservation devices available within the current South African legislative framework were presented.[6]

This exposition, coupled with the exposition of the search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention, facilitated a comparative analysis between the catalogue of criminal procedural search and seizure, production and preservation devices proposed by the Cybercrime Convention compared to the devices available within the current South African legislative framework.[7]

In considering any alignments and/or augmentations required in respect of the South African search and seizure, production and preservation mechanisms, the application of the equivalent domestic search and seizure, production and preservation mechanisms directed at electronic evidence used in the United States and England were considered in chapters 5 and 6 respectively.[8]

7.2 *Search hits*[9]

7.2.1 *A technical contextualisation*[10]

The findings extracted in respect of the overview provided in chapter 2 of the technicalities and terminology underpinning the deployment of search and seizure, production and preservation mechanisms proposed in the Cybercrime Convention and the devices available within the

---

4 In chapter 3 of this study.
5 The principal findings that can be extracted from this exposition are set out in paragraph 7.2.2. below.
6 In chapter 4 of this study.
7 The principal findings that can be extracted from this comparative analysis are presented in paragraph 7.2.3 below.
8 The principal findings that can be extracted from these overviews are presented in paragraph 7.2.4 below.
9 In this context, search hits are meant to refer to the extracted findings with regard to the main objective of this research (see the search engine definition in paragraph 7.1 above). See footnote 126 in paragraph 1.3 above for a definition of a "search hit".
10 In contextualising the technicalities and terminology underpinning the deployment of search and seizure, production and preservation procedural devices in computing environments, care was taken to root the legalities associated with these technicalities in the Cybercrime Convention and the relevant legislative provisions in South African law. The rationale for this was to facilitate a comparative analysis between the mechanisms available in current South African law compared to the mechanisms proposed in the Cybercrime Convention (see paragraph 7.2.3 below in this respect).

current South African legislative framework are listed below.

7.2.1.1 Computer data[11]

(a) Information has become digitised and dematerialised.

(b) Computer data, as the object of collection interventions, encompasses any electronic representation of information that is suitable for processing by a computer and, as such, is capable of being reduced to binary.

(c) Computer data may exist in two forms, namely:

(i) static, recorded or stored; or

(ii) fluid, in flux or movement or in the process of communication.

(d) The definition of computer data includes three specific types of communications data, namely:

(i) content data;

(ii) traffic data or communication-related information; and

(iii) subscriber information.

(e) It is important to distinguish between different types of computer data, because the Cybercrime Convention and the relevant provisions in the South African Criminal Procedure Act and the RICPCIA introduce different legal collection regimes for each type of data. The applicability of an evidence collection mechanism to a particular type or form of data depends on the nature and form of the data that is to be collected.

7.2.1.2 Electronic evidence[12]

(a) It is imperative to appreciate that when a law enforcement officer searches for and seizes electronic evidence, it is not simply a matter of transporting hardware from a crime scene to an evidence storage facility. Similarly, when the production or preservation of electronic evidence is requested, the process does not merely involve handing over or isolating hardware.

(b) Electronic evidence is probative binary data stored or transmitted by means of a computer system, and admissible as evidence in a court of law.

(c) Although the emphasis in this research was on the legal procedures designed to collect electronic evidence and not electronic evidence *per se*, it is important to appreciate that computer data is a new form of evidence that requires special consideration with regard to its collection, preservation and presentation.

---

11 See paragraph 2.2.1 above.
12 See paragraph 2.3.1 above.

(d) Electronic evidence constitutes the ultimate objective of any evidence collection intervention directed at computing environments.

7.2.1.3 Computer forensics[13] and anti-forensics[14]

(a) Computer forensics refers to the process of unearthing evidence from computer media in order to support legal proceedings. The objective in computer forensics is to recover, analyse and present computer-based material in such a way that it is successfully admitted as evidence in a court of law.

(b) Computer forensics provides the contemporary solution of choice by means of which computer data is collected and presented as electronic evidence.

(c) Anti-forensic techniques refer to the intentional or accidental changing of data that can obscure the data, encrypt it or hide it from forensic tools. Two of the most prevalent anti-forensic techniques are obscurity methods (such as file extension renaming, encoding, compression obscurity methods, data stored in slack, unallocated, and free space) and privacy measures (encryption, steganography, evidence eliminators and disk-wiping).

(d) Although this research focused on the legal procedures by means of which electronic evidence is collected, the legalities cannot be divorced from the technicalities associated with the unearthing of such *e*-evidence. A broad understanding of both the technical procedures and the tools used to collect electronic evidence, and of the techniques employed to counter such collection is required.

7.2.1.4 Evidence collection mechanisms[15]

(a) The approach taken by the international legal community, as reflected in the Cybercrime Convention, and also adopted for the purposes of this thesis, is to develop, supplement and continue to apply existing legal devices. The collection of electronic evidence is typically facilitated by means of the legal mechanisms of interception and monitoring, search and seizure, production, preservation and retention.

(b) In most jurisdictions, the powers of interception and monitoring of communications have traditionally been seen as more intrusive than the powers of searching and seizing. Content data is generally also more jealously guarded than, for example, traffic and subscriber data. In their turn, the powers to request and/or order the production or preservation of information could arguably be considered less of an infringement of the right to privacy than the powers of search and seizure. Consequently, the law has

---

13 See paragraph 2.3.1.2 above.
14 See paragraph 2.3.1.3 above.
15 See paragraph 2.4 above.

gradually evolved into different legal powers, emanating from different legal regimes, to protect different facets of the right to privacy.

(c) Interception and monitoring is directed at data that is fluid and in movement. It entails collecting data in currently generated communications which are collected at the time of the communication. Such data is, generally, in the process of being created at the time when it is gathered. The gathering of real-time data takes place during a certain period, in respect of data that will be created or, if the data has already been created and recorded, will be transmitted at a particular time or period in the future. References to interception and monitoring, for the purposes of this study, were made only to elucidate the search and seizure of electronic evidence.

(d) Search and seizure is directed at any computer data, including all forms of communications data, provided that such data is static, recorded and stored. Search and seizure is concerned with data that has been recorded or registered in the past, either in tangible or in intangible form, and the gathering of this data takes place at a single moment in time, in other words, the period of the search, and in respect of data that exists at that time.

(e) The distinction between search and seizure and interception and monitoring is based on the format and inertness of the data at the time when it is gathered. Data that is static, recorded and stored is acquired by means of a search and seizure intervention. However, if the data is fluid and in movement, acquisition is accomplished by means of an interception and monitoring intervention.

(f) Production is the submission or handing over of data under legal compulsion.

(g) Preservation is the activity that keeps existing, stored data secure and safe.

(h) Retention is the process of storing data which is currently being generated and the keeping or possession of such real-time data into a future period. References to data retention, for the purposes of this study, were made only to elucidate the preservation of electronic evidence.

(i) It is important to distinguish between the different legal collection mechanisms provided for in the Cybercrime Convention and in the relevant provisions in the South African Criminal Procedure Act and the RICPCIA. While the end result remains the acquisition of data, the preconditions for use, the accompanying safeguards and the scope of these different coercive powers differ.

(j) The applicability of an evidence collection mechanism depends on the nature and form of the data to be collected. For the purposes of this thesis, computer data is studied as the object of a search and seizure, production and preservation intervention. This implies that for the purposes of this study, the computer data referred to is static, recorded and stored.

(k) However, due to its definition in section 1 of the RICPCIA, "real-time communication-related information" could technically already have been stored by a telecommunications service provider for a period of 90 days. This definition of real-time communication-related information obscures the meaning given to "stored" (as opposed to "real-time") computer data in the Cybercrime Convention to some extent. For the purposes of this study, real-time communication-related information was considered to the extent that it overlaps with the concept of stored computer data as *per* the Cybercrime Convention. This research was not essentially concerned with data in transit (real-time) data but, instead, with the search and seizure, production and preservation of stored computer data.

7.2.1.5 Surfing the Third Wave[16]

(a) Being comfortable with the technology underpinning twenty-first century crimes and crime scenes is a non-negotiable skill for practitioners who need to address information technology crimes. A broad understanding of the computer systems, categories of computer systems and computing environments targeted for *e*-evidence collection purposes is essential. To use an analogy: being stuck in a world where bartering is the dominant mode when trying to penetrate to the heart of modern financial crimes leaves an investigator clueless – a basic appreciation of payment systems and current legal tender is essential.

(b) A computer system is a device or group of related devices that automatically processes data. Computer systems consist of hardware and software. Software can be divided into application software and system software. System software consists mainly of utility programs and operating systems. The storage portions of the computer system, where both the data and programs are located, are primarily where electronic evidence is located. The storage portions of a computer system are, therefore, predominantly what collection mechanisms are directed at. Storage can be divided into primary storage (such as RAM, ROM, memory cache, CMOS, flash memory, expansion slots and expansion cards) and secondary storage (such as floppy disks and diskettes, hard disks, CD's, memory sticks, tape, enterprise storage systems, PC Cards, miniature mobile storage media, microfilm and microfiche).

(c) Computer system categories cannot be demarcated precisely, but are generally categorised on the basis of differences in their size, speed, processing capabilities and price. The six main categories of computers are personal computers (desktops and laptops), handheld computers, information appliances, servers, mainframes and supercomputers.

---

[16] See paragraphs 2.5 and 2.6 above.

(d) The environment associated with computers that are targeted for electronic evidence collection has a vital impact, *inter alia*, on the way the collection is done, the collection potential and the human resources needed to conclude the collection of the sought-after electronic evidence successfully. A computer system may be stand-alone or may be connected to a network with other similar devices.

(e) Networks are complicated structures with many interrelated parts and, as such, pose considerable challenges when they are targeted for evidence collection purposes. Computer networks can be server-based or peer-to-peer, or they can consist of a hybridised combination of the two types. Different categories of computer networks include LANs, WANs, MANs, SANs, home networks, VPNs, intranets and extranets. The world's most famous and largest WAN is the Internet. The Internet is constructed of different services (such as the WWW, email, FTP, newsgroups, message boards, mailing lists, chat rooms and IM) that are offered to its users.

7.2.2 Search and seizure, production and preservation @ the Cybercrime Convention

The findings extracted from chapter 3 in respect of the search and seizure, production and preservation mechanisms proposed in the Cybercrime Convention are listed below.

7.2.2.1 Domestic search and seizure, production and preservation devices[17]

7.2.2.1.1 General findings

(a) The domestic search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention must be aimed at stored computer data. In addition, production orders are to be aimed at two particular types of stored computer data, namely specified stored computer data and subscriber information in the possession or control of a person or service provider respectively (only to the extent that the person or service provider maintains the required data or information).

(b) The scope of the domestic search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention are subject to article 14 of the Cybercrime Convention. This translates into:

(i) mechanisms that must be directed at specific criminal investigations or proceedings; and

(ii) mechanisms that must be capable of application to **any** criminal offence (including those offences established in terms of the Cybercrime Convention, and any other criminal offences committed by means of a computer system).

---

[17] See paragraphs 3.3, 3.5 and 3.7 above.

(c) Article 22 of the Cybercrime Convention requires parties to establish jurisdiction over the criminal offences created in articles 2 to 11 of the Cybercrime Convention on the basis of the principles of:

(i) territoriality, if the crimes are committed in its territory, or on ships flying its flag, or aircraft registered under its laws; and

(ii) nationality, by obliging the nationals of a member state to comply with its domestic law, even when they are outside its territory and if the conduct is also an offence under the law of the state in which the offence is committed, or if the conduct has taken place outside the territorial jurisdiction of any state.

These bases of jurisdiction are not exclusive and any other bases of jurisdiction in conformity with the domestic law of a member state are permitted.

(d) The domestic search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention are subject to certain conditions and safeguards embodied in article 15 of the Cybercrime Convention. This translates into the following:

(i) the mechanisms must generally be subject to the conditions and safeguards provided for under the domestic law of each party (including the right against self-incrimination, legal privileges and the specificity of individuals or places that are the object of the application of the mechanisms);

(ii) the mechanisms must generally be subject to some common standards or minimum safeguards aimed at balancing the interests of law enforcement on the one hand, and respect for fundamental human rights on the other, arising pursuant to obligations undertaken by a party under applicable international human rights instruments (including the right of everyone to hold opinions without interference; the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers; and the right to privacy);

(iii) the mechanisms must specifically be subject to (judicial or other independent) supervision by competent authorities, *inter alia*, to consider the grounds justifying the application of the mechanisms and the limitation on its scope and duration;

(iv) the mechanisms must specifically incorporate the principle of proportionality in accordance with the relevant principles of the domestic law of a party (such as reasonableness requirements for searches and seizures, limitations on overly broad search warrants and production orders and the limitation on coerced cooperation with the provision of information that is reasonably necessary to enable a search and seizure intervention);

(v) the mechanisms must specifically bring into the equation, to the extent consistent with the public interest and, particularly, the sound administration of justice, the impact of the mechanisms upon the rights, responsibilities and legitimate

interests of third parties, and the means to mitigate such an impact (including the means to minimise a disruption to consumer services, the protection of proprietary interests, protection from liability for disclosure, the engagement and financial compensation of witnesses and experts, and notification of a surreptitious search and seizure intervention without prejudicing the investigation);

(vi) in respect of preservation and production mechanisms, parties must specifically introduce an additional obligation of confidentiality; and

(vii) in respect of production mechanisms, privileged data or information may specifically be excluded from the application of production orders.

7.2.2.1.2 Findings specific to domestic search and seizure mechanisms

(a) Article 19 of the Cybercrime Convention provides for the procedural power at a national level to search and seize stored computer data. This domestic search and seizure mechanism must meet the following requirements:

(i) it must be equivalent to the power to search and seize tangible objects;

(ii) it must provide a comprehensive legal authorisation to search, copy or access computer data which is contained either within a computer system or a part of it, or in any related computer storage medium in the vicinity;

(iii) it must provide a comprehensive legal authorisation to seize or secure a computer system (or parts thereof) and independent storage media; and it must also allow for the copying, rendering inaccessible or removal of data whilst maintaining its integrity;

(iv) it must allow for an extension of the search or access by establishing a connection from a legally accessed computer system to other computer systems (or parts thereof) within the same territory, if reasonable grounds exist to believe that the data required is stored in such other computer systems (or parts thereof); and

(v) it must induce coerced cooperation for the purposes of enabling a search and seizure, if the circumstances reasonably permit.

7.2.2.1.3 Findings specific to domestic expedited preservation and partial disclosure mechanisms

(a) The importance of the distinction between preserved and retained computer data in the Cybercrime Convention is evident from, *inter alia*, the fact that articles 16 and 17 only refer to data preservation and not to data retention. This thesis is essentially concerned with data preservation. Data retention is considered relevant to the extent that it may supplement the expedited preservation of stored computer data and the expedited

preservation and partial disclosure of stored traffic data, as *per* articles 16 and 17 of the Cybercrime Convention.

(b) Article 16 of the Cybercrime Convention provides for the procedural power at a national level to expeditiously preserve stored computer data, up to a maximum of 90 days (subject to a renewal of the order), to enable competent authorities to seek its disclosure.

(c) Preservation simply requires that data which already exists in a stored form be kept safe from modification, deterioration or deletion.

(d) Other legal methods of achieving preservation are allowed, including production orders and search and seizure warrants that simultaneously facilitate the disclosure of the data to law enforcement agents. It is, however, recommended that parties consider establishing powers and procedures to actually order the recipient of the preservation order specifically to preserve the data.

(e) Article 17 of the Cybercrime Convention provides for the expeditious disclosure of some traffic data preserved in terms of article 16 of the Cybercrime Convention, so as to identify other service providers involved in the transmission of specified communications. Examples of such expeditious preservation mechanisms include the following:

(i) a series of separate preservation orders, to be served expeditiously on each service provider involved;

(ii) a single comprehensive preservation order, to be served sequentially, the scope of which would apply to all service providers identified subsequently as being involved in the transmission of that particular communication; or

(iii) participatory preservation orders and cumulative notices which require a service provider served with an order to notify the next service provider in the chain of the existence and terms of the preservation order.

7.2.2.1.4 Findings specific to domestic production mechanisms

(a) Article 18(1)(a) of the Cybercrime Convention provides for the procedural power at a national level to order a person in a party's territory to submit specified computer data stored in a computer system, or a data storage medium that is in that person's possession or control.

(b) Article 18(1)(b) of the Cybercrime Convention provides for the procedural power at a national level to order a service provider offering services in a party's territory to submit subscriber information in the service provider's possession or control.

(c) Article 18 of the Cybercrime Convention is applicable only to the extent that the person or service provider maintains the required data or information.

(d) Real-time traffic data and real-time content data cannot be acquired by means of an article 18 production order.

7.2.2.2 Transborder search and seizure, production and preservation devices[18]

7.2.2.2.1 General findings

(a) In terms of articles 23 and 25(1) of the Cybercrime Convention, international cooperation is to be provided among parties to the widest extent possible and impediments thereto (such as reservations, postponements and the imposition of conditions to the provision of assistance) must be strictly limited.

(b) The Cybercrime Convention does not create a separate general mutual assistance regime in *lieu* of existing mutual legal assistance frameworks (based on relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws):

(i) in respect of general matters, the parties to the Cybercrime Convention should in principle apply such other existing treaties or arrangements; and

(ii) in respect of specific matters dealt with only by the Cybercrime Convention, the parties should give precedence to the rules contained in the Cybercrime Convention.

(f) Article 25(2) of the Cybercrime Convention requires all parties to have a legal basis to carry out certain specific forms of cooperation if its treaties, laws and arrangements do not already contain such provisions. These specific minimum forms of cooperative measures are:

(i) the expedited preservation of stored computer data;

(ii) the expedited disclosure of preserved traffic data;

(iii) the accessing of stored computer data;

(iv) the transborder access to stored computer data with consent or where publicly available;

(v) the real-time collection of traffic data;

(vi) the interception of content data; and

(vii) the maintenance of a 24 hour, 7 day a week network.

(g) The parties must allow for making and attending to urgent mutual assistance requests through expedited means of communications rather than through the traditional transmission of written, sealed documents through diplomatic pouches or mail delivery systems.

---

[18] See paragraphs 3.4, 3.6 and 3.8 above.

(h) The grounds on which parties may refuse co-operation are those provided for in the domestic law of the requested party and in applicable mutual assistance treaties. Mutual assistance in respect of the offences referred to in articles 2 to 11 of the Cybercrime Convention may, however, not be refused solely on the ground that the request concerns an offence which it considers a fiscal offence.

(i) By agreement between parties or in the absence of a mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, the provisions of article 27 of the Cybercrime Convention in respect of issues expressly covered by it must be applied in *lieu* of otherwise applicable domestic laws governing mutual assistance. Issues covered by article 27 include the following:

(i) the establishment of a central authority or authorities in all member states that, as a general rule, communicate directly with each other in respect of sending, answering, executing or transmitting for execution any mutual legal assistance requests;

(ii) direct communication between the judicial authorities of the requesting and requested parties or Interpol in respect of both urgent mutual legal assistance requests and mutual legal assistance requests that can be complied with by the requested party without using coercive action;

(iii) an obligation on the requested party to execute requests in accordance with the procedures specified by the requesting party, unless to do so would be incompatible with its own law;

(iv) the keeping intact of the fundamental legal requirements of the requested party in executing a coercive power on behalf of a requesting party;

(v) the guarding of the confidentiality of the fact and content of the request in particularly sensitive cases, or in cases in which there could be disastrous consequences if the facts underlying the request were to be made public prematurely;

(vi) grounds for refusal and/or postponement of or qualified execution of mutual legal assistance requests –

- assistance may be refused where the execution of the request is likely to prejudice the sovereignty of the State, security, *ordre public* or other essential interests,
- assistance may be refused where the requested party considers the offence to be a political offence or an offence connected with a political offence,
- a requested party may postpone (rather than refuse) assistance where immediate action in response to the request would be prejudicial to investigations or proceedings in the requested party,

- where the assistance sought would otherwise be refused or postponed, the requested party may instead provide assistance subject to conditions, and
- reasons must be provided if a request is refused or postponed.

(j) The transborder search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention must be aimed at stored computer data. The spontaneous production of information under article 26 of the Cybercrime Convention is, however, not limited to stored computer data, but includes any information obtained within the framework of investigations carried out by the party forwarding the information.

(k) Article 25(1) of the Cybercrime Convention requires that transborder search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention must be capable of application to **any** criminal offence (including those offences established in terms of the Cybercrime Convention and any other criminal offences committed by means of a computer system).

(l) Article 22(5) of the Cybercrime Convention provides for consultation, with a view to determining the most appropriate jurisdiction for prosecution(s), when more than one party claims jurisdiction over an offence.

(m) The transborder search and seizure, production and preservation mechanisms proposed by the Cybercrime Convention are subject to the following conditions and safeguards:

(i) the mechanisms are subject to the conditions provided for by applicable mutual assistance treaties and domestic laws;

(ii) the mechanisms will not be executed on behalf of a requesting party, unless the requested party's fundamental domestic requirements are satisfied;

(iii) the condition of dual criminality must, however, be deemed to have been fulfilled, irrespective of whether a requested party's laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting party, as long as the conduct underlying the offence for which assistance is sought is a criminal offence under its laws;

(iv) in addition to this liberal definition of dual criminality, article 29(3) of the Cybercrime Convention sets out the general rule that parties must dispense with any dual criminality requirement with regard to preservation orders due to the volatility of data;

(v) a requesting party must be promptly informed if a preservation order will not ensure the future availability of the required data, or will threaten the confidentiality of, or otherwise prejudice the investigation of the requesting party;

(vi) article 28(2)(a) allows the requested party, when responding to a request for mutual assistance, to request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such a condition;

(vii) article 28(2)(b) provides that the requested party may also make the furnishing of the information or material dependent on the condition that it may not be used for investigations or proceedings other than those stated in the request;

(viii) two exceptions to the ability to limit use and ensure confidentiality are considered implicit in the terms of article 28(2), namely that evidence exculpatory to an accused person must be disclosed to the defence or a judicial authority and that once the material furnished has been used at trial (normally a public proceeding and including compulsory disclosure) it has essentially passed into the public domain;

(ix) the execution of mutual legal assistance requests may be refused, postponed or made subject to the following conditions:

- assistance may be refused where the execution of the request is likely to prejudice the sovereignty of the State, security, *ordre public* or other essential interests;
- assistance may be refused where the requested party considers the offence to be a political offence or an offence connected with a political offence;
- the assertion of any other basis (other than the two listed in the two preceding bullets) for refusing a mutual legal assistance request for the preservation of traffic data is precluded; and
- refusal of assistance on data protection grounds may be invoked only in exceptional cases, and a broad, categorical, or systematic application of data protection principles to refuse cooperation is precluded.

7.2.2.2.2 Findings specific to transborder search and seizure mechanisms

(a) Articles 31 and 32 of the Cybercrime Convention provides for the procedural power at an international level to search and seize stored computer data. This transborder search and seizure mechanism must meet the following requirements:

(i) it must (through the application of international instruments on international cooperation in criminal matters, arrangements agreed upon the basis of uniform or reciprocal legislation and domestic laws) enable the search and seizure of computer data located within its national territory, on behalf of another party;

(ii) it must enable an expedited search and seizure for the benefit of another party, where there are grounds to believe that the relevant data is particularly vulnerable to loss or modification, or otherwise where the relevant treaties, arrangements or laws provide for such expedited cooperation; and

(iii) it must allow for the unilateral access through a computer system in a party's own territory to computer data in the territory of another party (without that party's

authorisation) if the required data is open source stored computer data, or if a party has obtained the lawful and voluntary consent of a person authorised to disclose the data.

7.2.2.2.3 Findings specific to transborder preservation and partial disclosure mechanisms

(a) The transborder expedited preservation of stored computer data, for a period of no less than 60 days, is facilitated by means of article 29 of the Cybercrime Convention, pending the lengthier and more involved process of executing a formal mutual assistance request that will facilitate its actual disclosure.

(b) A requested party may use other legal methods, including the expedited issuance and execution of a production order or a search warrant for the data to ensure the rapid preservation of computer data. The preferred procedure is, however, that the requested party ensures that the custodian preserve the data, and not necessarily obtain possession of the data from its custodian.

(c) The transborder expedited disclosure of preserved traffic data is facilitated by means of article 30 of the Cybercrime Convention. A party requested to expeditiously preserve traffic data concerning a specific communication may be requested to disclose to the requesting party a sufficient amount of traffic data to identify service providers in, and the paths of the communication from, other territories.

7.2.2.2.4 Findings specific to transborder spontaneous production mechanisms

(a) Article 26 of the Cybercrime Convention empowers the party in possession of valuable information to forward it to the other party without a prior request if it believes such information may assist another party in a criminal investigation or proceeding.

(b) The confidentiality of information spontaneously forwarded in terms of article 26 of the Cybercrime Convention may be one of the conditions that can be imposed on the use of such information.

7.2.2.3 Declarations[19]

(a) A declaration is an acceptable interpretation of the provisions of the Cybercrime Convention and permits the inclusion of certain specified additional elements. The declaration provided for in article 27(9)(e) of the Cybercrime Convention is relevant to this study.

---

[19] See paragraph 3.2.5 above.

(b) Article 27(9)(e) of the Cybercrime Convention provides that a party may require that, for reasons of efficiency, urgent requests made under article 27(9) must also be addressed to its central authority and may not be made directly to its judicial authorities.

7.2.2.4 Reservations[20]

(a) A reservation permits the exclusion or modification of the legal effect of certain obligations set out in the Cybercrime Convention so as to avoid conflict with a party's constitutional or fundamental legal principles. The reservations provided for in articles 14(3), 22(2), 29(4) and 41 of the Cybercrime Convention are relevant for the purposes of this research.

(b) Article 14(3) of the Cybercrime Convention provides that a party may reserve the right to apply the measures referred to in article 20 (the real-time collection of traffic data) only to offences or categories of offences specified in the reservation. The range of such offences or categories of offences specified in the reservation must not be more restricted than the range of offences to which it applies the measures referred to in article 21 (the interception of content data). Parties should, however, consider restricting such a reservation to enable the broadest possible application of the measure referred to in article 20.

(c) Article 22(2) of the Cybercrime Convention allows parties to enter a reservation to all of the jurisdiction grounds laid down in article 22(1), excluding the establishment of territorial jurisdiction under article 22(1)(a) and jurisdiction in cases falling under the principle of *aut dedere aut judicare* in article 22(3).

(c) Article 29(4) provides that a party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or the disclosure of the data, may reserve the right to refuse the request for the expedited preservation of stored computer data in cases where it has reason to believe that, at the time of disclosure, the condition of dual criminality cannot be fulfilled. This reservation applies only in respect of offences other than those established in accordance with articles 2 to 11 of the Cybercrime Convention.

(d) Article 41 of the Cybercrime Convention allows for a reservation that accommodates minor variations in its applicability, as a result of the well-established domestic law and practice of a party that is a federal state. The scope of application of the federal clause has been restricted to the provisions of chapter II of the Cybercrime Convention. Federal states entering this reservation are still obliged to cooperate with the other parties under chapter III of the Cybercrime Convention.

---

[20] See paragraph 3.2.5 above.

7.2.3 *South African search and seizure, production and preservation mechanisms compared to the mechanisms proposed by the Cybercrime Convention*

The exposition of the findings in respect of the search and seizure, production and preservation devices proposed in the Cybercrime Convention[21] can be used as the yardstick with which to measure South Africa's compliance with the relevant procedural requirements set out in the Cybercrime Convention. The findings that can be extracted from a comparative analysis between the South African search and seizure, production and preservation mechanisms proposed in the Cybercrime Convention are listed below.

7.2.3.1 Domestic search and seizure, production and preservation devices[22]

7.2.3.1.1 Findings specific to domestic search and seizure mechanisms

(a) The relevant domestic search and seizure mechanisms in the South African legislative framework are provided for in chapter 2 of the Criminal Procedure Act and chapter XII of the Electronic Communications and Transactions Act.

(b) General search and seizure warrants can be obtained under authority of section 21 of the Criminal Procedure Act. Warrants to maintain internal security and law and order can be obtained under authority of section 25 of the Criminal Procedure Act. Warrants can be issued to cyber inspectors in terms of section 83 of the Electronic Communications and Transactions Act.

(c) The warrantless search and seizure doctrines provided for in the Criminal Procedure Act include the following:

(i) consensual searches and seizures;

(ii) searches and seizures under exigent circumstances;

(iii) searches for the purposes of effecting an arrest;

(iv) searches of arrested persons;

(v) entering premises for the purpose of obtaining evidence; and

(vi) searches of premises reasonably suspected of housing stolen stock or produce.

(d) Article 19 of the Cybercrime Convention directs that the domestic search and seizure mechanisms are to be aimed at stored computer data, as opposed to flowing data in transfer (which is to be collected by means of an interception and monitoring intervention). This differentiation is also applicable to search and seizure *vis-à-vis* interception and monitoring mechanisms in South African law. Section 1(2)(b) of the

---

21 In paragraph 7.2.2 above.

22 See paragraphs 4.2, 4.4 and 4.6 above.

RICPCIA further clarifies the application of this distinction to computer data. It provides that indirect communications stored by a telecommunications system that transmits or has transmitted such indirect communications in a manner that enables the intended recipient to collect it or otherwise to have access to it is considered to be data in transfer. Access to such indirect communications must therefore be facilitated by means of an interception direction under the RICPCIA.

(e) Article 19 of the Cybercrime Convention requires that domestic search and seizure mechanisms aimed at computer data must be equivalent to the power to search and seize tangible objects. The South African Law Reform Commission found that chapter 2 of the Criminal Procedure Act would not apply to the search of a computer and the seizure of information located on that computer, although the seizure of a particular computer would be allowed. The provisions of the Criminal Procedure Act need to be aligned in order to solve problems with the restricting interpretations of the words "premises" and "article" as physical entities. This argument is reflected in section 82(4) of the Electronic Communications and Transactions Act that provides that, for purposes of that Act, any reference in the Criminal Procedure Act to "premises" and "article" includes an information system, as well as data messages. Sections 82 and 83 of the Electronic Communications Act also include technology-friendly phrases such as the following: the "accessing of an information system"; the "taking of extracts from or the making of copies of any documents or records in an information system"; and the "searching of data contained in or available to an information system".

(f) It could be argued that, for the word "article" at least, an alignment is unnecessary, due to the fact "anything" may be seized in terms of article 20 of the Criminal Procedure Act (the word "article" is referenced from the word "anything"). The specific insertion of section 82(4) of the Electronic Communications and Transactions Act by the legislature could, however, dictate against this supposition.

(g) Any statutory body with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector but cannot otherwise avail itself of a warrant issued in terms of section 83 of the Electronic Communications and Transactions Act. The existing search and seizure mechanisms provided for in the Criminal Procedure Act are the only mechanisms available to law enforcement officers. These criminal procedural mechanisms are routinely aimed at computer data in current law enforcement practice. The uncertainty pertaining to the applicability of the search and seizure mechanisms provided for in the Criminal Procedure Act to computer data and information systems is undesirable and must be addressed. It is submitted that this alignment is necessary, regardless of whether the cyber inspectors are, in fact, appointed at a future stage. It is untenable that all law enforcement efforts directed at electronic evidence be channelled via the cyber inspectorate. The appointment of cyber

inspectors is, however, supported on the basis of, *inter alia,* their envisaged mandate in respect of compliance monitoring under the Electronic Communications and Transactions Act. Also, a centralised cybercrime fighting capacity within government will contribute to economy of government effort (particularly for smaller law enforcement units that cannot invest in full-blown in-house computer forensic capacity).

(h) Article 19 of the Cybercrime Convention requires that domestic search and seizure mechanisms must provide a comprehensive legal authorisation to search, copy or access computer data which is contained either in a computer system or in a part of it, or in any related computer storage medium in its vicinity. The domestic search and seizure mechanisms must also provide a comprehensive legal authorisation to seize or secure a computer system (or parts thereof) and independent storage media. The copying, rendering inaccessible or removal of data whilst maintaining its integrity must also be made possible. Sections 82 and 83 of the Electronic Communications and Transactions Act comply with both these requirements, as detailed in article 19 of the Cybercrime Convention. The wording in section 7 of the South African Law Reform Commission's proposed Computer Misuse Bill addresses both these requirements. This proposed alignment could dictate against a finding that the existing search and seizure mechanisms provided for in the Criminal Procedure Act comply with these requirements. This issue is also linked to the uncertainty in respect of the applicability of these search and seizure mechanisms to computer data and information systems. A sufficiently broad, but nevertheless specific, warrant could, to some extent, address the need for a comprehensive legal authorisation to search and access or seizure and copy computer data. Any uncertainty in respect of the comprehensive application of the search and seizure mechanisms to computer data and information systems is, however, undesirable and must be addressed.

(i) Article 19 of the Cybercrime Convention requires that domestic search and seizure mechanisms must allow for an extension of the search or access by establishing a connection from a legally accessed computer system to other computer systems (or parts thereof) within the same national territory. Such an extension must be based on reasonable grounds to believe that the data required is stored in such other computer systems (or parts thereof). This requirement is adhered to in section 83(2) of the Electronic Communications and Transactions Act. This section allows a magistrate or a judge to issue a warrant where information pertinent to the investigation is accessible from within the area of jurisdiction of the court. Section 21(1)(b) of the Criminal Procedure Act also empowers a judicial officer presiding over criminal proceedings to issue a warrant for articles required in evidence at such proceedings without qualifying that such an article should specifically be in the issuing judicial officer's area of jurisdiction. Sections 21(1)(a) and 25(1) of the Criminal Procedure Act, however,

stipulate that a magistrate may issue warrants only for articles within her specific area of jurisdiction, rendering the tedious acquisition of multiple warrants a necessity in networked environments. This restrictive territoriality requirement is not conducive to effective law enforcement and it must be addressed. The jurisdiction of commissioned officers within the SAPS includes the whole of the country and it could be argued that, as justices of the peace, they may issue warrants that will not be subject to this restriction. However, the practice of the issuance of warrants by justices of the peace is itself not a practice that is widely supported and/or encouraged in post-1994 South Africa. It could also be argued that section 22(b) and 25(3) of the Criminal Procedure Act would allow for the extension required by article 19 of the Cybercrime Convention. Such an extension would, however, be limited only to circumstances where exigency can be proved.

(j) Article 19 of the Cybercrime Convention requires that domestic search and seizure mechanisms must be capable of inducing coerced cooperation for the purposes of enabling a search and seizure, if circumstances reasonably permit. Section 82(h), read with section 82(2), of the Electronic Communications and Transactions Act provides for such an active duty to cooperate. The prohibition on the obstruction of the course of justice, as provided for in section 80(5)(a) of the Electronic Communications and Transactions Act, and the use of reasonable force to overcome resistance, as provided for in section 27 of the Criminal Procedure Act, do not *per se* induce coerced cooperation in a search and seizure context. Section 7(4) of the proposed Computer Misuse Bill also provides for a duty to cooperate. It could be argued that coerced cooperation could be induced by means of section 205 of the Criminal Procedure Act. Recourse to this production mechanism would, however, not suffice, as it is not capable of an expedient enough application to address the demands of a search and seizure intervention in a computing context. The search and seizure mechanisms provided for in the Criminal Procedure Act are not capable of inducing forced cooperation. They need to be augmented in accordance with article 19 of the Cybercrime Convention.

(k) Section 31(2) of the Electronic Communications and Transactions Act provides that information contained in the cryptography register maintained by the Department of Communications may be disclosed to a relevant authority investigating a criminal offence for the purposes of any criminal proceedings, to government agencies responsible for safety and security in South Africa or to a cyber inspector. The RICPCIA makes provision for assistance to be given by postal service providers, telecommunications service providers and decryption key holders in the execution of directions under the RICPCIA. The deployment of decryption directions under section 21 of RICPCIA is, however, confined to applications for interception directions in terms of section 16 of the RICPCIA that can also only be directed at a limited category of

serious offences. Decryption directions cannot be utilised to decrypt encrypted electronic evidence obtained by means of search and seizure interventions. Also, cyber inspectors are not allowed to apply for a decryption direction under section 16 of the RICPCIA.

(l) It is submitted that section 205 of the Criminal Procedure Act may be utilised as a measure to induce decryption assistance in respect of all types of data relevant to all categories of offences.

7.2.3.1.2 Findings specific to domestic production mechanisms

(a) Domestic production devices available in the South African legislative framework are provided for in section 205 of the Criminal Procedure Act and section 19 (read with sections 13 and 14), section 39(3) and section 40(3) of the RICPCIA.

(b) Article 18 of the Cybercrime Convention is only directed at specified computer data stored in a computer system or in a data storage medium, and at subscriber information in the possession or control of a person or service provider offering its services in a party's territory. Section 205 of the Criminal Procedure Act is not similarly limited.

(c) Section 205 of the Criminal Procedure Act may be deployed to obtain material or relevant information pertaining to any alleged offence.

(d) Section 205 is furthermore not solely concerned with stored computer data, as section 15(2) of the RICPCIA provides that section 205 may also by deployed to obtain real-time communication-related information. Section 205 may, however, not be used to obtain real-time and archived communication-related information on an ongoing basis. This proviso ensures that the difference between production orders (and implicitly search and seizure devices) as opposed to interception and monitoring directions remains clear.

(e) Sections 13, 14 and 19 of the RICPCIA allow for the provision of archived communication-related information and the application for and issuing of archived communication-related directions. Archived communication-related information can be considered similar to stored traffic data as *per* the Cybercrime Convention.

(f) Sections 39(3) and 40(3) of the RICPCIA provide for the production of subscriber information, namely the identity of a customer and her telephone, cellular phone or any other number(s) allocated to the person by the telecommunications service provider. These sections are only concerned with the disclosure of limited information for the purposes of facilitating the application of directions in terms of the RICPCIA that can only be directed against a limited category of serious offences. There is an active duty on service providers to maintain subscriber information. In this respect, these sections are wider in application than article 18 of the Cybercrime Convention, as the latter is applicable only to the extent that the required data or information is maintained by the person or service provider.

(g) The South African domestic production mechanisms comply with their counterparts proposed in the Cybercrime Convention.

7.2.3.1.3 Findings specific to domestic expedited preservation and partial disclosure mechanisms

(a) No specific provision is made in the South African legislative framework for the preservation of stored computer data and the preservation and partial disclosure of stored traffic data. Such preservation and/or partial disclosure must be facilitated by means of the traditional mechanisms of search and seizure and/or production. This is acceptable, but not recommended, practice in terms of the provisions of the Cybercrime Convention. It must accordingly be considered whether specific mechanisms directed at the expedited preservation of stored computer data and the expedited preservation and partial disclosure of stored traffic data need to be built into the South African legislative framework.

(b) The default effect of the data retention requirement provided for in section 30 of the RICPCIA is that communication-related information remains available, without its preservation having been specifically ordered, for a period of between three[23] to five years (and not only for a maximum period of 90 days, as required in terms of articles 16 and 17 of the Cybercrime Convention). There is accordingly no need to create a specific mechanism to induce the expedited preservation of stored traffic data in the South African legislative framework, as this need is amply catered for, albeit by default. Section 30 of the RICPCIA is, however, not concerned with all categories of computer data, but is only directed at communication-related information.

(c) Certain other categories of computer data may be preserved by default on the basis of the retention requirements embodied in specific pieces of legislation (read with section 16 of the Electronic Communications and Transactions Act).

(d) No specific means exist within the South African legislative framework to order the preservation of categories of computer data that are not covered by the combined application of these existing data retention provisions. Such preservation can only be induced by means of the traditional search and seizure and production mechanisms. It must be considered whether the creation of a mechanism dedicated to the preservation of computer data which is not retained by legislative direction is required. It must be borne in mind that a preservation mechanism merely preserves targeted data. The disclosure of the data is still subject to the deployment of the traditional search and seizure or production devices. It is submitted that the expedited preservation of stored

---

[23] The current directives issued in respect of Mobile Cellular Operators and Fixed Line Operators under section 30(2) of the RICPCIA provide for an initial period of three years. The directive applicable to Internet Service Providers does not indicate a current retention slot (despite the peremptory wording of section 30 of the RICPCIA).

data protects the privacy of the data whilst ensuring its future availability. A criminal law mechanism similar to an Anton Pillar order (operative in a civil law context) could protect the privacy of data whilst ensuring its future availability on an expedient basis. It could also be useful to consider a preservation mechanism similar to the one provided for in the Electronic Communications Privacy Act of the United States.[24]

(e) The expedited disclosure of traffic data is aimed at the identification of other service providers and the path through which a communication was transmitted. Although it could be argued that this purpose is served by the data retention obligation on all telecommunications service providers, it must be borne in mind that not all countries impose an obligation on their service providers to retain traffic data. So as to enable the preservation of the required data in such countries, the relevant data within South Africa needs to be disclosed expeditiously (regardless of whether the data will be retained for a period of between three and five years). It is, however, submitted that no specific mechanism aimed at the partial disclosure of traffic data is required in the South African legislative framework.

(f) Archived communication-related information may be obtained under section 19 of the RICPCIA. Archived communication-related directions are issued by the Lower and High Courts on the basis of a limited category of grounds in respect of certain specified serious offences. Real-time communication-related information may be obtained on an ongoing basis under section 17 of the RICPCIA. Real-time communication-related directions are issued by the High Court on the basis of a limited category of grounds in respect of certain specified serious offences.

(g) Section 205 of the Criminal Procedure Act can be aimed at the production of both archived communication-related information and real-time communication-related information (although not on an ongoing basis). Section 205 orders are issued by the Lower and Higher Courts and in respect of information relevant to all offences.

(h) Section 23 of the RICPCIA provides for the oral application for and issuing of a direction or entry warrant, oral or otherwise. Section 23 includes in its scope, *inter alia*, real-time communication-related directions under section 17, combined applications under section 18 and decryption directions under section 21 of the RICPCIA. Section 23 oral directions are issued when it is not reasonably practicable, taking into account the urgency of the case or the existence of exceptional circumstances, to make a written application. Archived communication-related directions cannot be obtained under section 23 of the RICPCIA. Archived communication-related information is defined in section 1 of the RICPCIA as communication-related information that has been in existence for at least 90

---

[24] See also paragraph 7.2.4.5 below for a discussion of domestic preservation mechanisms available in the United States and in England.

days. This means that urgency in the sense of the expeditious disclosure of enough traffic data to enable the identification of other service providers involved in the transmission of specified communications, as envisaged by article 17 of the Cybercrime Convention, is no longer required.

7.2.3.1.4 General findings

(a) All search and seizure, production and preservation mechanisms set out in the Cybercrime Convention are aimed at stored computer data. The definition of real-time communication-related information in section 1 of the RICPCIA extends the meaning of "real-time" communication-related information to communication-related information which is immediately available to a telecommunications service provider before, during or for a period of 90 days after the transmission of an indirect communication. This has brought about exceptions in the South African legislative context, rendering section 205 of the Criminal Procedure Act, and sections 17, 18 and 23 of the RICPCIA also applicable to real-time (as opposed to stored) communication-related information. Chapter 2 of the Criminal Procedure Act, chapter XII of the Electronic Communications and Transactions Act and sections 19, 39(3) and 40(3) of the RICPCIA are, however, directed at stored data.

(b) South African domestic search and seizure, production and preservation mechanisms must be directed at specific criminal investigations or proceedings. It could be argued that section 82(1)(f) of the Electronic Communications and Transactions Act allows for a broader application, in that it is the only subsection that does not refer to a specific investigation but, instead, refers to "any offence". Taking into account the general introduction to section 82(1), it is, however, submitted that section 82(1)(f) is also to be employed within the context of an initially specified investigation. The scope of such an investigation may be extended to access and inspect the operation of any computer or equipment that forms part of an information system and any associated apparatus or material that is reasonably suspected to be or to have been used "in connection with any offence". To the extent that data retention, by default, causes the preservation of data, section 30 of the RICPCIA calls for the retention of **all** communication-related information, whether related to a specific investigation or not.

(c) Section 205 of the Criminal Procedure Act and the search and seizure mechanisms provided for in chapter 2 of the Criminal Procedure Act and chapter XII of the Electronic Communications and Transactions Act are capable of application to criminal proceedings in respect of all criminal offences. Applications for all the mechanisms under the RICPCIA can only be based on limited grounds and can only be directed at a limited category of offences. These mechanisms include the following:

(i) archived communication-related directions under section 19 of the RICPCIA;

(ii) the production mechanisms provided for in sections 39(3) and 40(3) of the RICPCIA;

(iii) real-time communication-related directions under section 17 of the RICPCIA;

(iv) oral directions under section 23 of the RICPCIA; and

(v) combined directions under section 18 of the RICPCIA.

To the extent that data retention, by default, causes the preservation of data, section 30 of the RICPCIA calls for the retention of **all** communication-related information, whether related to a specific criminal offence or not. To the limited extent that the expedited and urgent disclosure of traffic data under the RICPCIA is limited to a range of serious offences or categories of offence, South Africa could resort to the reservation provided for in section 14(3) of the Cybercrime Convention. This would be in order as the range of offences or categories of offences is not more restricted than the range of offences to which South Africa applies the measures applicable to the interception of content data. Due to the wide application of section 205 of the Criminal Procedure Act, *inter alia*, to real-time communication-related information, a reservation in terms of section 14(3) of the Cybercrime Convention is restricted and allows for a broad application.

(d) As substantive jurisdiction with regard to specific criminal offences technically does not resort within the scope of this research, suffice it to point out that the bases of territoriality and nationality, required in terms of article 22 of the Cybercrime Convention, is provided for in the South African legislative framework. In respect of offences created in terms of the Electronic Communications and Transaction Act, section 90 of the Electronic Communications and Transactions Act establishes extended extra-territorial jurisdictional bases.

(e) All South African domestic search and seizure, production and preservation mechanisms may be deployed within South African national territory. Section 21(1)(b) empowers a judge or judicial officer presiding over criminal proceedings to issue a search warrant for articles required in evidence at such proceedings without qualifying that such an article should specifically be in her area of jurisdiction. An application for a subpoena in terms of section 205 of the Criminal Procedure Act may be made to any judge or magistrate. The section 205 subpoena may be directed to any person and the examination may be conducted at any place designated by the judge or magistrate. Applications for archived communication-related directions under section 19 of the RICPCIA may be made to any judge of the High Court or a magistrate of the Lower Court. Combined directions under section 18 of the RICPCIA, oral directions under section 23 and real-time communication-related directions may be made by a judge designated by the Minister of Justice and Constitutional Development to perform the functions of a designated judge for the purposes of the RICPCIA.

(f) Sections 21(1)(a) and 25(1), however, stipulate that a magistrate or justice may issue warrants only within her specific area of jurisdiction. This becomes problematic in networked computing environments, in that multiple warrants may have to be obtained from different magistrates in different jurisdictions. These jurisdictional requirements must be updated to address the associated logistic problems that are not conducive to efficient law enforcement. Section 83(2) of the Electronic Communications and Transactions Act significantly broadens the jurisdictional requirements set out in sections 21 and 25 of the Criminal Procedure Act, namely the restrictive territorial requirement that the offence has been committed or is being committed within the jurisdiction of the issuing magistrate. Section 83(2) of the Electronic Communications and Transactions Act provides that a cyber inspector warrant may also be issued where the subject of an investigation is present in South Africa at the time when the warrant is applied for or where information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

(e) South African domestic search and seizure, production and preservation mechanisms are generally subject to South African domestic conditions and safeguards, specifically including the right against self-incrimination, legal privileges and the specificity of individuals or places that are the object of the application of the mechanisms. South African domestic search and seizure, production and preservation mechanisms are similarly generally subject to the common standards and minimum safeguards aimed at balancing the interests of law enforcement and respect for fundamental human rights arising pursuant to its obligations undertaken under applicable international human rights instruments. These safeguards include the right of everyone to hold opinions without interference; the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and the right to privacy. The practical application of these domestic and international conditions and safeguards to electronic evidence could, however, pose problems that could be alleviated by benchmarking against the legislative frameworks of, *inter alia*, the United States and England.[25]

(f) All South African domestic search and seizure, production and preservation mechanisms are specifically subject to judicial or other (independent) supervision by competent authorities to consider, *inter alia*, the grounds justifying the application of the mechanisms and the limitation on its scope and duration.

(g) South African domestic search and seizure, production and preservation mechanisms specifically incorporate the principle of proportionality, as provided for in section 36 of

---

[25] See paragraph 7.2.4 below for an overview of some of the findings with regard to search and seizure, production and preservation in the United States and England.

the Constitution, in that all legislative provisions are subject to the supremacy of the Constitution. Reasonableness, specificity and particularity requirements are also specifically made applicable to search and seizure and production mechanisms. It can also be argued that the limitations clause specifically brings into the equation (to the extent consistent with the public interest and, particularly, the sound administration of justice) the impact of the South African search and seizure, and production mechanisms upon the rights, responsibilities and legitimate interests of third parties. The Cybercrime Convention allows for preservation to be facilitated by means of the traditional search and seizure and production mechanisms. To the extent that data retained under section 30 of the RICPCIA is preserved by default, it could, however, be argued that the fact that **all** communication-related information must indiscriminately be retained offends the proportionality principle and that it does not duly consider the rights, responsibilities and legitimate interests of third parties. It is submitted that the South African data retention requirements are rather extensive (even if compared to data retention in the European Union) and could be made the subject of constitutional attack.

(h) South African domestic search and seizure, production and preservation mechanisms specifically introduce an additional obligation of confidentiality. Section 84 of the Electronic Communications and Transactions Act specifically provides for the protection of confidentiality. Section 205(3) of the Criminal Procedure Act provides that an examination under section 205 may be conducted in private at any place designated by the judicial officer concerned. Section 42 and 43 of the RICPCIA introduces a confidentiality requirement in respect of, *inter alia*, sections 17, 18, 19, 23, 39(3) and 40(3) of the RICPCIA. An obligation of confidentiality is not pertinently introduced in chapter 2 of the Criminal Procedure Act. Section 21(4) of the Criminal Procedure Act provides that a law enforcement officer executing a warrant under sections 21 or 25 must, after such execution, hand a copy of the warrant to the person upon the demand of any person whose rights have been affected in respect of the search and seizure.

(i) Privileged data or information may be specifically excluded from the application of production orders as *per* the Cybercrime Convention. Neither the South African domestic search and seizure nor the production and preservation mechanisms, in fact, can be aimed at privileged data or information. If, however, a fact, matter or thing came to the knowledge of a legal practitioner before she was professionally employed or consulted with reference to the defence of the person concerned, the situation is different. A legal practitioner is competent and compellable to give evidence as to any such fact, matter or thing which relates to or is connected with the commission of any offence with which the person by whom such a legal practitioner is professionally employed or consulted, is charged. This requirement becomes very complex in computing environments where legally privileged data are often commingled with vast

amounts of other so-called unprotected data, which law enforcement agencies may indeed lawfully access. The practical ways of addressing this issue in the legislative frameworks of England and the United States could prove to be instructive.[26]

7.2.3.2 Transborder search and seizure, production and preservation devices[27]

7.2.3.2.1 General findings

(a) Articles 23 and 25(1) of the Cybercrime Convention requires that international cooperation is to be provided among parties to the widest extent possible and impediments thereto are to be strictly limited. South Africa has generally aligned itself with the injunction to afford other jurisdictions the widest possible measure of mutual legal assistance. Although it is not explicitly stated in the International Cooperation in Criminal Matters Act, section 31 thereof specifically does not limit other forms of assistance.

(b) The Cybercrime Convention does not create a separate general mutual assistance regime in *lieu* of existing mutual legal assistance frameworks and, as such, is to be incorporated into the existing South African legislative framework:

(i) in respect of general matters, South Africa is to apply existing international instruments on international cooperation in criminal matters, arrangements agreed upon the basis of uniform or reciprocal legislation and domestic laws treaties or arrangements; and

(ii) in respect of specific matters dealt with only by the Cybercrime Convention, South Africa is to give precedence to the rules contained in the Cybercrime Convention.

(c) There is no prohibition in the existing South African legislative framework against making and attending to urgent mutual assistance requests through expedited means of communication, as required in article 25(3) of the Cybercrime Convention. It might, however, be prudent to lay down certain levels of security and authentication required for the purposes of such communications. Defining what constitutes acceptable expedited means of formal confirmation is also advisable. This can be done by means of a direction or regulation under section 33 of International Cooperation in Criminal Matters Act.

(d) In case of urgency, section 2(4) of the International Cooperation in Criminal Matters Act provides that a letter of request from South Africa may be sent directly to the court or tribunal exercising jurisdiction in the place where the evidence is to be obtained, or to

---

[26] See paragraph 7.2.4 below.
[27] See paragraphs 4.3, 4.5 and 4.7 above.

the appropriate government body in the requested state. The Director-General: Justice and Constitutional Development must, however, be notified and furnished with a copy of the letter of request. There is no requirement in the International Cooperation in Criminal Matters Act that the response to a letter of request has to be sent to or via the Director-General.

(e) The Director-General: Justice and Constitutional Development is the South African central authority in terms of the International Cooperation in Criminal Matters Act. The International Cooperation in Criminal Matters Act was, however, promulgated before the creation of the National Prosecuting Authority, when there were still close structural links to the prosecution service and coordination with criminal law practitioners was a matter of course. Due to constitutional and administrative changes, a hiatus has, however, developed since. In response, liaison between the responsible section in the Department of Justice and the National Prosecuting Authority takes place in the interests of best practice. The Minister of Justice and Constitutional Development should either by directive or by regulation under section 33 of the International Cooperation in Criminal Matters Act require collaboration as a matter of course. Since a number of agencies, including the Department of Foreign Affairs, the SAPS, Interpol, Correctional Services, the National Prosecuting Authority (the National Prosecution Service/the Asset Forfeiture Unit/the Directorate of Special Operations), are involved in some or other facet of cooperation, it would be good practice to establish a coordinating mechanism at an operational level. Such a coordinating mechanism could contribute greatly in achieving the aim of prompt and speedy action. Alternatively, the central authority should submit any mutual legal assistance request not only to the magistrate within whose area of jurisdiction the witness resides or is believed to be present, but also to the National Director of Public Prosecutions.

(f) Foreign requests for assistance in obtaining evidence must be submitted to the Director-General: Justice and Constitutional Development. She must submit the request for ministerial approval, prior to forwarding the request to the magistrate within whose area of jurisdiction the witness resides. It is recommended that the Minister delegates this function in terms of section 28 of the International Cooperation in Criminal Matters Act. It is unnecessary that approval needs as a rule be sought from the highest level. It will serve the interests of expedience if mutual legal assistance requests can be submitted directly to the South African central authority.

(g) The option of direct communication between judicial authorities or Interpol in urgent cases is not specifically provided for in section 7 of the International Cooperation in Criminal Matters Act with regard to requests from foreign states to South Africa. The option of expedited direct communication must also be considered for the purposes of requests from foreign states. In the absence of a specific provision to this effect within

the relevant South African legislative framework, article 27(9) of the Cybercrime Convention will become operative to provide for such urgent requests by foreign states (unless this is ruled out by means of the declaration provided for in article 40 read with article 27(9)(e)).[28]

(h) Article 27(9)(e) of the Cybercrime Convention further allows for direct communication between the judicial authorities or Interpol in respect of mutual legal assistance requests that can be complied with by the requested party without making use of coercive action. This provision will also apply in the South African mutual assistance legislative framework, as no specific provision has been made in this respect.

(i) Article 25(4) of the Cybercrime Convention directs that the grounds on which parties may refuse co-operation are those provided for in the domestic law of the requested party and in applicable mutual assistance treaties. Mutual assistance in respect of the offences referred to in articles 2 to 11 of the Cybercrime Convention may, however, not be refused solely on the ground that the request concerns an offence which South Africa considers a fiscal offence. Barring the one exception in section 16 of the International Cooperation in Criminal Matters Act that enables the Minister of Justice and Constitutional Development to apply the dual criminality requirement in respect of the mutual execution of sentences and compulsory orders, there is no statement of grounds for refusal in the International Cooperation in Criminal Matters Act. This is a *lacuna* in South African domestic legislation.

(j) Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between South Africa and a requesting or requested state, articles 27 and 28 of the Cybercrime Convention apply. The grounds of refusal and/or postponement of or qualified execution of mutual legal assistance requests provided for in article 27 of the Cybercrime Convention are the following:

(i) assistance may be refused where the execution of the request is likely to prejudice the sovereignty of the State, security, *ordre public* or other essential interests;

(ii) assistance may be refused where the requested party considers the offence to be a political offence or an offence connected with a political offence;

(iii) a requested party may postpone (rather than refuse) assistance where immediate action on the request would be prejudicial to investigations or proceedings in the requested party;

(iv) where the assistance sought would otherwise be refused or postponed, the requested party may instead provide assistance subject to conditions; and

(v) reasons must be provided if a request is refused or postponed.

---

[28] It is recommended that South Africa does not make use of this declaration. See paragraph 7.2.3.3 below.

(k) In addition to the grounds of refusal provided for in article 27 of the Cybercrime Convention, article 29(5) provides that the assertion of any other basis for refusing a mutual legal assistance request for the preservation of traffic data is precluded. Apart from the grounds of refusal explicated in article 28 of the Cybercrime Convention, refusal of assistance on data protection grounds may also be invoked only in exceptional cases. As South African law has explicated no grounds of refusal (other than double criminality in respect of the mutual execution of sentences and compulsory orders), it is in line with both these requirements.

(l) Article 27(3) of the Cybercrime Convention obliges a requested party to execute requests in accordance with the procedures specified by the requesting party, unless to do so would be incompatible with its own law. South Africa is in accord with this requirement, in that section 30 of the International Cooperation in Criminal Matters Act provides that any deposition, affidavit, record of any conviction or any document evidencing an order of a court issued in a foreign state[29] may be received in evidence at any proceedings in terms of a provision of the said Act, if

(i) it is authenticated in the manner in which foreign documents are authenticated; or

(ii) authenticated in the manner provided for in any agreement with the foreign state concerned.

(m) Under article 27 of the Cybercrime Convention, South Africa may keep its fundamental legal requirements intact when executing a coercive power on behalf of a requesting party.

(n) Although the aspects of confidentiality and use limitations are addressed in certain treaties to which South Africa is a party, the International Cooperation in Criminal Matters Act is silent on these aspects. This is a *lacuna* in the South African mutual legal assistance framework. Articles 27 and 28 of the Cybercrime Convention are therefore applicable. Article 27(8) of the Cybercrime Convention provides that the confidentiality of the fact and content of the request must be guarded in particularly sensitive cases, or in cases in which there could be disastrous consequences if the facts underlying the request were to be made public prematurely. Article 28(2)(a) of the Cybercrime Convention states that the furnishing of information or material in response to a request may be made dependent on the condition that it is kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition. Article 28(2)(b) of the Cybercrime Convention directs that the furnishing of information or material in response to a request may be made dependent on the condition that it is not used for investigations or proceedings other than those stated in the request. In

---

[29] Or any copy or sworn translation thereof.

addition, the confidentiality of information spontaneously forwarded in terms of article 26 of the Cybercrime Convention may be one of the conditions that can be imposed on the use of such information.

(o) Under article 25(2) of the Cybercrime Convention, South Africa is required to adopt such legislative measures and other measures as may be necessary to provide for the following types of mutual legal assistance in respect of search and seizure, production and preservation:

(i) the expedited preservation of stored computer data;

(ii) the expedited disclosure of preserved traffic data;

(iii) the accessing of stored computer data;

(iv) the transborder access to stored computer data with consent or where publicly available; and

(v) the maintenance of a 24 hour, 7 day a week network.

(p) In any given case where coercive assistance is involved, it must be determined whether South Africa is a bilateral or multilateral treaty partner with the requesting or requested state involved. The provisions of such a treaty will govern mutual legal assistance requests for, *inter alia*, search and seizure, production, preservation and partial disclosure. In addition, the International Cooperation in Criminal Matters Act constitutes the domestic legal basis for the provision of mutual legal assistance to foreign states. Section 7 of the International Cooperation in Criminal Matters Act is of particular importance regarding the obligatory assistance to be provided by South Africa under article 25(2) of the Cybercrime Convention. Uncertainty exists with regard to whether all requests for mutual assistance need to be channelled via the mechanism created in section 7 of the International Cooperation in Criminal Matters Act. In current law enforcement practice, for example, some practitioners facilitate searches and seizures on behalf of other states under chapter 2 of the Criminal Procedure Act. Sections 20(a) and (b) of the Criminal Act allow for the search and seizure of certain articles which are concerned in or which may afford evidence of the commission of an offence, "whether within South Africa or elsewhere". Section 31 of the International Cooperation in Criminal Matters Act specifically does not limit the provision of mutual legal assistance on other bases. Other practitioners, however, contend that all requests for searches and seizures on behalf of another state need, firstly, to be facilitated via section 7 of the International Cooperation in Criminal Matters Act, prior to recourse being taken to, for example, chapter 2 of the Criminal Procedure Act. It is submitted that this is the advisable route to follow. The uncertainty in this respect must, however, be addressed. This can be done by direction or regulation under section 33 of the International Cooperation in Criminal Matters Act.

(q) Where a request for mutual legal assistance relates to various magisterial districts, a literal interpretation of section 7 of the International Cooperation in Criminal Matters Act could be that the request must be forwarded to a number of magistrates. This could be cumbersome, cause delays and pose problems of coordination. An amendment to the International Cooperation in Criminal Matters Act, to the effect of providing for any one magistrate to be designated with concomitant trans-jurisdictional powers to deal with the whole request, must be considered.

(r) In popularising mutual legal assistance practice, it is suggested that the South African central authority should consider compiling and circulating guidelines for the contents of both outgoing and incoming requests to all role players in the mutual legal assistance framework. The compilation of a database of the relevant legislation and requirements for the requests of foreign states, including their contact particulars, would also be very useful.

(s) Article 35 of the Cybercrime Convention requires that South Africa designate a point of contact for the purposes of the Cybercrime Convention's 24 hour a day, 7 days a week network. The South African National Prosecuting Authority has volunteered and currently acts as the entry point-of-contact for the G8 24 hour, 7 day a week network. The designation of a point of contact is a matter that needs to be negotiated by the relevant governmental entities that have the capacity, competency and (technical) ability to fulfil this function. It is recommended that the South African central authority facilitates discussions between the relevant role-players in this respect. This is another issue that can be resolved by establishing a coordinating mechanism at an operational level.

(t) South African mutual legal assistance to foreign states cannot exceed the existing domestic ability to search and seize, preserve or produce electronic evidence. It is submitted that the available domestic mechanisms will be utilised once a request for mutual legal assistance is processed via section 7 of the International Cooperation in Criminal Matters Act. The findings extracted with regard to the domestic search and seizure, production and preservation mechanisms[30] will accordingly be equally applicable to, *inter alia*, the following general requirements extracted from the Cybercrime Convention in respect of the transborder search and seizure, production and preservation mechanisms:[31]

(i) The transborder mechanisms are to be aimed at stored computer data. The spontaneous production of information under article 26 of the Cybercrime Convention is, however, not limited to stored computer data, but includes any

---

30 See paragraph 7.2.3.1.1., 7.2.3.1.2, 7.2.3.1.3 above.
31 See paragraph 7.2.2.2. above.

information obtained within the framework of investigations carried out by the party forwarding the information.

(ii) The transborder mechanisms must be capable of application to **any** criminal offence.

(iii) The transborder mechanisms are subject to the conditions provided for by the South African domestic laws and will not be executed on behalf of a requesting party, unless the South African fundamental domestic requirements are satisfied. In addition, these mechanisms are subject to the conditions provided for by the applicable mutual assistance treaties.

(iv) In addition to the South African domestic use limitations and confidentially requirements, article 28(2)(a) of the Cybercrime Convention allows the requested party, when responding to a request for mutual assistance, to request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such a condition. Under article 28(2)(b) of the Cybercrime Convention, the requested party may also make the furnishing of the information or material dependent on the condition that it may not be used for investigations or proceedings other than those stated in the request. There are two exceptions to the ability to limit use and ensure confidentiality, considered implicit in the terms of article 28(2) of the Cybercrime Convention: evidence exculpatory to an accused person must be disclosed to the defence or a judicial authority; and, once the material furnished has been used at trial (normally a public proceeding and including compulsory disclosure), it is considered to have essentially passed into the public domain.

(u) The condition of dual criminality under the Cybercrime Convention must be deemed to have been fulfilled, irrespective of whether South African laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting party, as long as the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. In addition to this liberal definition of dual criminality, article 29(3) of the Cybercrime Convention sets out the general rule that parties must dispense with any dual criminality requirement with regard to preservation orders due to the volatility of data. The South African mutual legal assistance framework is in accord with these requirements in respect of the dual criminality safeguard. Section 16 of the International Cooperation in Criminal Matters Act provides for the express introduction of the dual criminality rule of extradition law in our mutual assistance law, by way of prominent exception. This dual criminality requirement is only applicable to the mutual execution of sentences and compulsory orders (with South Africa as the requested state).

(v) Nothing in the South African mutual legal assistance framework prohibits consultation, as required under article 22(5) of the Cybercrime Convention, with a view to determining the most appropriate jurisdiction for prosecution(s), when more than one party claims jurisdiction over an offence. It is, however, recommended that explicit provision is made for this requirement, and the practicalities associated with it, in the regulations issued by the Minister of Justice and Constitutional Development under section 33 of the International Cooperation in Criminal Matters Act.

7.2.3.2.2 Findings specific to transborder search and seizure mechanisms

South African mutual legal assistance to foreign states cannot exceed the existing domestic ability to search and seize. It is submitted that the available domestic mechanisms will be utilised once a request for mutual legal assistance is processed via section 7 of the International Cooperation in Criminal Matters Act. The findings extracted with regard to the domestic search and seizure[32] will accordingly be equally applicable to the search and seizure specific requirements under articles 31 and 32 of the Cybercrime Convention.

7.2.3.2.3 Findings specific to transborder preservation and partial disclosure mechanisms

(a) South African mutual legal assistance to foreign states cannot exceed the existing domestic ability to preserve and partially disclose. It is submitted that the available domestic mechanisms will be utilised once a request for mutual legal assistance is processed via section 7 of the International Cooperation in Criminal Matters Act. The findings extracted with regard to domestic preservation and partial disclosure[33] are accordingly equally applicable to the requirements under articles 29 and 30 of the Cybercrime Convention specific to preservation and partial disclosure.

(b) In addition, South Africa must promptly inform a requesting party if a preservation order will not ensure the future availability of the required data, or will threaten the confidentiality of, or otherwise prejudice the investigation of the requesting party. This can be done by means of direction or regulation under section 33 of International Cooperation in Criminal Matters Act.

---

32 See paragraphs 7.2.3.1.1 and 7.2.3.1.4 above.
33 See paragraphs 7.2.3.1.3 and 7.2.3.1.4 above.

7.2.3.2.4 Findings specific to transborder spontaneous production mechanisms

Nothing in the South African mutual legal assistance framework prohibits the spontaneous production of information, as provided for under article 26 of the Cybercrime Convention. It is, however, recommended that explicit provision is made for this requirement, and the practicalities associated with it. This can be done by means of direction or regulation under section 33 of International Cooperation in Criminal Matters Act.

7.2.3.3 Declarations[34]

(a) Article 27(9)(e) of the Cybercrime Convention provides that a party may require that, for reasons of efficiency, urgent requests made under article 27(9) must also be addressed to its central authority and may not be made directly to its judicial authorities.

(b) Under section 27(9) of the Cybercrime Convention South Africa must facilitate the direct communication between judicial authorities or Interpol in urgent cases in respect of requests from foreign states to South Africa. It is doubtful whether a declaration under article 40, read with article 27(9)(e) of the Cybercrime Convention, directing that urgent mutual legal assistance requests from foreign states be addressed to the South African Central Authority, will be in the interests of efficiency. It is therefore recommended that South Africa does not avail itself of this reservation.

7.2.3.4 Reservations[35]

(a) A reservation permits the exclusion or modification of the legal effect of certain obligations set out in the Cybercrime Convention so as to avoid conflict with a party's constitutional or fundamental legal principles. The reservations provided for in articles 14, 22(2), 29(4) and 41 of the Cybercrime Convention are relevant to this research.

(b) To the limited extent that the expedited and urgent disclosure of traffic data under the RICPCIA is limited to a range of serious offences or categories of offence, it is necessary for South Africa to resort to the reservation provided for in section 14(3) of the Cybercrime Convention. This would be in order, as the range of offences or categories of offences is not more restricted than the range of offences to which South Africa applies the measures applicable to the interception of content data. Due to the wide application of section 205 of the Criminal Procedure Act to, *inter alia*, real-time

---

34 See paragraph 7.2.3.3. above.
35 See paragraph 7.2.3.4 above.

communication-related information, a reservation in terms of section 14(3) of the Cybercrime Convention is restricted and allows for a broad application.

(c) Article 22(2) of the Cybercrime Convention allows parties to enter a reservation to all the jurisdiction grounds laid down in article 22(1), excluding the establishment of territorial jurisdiction under article 22(1)(a) and jurisdiction in cases falling under the principle of *aut dedere aut judicare* in article 22(3).

(d) It is unnecessary for South Africa to avail itself of the reservation provided for in section 29(4) of the Cybercrime Convention, as dual criminality is only required in the South African mutual legal assistance framework for the purposes of section 16 of the International Cooperation in Criminal Matters Act.

(e) It is unnecessary for South Africa to avail itself of the reservation provided for in section 41 of the Cybercrime Convention. For the purposes of chapter II of the Cybercrime Convention, article 41 allows for a reservation that accommodates minor variations in its applicability, as a result of the well-established domestic law and practice of a party that is a federal state.

7.2.4 Search and seizure, production and preservation troubleshooting @ the United States and England[36]

(a) A comparative troubleshooting utility between the South African search and seizure, production and preservation mechanisms and those available in the legislative frameworks of the United States and England was enabled by means of chapters 5 and 6 respectively. This was done, firstly, by identifying equivalent devices (where such devices exist); secondly, by gaining a broad understanding of the legislative frameworks from which these devices emanate; and, lastly, by examining the ways in which they are applied to electronic evidence.

(b) In serving the main objective of this thesis, the purpose behind the enablement of such a troubleshooting utility was to contribute towards an investigation into whether any alignments and/or augmentations are required in respect of the South African domestic search and seizure, production and preservation mechanisms. Precedents regarding the practical deployment and application of equivalent or analogous measures in the United States and England to electronic evidence are useful to South African law enforcement and legal practitioners. It is furthermore axiomatic that the outcome of any challenge to the legality of a search and seizure, production or preservation intervention depends on the judicial interpretation and application not only of domestic criminal procedural and evidence law, but also of human rights law. The parallel evolution of human rights law to stand its ground in the Third Wave, in other jurisdictions, cross-pollinates the debate in

[36] See chapters 5 and 6 of this thesis.

respect of the legal response to technological developments. It is therefore also useful to compare safeguards afforded by the South African Constitution, the English HRA, the European Convention on the Protection of Human Rights and those granted by the Constitution of the United States. Whilst there may be differences of emphasis and of detail, there are similarities of principle and it is possible to draw insightful analogies.

(c) Some of the most instructive findings that can be extracted from the snapshots provided of the different catalogues of search and seizure, production and preservation mechanisms available in the legislative frameworks of the United States and England, compared to South Africa, are listed below.

7.2.4.1 Right to privacy

(a) Of the spectrum of widely acknowledged fundamental rights, the collection of evidence impacts most profoundly on the right to privacy.[37] Article 14 of the South African Constitution makes explicit provision for a right to privacy. In England, the HRA introduced into English domestic law in 1998, for the first time, a right to privacy as *per* article 8 of the European Convention on the Protection of Human Rights. In much the same way as in post-1994 South Africa, existing English law enforcement methodology has been subjected to an ongoing re-evaluation. Despite the fact that the United States Bill of Rights at no point makes any mention of a constitutional right to privacy, the right to privacy is considered an implicit part of several of the provisions of the Bill of Rights. There is an entrenched protection of the right to privacy in the United States and there is consequently a wealth of case law that can be drawn upon for comparative purposes. Case law in England and South Africa is embryonic in comparison to that of the United States Supreme Court.

(b) One important distinction between the Fourth Amendment of the United States Constitution and article 14 of the South African Constitution on the one hand and article 8 of the European Convention on the Protection of Human Rights on the other, is that the latter makes no specific reference to powers of search. Article 8(1) of the European Convention on the Protection of Human Rights creates a general right to privacy by stating that everyone has the right to respect for her private and family life, her home and her correspondence.

(c) The right to privacy is not absolute and derogation is permitted. The reasonable expectation to privacy test endorsed in the United States has been applied by the South African Constitutional Court. The United States Supreme Court has generally held that a person has a reasonable expectation to privacy regarding items in closed containers. It

---

37 See paragraph 4.2.4.1 above with regard to the right to privacy in South Africa, paragraph 5.2.2 above with regard to the United States and paragraph 6.2.2 above with regard to England.

is generally accepted that technological storage media should be considered equivalent to a special filing cabinet or a briefcase. Although courts in the United States have generally agreed that electronic storage devices can be compared to closed containers, they have reached different conclusions regarding whether each individual file stored on a computer or disk should be treated as a separate closed container. These precedents could prompt relevant issues in the local debate.

(d) An important structural difference between the application of the Fourth Amendment and article 14 of the South African Constitution on the one hand and the Human Rights Act on the other, is the fact that, in England, the legislation conferring the right to privacy may be repealed like any other enactment. Also, any pre-existing legislation will not automatically be repealed to the extent that it is inconsistent with the Human Rights Act. The English courts must strive to interpret statutes in accordance with the Human Rights Act and with jurisprudence concerning the European Convention on the Protection of Human Rights, but, where this is impossible, a declaration of incompatibility may be made. Striking down inconsistent legislation is not within the hands of the judiciary, but in those of a government minister who may, by order, make amendments to the incompatible legislation if the minister considers that there are compelling reasons to do so. The extent to which the search and seizure, production and preservation mechanisms may be circumscribed by reasonableness criteria is affected by the structural difference between constitutional protections in England and those in the United States and South Africa.

7.2.4.2 Unconstitutionally obtained evidence

(a) Prior to section 78(1) of PACE, there was an acknowledged, but rarely applied, judicial discretion in English law to exclude evidence that had been improperly obtained. Section 78 now provides for a clear discretion to exclude the fruits of an illegal evidence collection intervention. Section 78(1) provides that the court may refuse to allow evidence on which the prosecution proposes to rely to be given, if it appears to the court that, taking into account all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it. The English courts have, however, traditionally been slow to disallow evidence on this basis. In England, maintaining the reputation and integrity of the criminal justice system is not the crucial concern when judicial discretion to exclude evidence is being exercised.

(b) The adversarial common law culture that applies to proceedings in the United States, however, permits the argument that evidence should be excluded, despite its inherent reliability, if it is obtained in violation of powers granted to law enforcement officers. Evidence seized in violation of the Fourth Amendment cannot be used against the

defendant in a criminal prosecution. Because computers have the capacity to store massive amounts of information, there is a very real danger that information obtained from, for example, the unconstitutional seizure of a computer will lead law enforcement agencies to evidence that would have remained undiscovered but for the search of the computer. If, therefore, a Fourth Amendment violation can be proved, some or all subsequently obtained evidence may accordingly be excluded as "fruits of the poisonous tree".

(c) Article 35(5) of the South African Constitution instructs that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice. This exclusionary rule signals clearly to all law enforcement officers that it is futile to gather evidence in an unlawful manner, since evidence obtained unlawfully will not be taken into account by the court in reaching a verdict. Fairness may, however, require that unconstitutionally obtained evidence sometimes be admitted and other times be excluded

7.2.4.3 Domestic search and seizure devices[38]

(a) In current South African law enforcement practice, the provisions of chapter 2 of the Criminal Procedure Act are widely applied to facilitate the search and seizure of intangible computer data. This practice has not been contested in court as yet.[39] The cyber inspectors have not been appointed to date and there is no indication as to when this will happen, if it indeed does happen. However, regardless of whether the cyber inspectorate is established and made fully operational, it is infeasible to render the other mainstream law enforcement agencies, as a matter of course, dependent on the services of the cyber inspectors. Some alignment of chapter 2 of the Criminal Procedure Act is requisite.[40]

(b) It is interesting to note that Rule 41(a)(2)(2A) of the Federal Rules of Criminal Procedure defines "property" to specifically include "tangible objects such as documents, books, papers, as well as information". In England, sections 19 and 20 of PACE are aimed at computer data in particular. This is in accord with the recommendation made in paragraph 7.3 below that the Criminal Procedure Act be aligned to specifically incorporate computer data and information.

---

38 See paragraph 4.2 above with regard to domestic search and seizure in South Africa, paragraph 5.2 above with regard to the United States and paragraph 6.2 above with regard to England.

39 Although there were, in fact, a few cases in which electronic evidence was adduced as evidence, the procedure by means of which such evidence was collected was not contested. The only South African case, to date, where the procedure deployed to collect the required electronic evidence came under scrutiny of the Court is *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* [2005] JOL 13758 (C). See a reference to the detail of the case in footnote 135 of paragraph 4.2.3.1. above. This case is also relevant in a transborder search and seizure context (see paragraph 4.3.1.5 above).

40 See paragraph 7.3 below in this respect.

(c) The general rule in England, the United States and South Africa is that all searches and seizures must be conducted under authority of a warrant. These search and seizure warrants in all three jurisdictions must, *inter alia*, adhere to the requirements of particularity and specificity, judicial supervision and probable cause or reasonable grounds. These requirements are also referred to in the Cybercrime Convention.

(d) The doctrine of particularity and specificity, by means of example, becomes quite complex when one examines the issuance of a search warrant involving *e*-evidence. Although very little case law exist in respect of the search and seizure of electronic evidence in England and South Africa, the United States, once again has litigated quite extensively on it. Regrettably, there is little final authority on the subject, because the United States Supreme Court has not yet ruled on particularity and specificity, which means that the sometimes-conflicting opinions of the High Court and various circuit courts apply. This case law is, however, of significance to the South African legal landscape in that it can, at the very least, feed the local debate.

(e) In the United States, law enforcement officers have been advised that the most important decision to make when describing the property in the warrant is whether the seizable property is the computer hardware itself, or merely the information that the hardware contains. If computer hardware is contraband, evidence, fruits, or instrumentalities of crime, the warrant should describe the hardware itself. If the probable cause relates only to information, the warrant should describe the information, rather than the physical storage devices which happen to contain it. Although this is not a clear-cut rule that will be practicable in all scenarios in the South African context, it is a good rule of thumb to take note of and to follow whenever possible.

(f) A lack of judicial scrutiny could preclude an assessment of probable cause in all three of the jurisdictions discussed in this research. Law enforcement officers, or a forensic expert instructed by them, must accordingly explain the complexities involved in the investigation of high technology crimes to judicial officers who need to issue warrants. There are a few areas of search and seizure where this is more important than in cases involving high technology crimes and/or *e*-evidence. To counter the argument that law enforcement is on an evidential "fishing expedition", it is imperative that the judicial officer issuing the warrant be made to understand the following issues:

(i) the importance of the *e*-evidence to the successful prosecution of the state's case and the volatility of such evidence;

(ii) the need to examine all of the various storage media; and

(iii) the fact that items seized that do not contain evidence of the crime for which the search warrant was issued will not be examined and will be released back to the owner.

(g) Law enforcement officers in the United States, when drafting a successful search warrant operable in a computing context, are required to provide an exposition of the envisaged search strategy encapsulating both its practical and legal considerations in the affidavit accompanying the search warrant. In general, the issues that must be considered when formulating such a strategy to search and seize *e*-evidence can be divided into four questions: Firstly, what is the role that the computer played in the commission of the offence and how can this enable the most effective search strategy compliant with the relevant legislative prescripts? Secondly, will the search require multiple warrants? Thirdly, should law enforcement officers request special permission to conduct a no knock or surreptitious search, without having to notify the person whose premises are searched at the time of the search? And fourthly, does the search strategy need to be modified and will it be necessary to search and sift before the actual seizure of the relevant data, to minimise liability issues? South African law enforcement officers could do well by devising similar search strategies and by attaching such strategies to the application for warrants for electronic evidence. Benchmarking against the existing practices in these respects in the United States and England will prove valuable. Consider in this regard, for example the innovative English search and sift power conferred by section 50 of the Criminal Justice and Police Act 2001, which empowers the removal of items for more detailed inspection. Privileged files in the United States are reviewed by the court *in camera*, by a taint team or by a special master.

(h) Warrantless searches and seizures in the legislative frameworks of South Africa, the United States and England are exceptions to the rule that all search and seizure interventions must be performed under authority of a warrant. There are significant similarities not only between the different warrantless doctrines that exist in South Africa, the United States and England, but also regarding the application thereof. Although very little case law exist in respect of the search and seizure of electronic evidence in England and South Africa, the United States, once again has litigated quite extensively on it. South African law enforcement practitioners can benefit from these precedents. Consider for example the following scenarios:

(i) In the United States, when examining third party consent to search technological devices, the most important consideration is perhaps whether the individual has the right to grant consent to search the computer in question. It is common for several people to use or own the same computer equipment. If the individual lives in the same residence, has access to the room in which the computer is placed, and has access to the data on the computer, law enforcement officers should not encounter any problems with regard to the validity of the search. If any one of those people gives the law enforcement officers permission to search for data, the officers may generally rely on that consent, provided that the person

has authority over the computer. All users have assumed the risk that a co-user might discover everything in the computer and might also permit law enforcement to search this common area. Although the co-users of a computer generally have the ability to consent to a search of its files, a search warrant should be obtained before continuing the search if any of the files are password-protected or if the entire computer is password-protected. Regardless of whether the password may be obtainable from or by a third party, a court could easily view the use of a password as an attempt to ensure privacy from a third party. When an individual protects her files with passwords and has not shared the passwords with others who also use the computer, the authority of those other users to consent to a search of the computer does not extend to password-protected files. Conversely, if the co-user has been given the password by the suspect, then she probably has the requisite common authority to consent to a search of the files. These considerations are equally relevant to South African consensual searches and seizures.

(ii) Due to the increasing use of handheld and portable computers, pagers, cellular phones and other electronic storage devices, law enforcement officers often encounter computers when they conduct searches incident to lawful arrests. The question is whether the search incident to arrest exception to the warrant requirement permits both the seizure and the search of such storage media. Due to the considerable storage capacities of contemporary technological devices, the length of time between the seizure of a disk and the search of its contents also poses problems. Numerous courts in the United States have held that lengthy searches after an arrest are invalid because the exigency of the situation diminishes and disappears over time. Law enforcement officers are encouraged to seize the technological device upon the arrest of the individual in order to protect the data on the disk or device, but to obtain a search warrant before they search the contents of the device. These considerations are equally relevant to South searches incident to arrest. In England, a search on arrest is permitted by section 18 of PACE but there is no associated element of exigency and it may be conducted at any time after arrest. This is a considerable extension of a warrantless search power that is usually linked to urgency or exigent circumstances. The power may be challenged under article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, since there is no requirement of judicial scrutiny even in those circumstances where it would be feasible to obtain a warrant. This will not accord with the South African Constitution.

(iii) Exigent circumstances often arise in computer cases because electronic data is perishable. The main issue with regard to the exigent circumstance seizure of digital evidence is how likely it is that the data would be lost if law enforcement officers were to take the time to obtain a warrant. It is important that the existence of exigent circumstances does not permit officers to search or seize beyond what is necessary to prevent the destruction of the evidence. When the exigency ends, the right to conduct warrantless searches ends as well. The need to take certain steps to prevent the destruction of evidence does not authorise law enforcement officers to take further steps without a warrant. Accordingly, the seizure of computer hardware to prevent the destruction of any information it contains in the United States does not ordinarily support a subsequent search of that information without a warrant. This is a sound approach to follow and South African law enforcement officers could do well in adhering to the same principle.

7.2.4.4 Domestic production devices[41]

(a) Law enforcement agencies in the United States can avail themselves of five different mechanisms to compel service providers to disclose, for example, the contents of stored wire or electronic communications, including email and voice mail and other information, such as account records and basic subscriber information. The five mechanisms, in ascending order of required threshold showing, are the following:

(i) a subpoena;

(ii) a subpoena with prior notice to the subscriber or customer;

(iii) a section 2703(d) court order;

(iv) a section 2703(d) court order with prior notice to the subscriber or customer; and

(v) a search warrant.

Greater process generally includes access to information that can be obtained with lesser process. A higher-level process will always prevail. The stored communication portion of the Electronic Communications Privacy Act[42] offers varying degrees of legal protection, depending on the perceived importance of the privacy interest involved when requesting the production of information. Generally, the greater the perceived privacy interest, the greater the privacy protection that is afforded. This is similar to the production devices available in the South African legislative context. In this regard, consider, for example, the differentiation between archived and real-time communication-related information and the different ways in which to access such

41 See paragraph 4.4 above with regard to domestic production devices in South Africa, paragraph 5.3 above with regard to the United States and paragraph 6.3 above with regard to England.

42 Sections 2701-2712 of 18 USC.

information. Information can be accessed both on a once-off basis under section 205 of the Criminal Procedure Act, and on an ongoing basis under the communication-related directions provided for in the RICPCIA.

(b) In the United States, providers of services that are not available to the public may also freely disclose both contents and other records relating to stored communications, but the Electronic Communications Privacy Act imposes restrictions on voluntary disclosure by providers of services to the public. If a provider may disclose the information to a law enforcement agency and is willing to do so voluntarily, law enforcement officers do not need to obtain a legal order to compel the disclosure. However, if the provider either may not or will not disclose the information, law enforcement agencies must rely on the appropriate legal orders to compel disclosure. No such voluntary disclosure mechanisms exist in South Africa or in England.

(c) In England, PACE was passed with complicated safeguards to protect three classes of material. These classes are legally privileged material, special procedure material and excluded material. Access to special procedure and excluded material may normally be obtained by means of a production order issued in terms of Schedule 1 of PACE. Items which a law enforcement officer has reasonable grounds for suspecting to be subject to legal privilege may never be seized, whatever the basis of the law enforcement officer's presence. Presumably, reasonable grounds require more than a mere statement by the owner that the items are subject to legal privilege. Law enforcement officers may well be entitled to inspect the documents to a limited extent in order to ascertain their character. Items held with the purpose of furthering a criminal purpose, however, cannot enjoy legal privilege. In any case, English law enforcement agents also have at their disposal the search and sift power conferred by section 50 of the Criminal Justice and Police Act of 2001, which empowers them to remove items for more detailed inspection.

(d) In England, chapter II of Part I of RIPA provides a legislative framework that covers the requisition, provision and handling of communications data. There are essentially two ways in which communications data may be obtained. Firstly, section 22(3) of RIPA provides a means for a designated person to authorise someone within the same relevant public authority to provide the legal basis upon which the public authority may itself collect the communications data. Section 22(4) of RIPA provides the second way in which communications data may be obtained, namely by allowing a designated person to serve a notice upon the holder of the data, requiring the holder to comply with the terms of the notice.

(e) Attempts to introduce legal regulation of encryption in the United States have attracted considerable opposition in the past. No specific provision is accordingly made for decryption assistance, *per se*. As with any kind of stored and transmitted data, law enforcement agents may obtain both encrypted text and decryption keys pursuant to a

lawful process. Such processes may include a wiretap order, a search warrant, a subpoena or the consent of the party possessing the required item. In the United States, the government has also introduced a voluntary key escrow device under which law enforcement agencies can unlock encrypted communications.

(f) Sections 49 to 56 of RIPA facilitate the disclosure of protected data. Properly authorised members of law enforcement are empowered to serve notices on individuals or bodies requiring the disclosure of protected information which they lawfully hold, or are likely to hold, in an intelligible form. These provisions of RIPA are currently in the process of being promulgated.

7.2.4.5 Domestic data preservation devices[43]

(a) The United States follows a model of data preservation, whereas South Africa and the European Union follow a data retention approach.

(b) No law regulates how long network service providers in the United States must retain account records. To minimise the risk that crucial electronic evidence may be lost or destroyed, the Electronic Communications Privacy Act permits the government to direct providers to freeze stored records and communications pursuant to section 2703(f) of 18 USC. A provider of wire or electronic communication services or a remote computing service, upon a law enforcement request, is obliged to take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process. However, the authority to direct providers to preserve records and other evidence is not prospective. Some network service providers may also be technically unable to comply effectively with section 2703(f) requests. A section 2703(f) preservation order could be considered when considering how to devise a preservation order for the expedited preservation of stored computer data that is not retained by legislative direction[44] in South Africa.

(c) As in England, no specific provision has been made in the South African criminal procedural law framework for preservation and partial disclosure mechanisms. The traditional measures of search and seizure and production set out above must accordingly be utilised to accomplish the expedited preservation of stored computer data and the expedited preservation and partial disclosure of traffic data. However, data that has been retained is, by default, preserved. The retention of communications data in England is currently addressed by the current Code of Practice for Voluntary Retention of Communications Data, issued by the Home Secretary in 2003 under authority of the

---

43 See paragraph 4.6 above with regard to domestic preservation mechanisms in South Africa, paragraph 5.4 above with regard to the United States and paragraph 6.4 above with regard to England.

44 Communication-related information that is retained pursuant to section 30 of the RICPCIA and those categories of computer data that are retained on the basis of specific legislation, read with section 16 of the Electronic Communications and Transactions Act.

Anti-Terrorism, Crime and Security Act. The Code prescribes a range of maximum retention periods for communications and traffic data.

(d) The European Union has now accepted the European Union Data Retention Directive and England will have to align itself with its provisions. The European Union Data Retention Directive provides, *inter alia*, for the mandatory retention of data for a period between six and 24 months, although member states may extend the retention period. The European Union Data Retention Directive is aimed at harmonising the following elements: the types of data to be retained; the length of time for which the data should be retained; and the purposes for which the data may be supplied to competent authorities. Content is specifically excluded from the operation of the European Union Directive. Access to data must be provided in accordance with national legislation. Minimum data security principles are prescribed in respect of data retained in accordance with the present Directive. The mandatory retention of traffic data for a fixed length of time can impose huge and even infeasible obligations on an Internet Service Provider. The difficulty with introducing a mandatory general retention of traffic data is that not only the "fingerprints" of an extremely small minority of the population are being kept, namely those of suspected criminals, but also those of a whole population to whom no suspicion is attached. At the very least, the emerging regulations on the mandatory general retention of traffic data create an unpredictable legal framework and should be the subject of a more refined legal debate. The details of this discourse could be instructive to the South African debate.

7.3 *Cursors*[45]

(a) The uncertainty pertaining to the applicability of the search and seizure mechanisms provided for in the Criminal Procedure Act to computer data and information systems is undesirable and must be addressed. This can be done by inserting into section 1 of the Criminal Procedure Act a provision similar to section 82(4) of the Electronic Communications and Transactions Act, namely that "any reference in this Act [the Criminal Procedure Act] to 'premises' and 'article' includes an information system as well as data messages".

(b) Any uncertainty pertaining to making available comprehensive legal authorisation to search and access and seize or copy computer data in the Criminal Procedure Act is undesirable and must be addressed. This can be done by aligning the wording of the search and seizure mechanisms provided for in the Criminal Procedure Act with the

[45] In this context, cursors refer to recommendations aimed at aligning the South African search and seizure, production and preservation devices with the devices proposed in the Cybercrime Convention. See footnote 127 in paragraph 1.2 above for a definition of a "cursor".

wording proposed in section 7 of the proposed Computer Misuse Bill and/or sections 82 and 83 of the Electronic Communications and Transactions Act.

(c) The search and seizure mechanisms provided for in the Criminal Procedure Act are not capable of inducing coerced cooperation in the execution of a search and seizure intervention. They need to be augmented in accordance with article 19 of the Cybercrime Convention. This can be done by inserting an additional provision into chapter 2 of the Criminal Procedure Act (similar to the ones contained in section 82(1)(h) of the Electronic Communications and Transactions Act and section 7(4) of the proposed Computer Misuse Bill). It is, however, doubtful whether such evidence will be admissible against an accused in a subsequent trial.

(d) The expedited preservation of stored computer data that is not retained by legislative direction[46] must be specifically provided for. This can be done either by expediting the existing search and seizure and production mechanisms or by creating a specific preservation mechanism. It is submitted that it is advisable to create a criminal law mechanism similar to an Anton Pillar order (operative in civil law context). Such a preservation mechanism will protect the privacy of data, and ensure its future availability on an expedient basis.

(e) Sections 21(1)(a) and 25(1) of the Criminal Procedure Act stipulate that a magistrate or justice may issue warrants only within her specific area of jurisdiction. This becomes problematic in networked computing environments, in that multiple warrants may have to be obtained from different magistrates in different jurisdictions. This issue has also not been covered by section 7 of the proposed Computer Misuse Bill. The problem can be addressed by the insertion of additional jurisdictional bases in the relevant provisions of the Criminal Procedure Act. Magistrates and justices must also be capable of issuing search warrants under chapter 2 of the Criminal Procedure Act where the subject of an investigation is present in South Africa at the time when the warrant is applied for or where information pertinent to the investigation is accessible from within the area of jurisdiction of the court. It is recommended that the restrictive jurisdictional requirements in sections 21(1)(a) and 25(1) be updated. This can be done by aligning sections 21 and 25 of the Criminal Procedure Act with section 83(2) of the Electronic Communications and Transactions Act.

(f) For the purposes of making and attending to urgent mutual legal assistance requests through expedited means of communication as required under article 25(3) of the Cybercrime Convention, it is advised that certain levels of security and authentication required for purposes of these communications be prescribed. Prescribing what

---

[46] Communication-related information that is retained pursuant to section 30 of the RICPCIA and those categories of computer data that are retained on the basis of specific legislation, read with section 16 of the Electronic Communications and Transactions Act.

constitutes acceptable expedited means of formal confirmation of mutual legal assistance requests is also recommended. This can be done by means of direction or regulation under section 33 of the International Cooperation in Criminal Matters Act.

(g) In the interests of expediency, it is recommended that both the Minister of Justice and Constitutional Development and the Director General: Justice and Constitutional Development (as the South African Central Authority) make use of the delegation provisos in sections 28 and 29 of the International Cooperation in Criminal Matters Act.

(h) Under section 27(9)(a)-(d) of the Cybercrime Convention, in respect of requests from foreign states to South Africa, South Africa must facilitate direct communication between judicial authorities or Interpol in urgent cases. Under article 27(9)(e) of the Cybercrime Convention, South Africa must also allow for direct communication between the judicial authorities or Interpol in respect of mutual legal assistance requests that can be complied with by the requested party, without making use of coercive action. It is doubtful whether a declaration under article 40, read with article 27(9)(e) of the Cybercrime Convention, to direct that urgent mutual legal assistance requests from foreign states be addressed to the South African central authority, will be in the interests of efficiency. It is therefore recommended that South Africa does not avail itself of this reservation. It is, however, imperative to ensure that all the respective role-players are informed about developments.

(i) Barring the one exception in section 16 of the International Cooperation in Criminal Matters Act that enables the Minister of Justice and Constitutional Development to apply the dual criminality requirement in respect of the mutual execution of sentences and compulsory orders, there is no statement of grounds for refusal in the International Cooperation in Criminal Matters Act. This is a *lacuna* in South African domestic legislation and it needs to be addressed. In the absence of a legislative intervention and where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between South Africa and a requesting or requested state, articles 27 and 28 of the Cybercrime Convention apply. Under article 29(5), the assertion of any other basis (than those provided for in articles 27 and 28) for refusing a mutual legal assistance request for the preservation of traffic data is precluded. Mutual assistance in respect of the offences referred to in articles 2 to 11 of the Cybercrime Convention may, moreover, not be refused solely on the ground that the request concerns an offence which it considers a fiscal offence. Refusal of assistance on data protection grounds may also be invoked only in exceptional cases.

(j) The Minister of Justice and Constitutional Development should, either by directive or by regulation under section 33 of the International Cooperation in Criminal Matters Act, require collaboration between the South African central authority and the National Prosecuting Authority as a matter of course. Since a number of agencies, including the

Department of Foreign Affairs, the SAPS, Interpol, Correctional Services, the National Prosecuting Authority (the National Prosecution Service/the Asset Forfeiture Unit/the Directorate of Special Operations) are involved in some or other facet of international cooperation, it would be good practice to establish a coordinating mechanism at an operational level. Such a coordination mechanism could contribute greatly in achieving the aim of prompt and speedy action and establishing synergy between the efforts of all the stakeholders. Alternatively, it is recommended that the central authority be required to submit any mutual legal assistance request not only to the magistrate within whose area of jurisdiction the witness resides or is believed to be present, but also to the National Director of Public Prosecutions.

(k) An amendment must be considered to the International Cooperation in Criminal Matters Act, providing for any one magistrate to be designated with concomitant trans-jurisdictional powers to deal with the whole of a request in terms of section 7 of the International Cooperation in Criminal Matters Act. This would prevent cumbersome delays and problems with coordination in instances where a request for mutual legal assistance relates to various magisterial districts, as is the case more often than not when one is collecting electronic evidence.

(l) The aspects of confidentiality and use limitations are not addressed in the International Cooperation in Criminal Matters Act. This is a *lacuna* in the South African mutual legal assistance framework and it needs to be addressed. In the absence of a legislative intervention and where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between South Africa and a requesting or requested state, articles 27 and 28 of the Cybercrime Convention apply.

(m) In order to eliminate any uncertainty in this respect, it is recommended that the Minister of Justice and Constitutional Development directs that all mutual legal assistance requests by foreign states to South Africa be channelled via section 7 of the International Cooperation in Criminal Matters Act. This can be done by direction or regulation under section 33 of the International Cooperation in Criminal Matters Act.

(n) It is recommended that the South African central authority facilitates discussions between the relevant role-players to sensibly consider the designation of a point of contact for the purposes of the Cybercrime Convention 24 hour a day, 7 days a week network. It is envisaged that this is a matter that will also greatly benefit from establishing a coordinating mechanism under the auspices of the central authority at an operational level.

(o) In popularising mutual legal assistance practice, it is suggested that the South African central authority should consider compiling and circulating guidelines for the contents of both outgoing and incoming requests to all role players in the mutual legal assistance framework. The compilation of a database of the relevant legislation and requirements

for the requests of foreign states, including their contact particulars, would also be very useful.

(p) Nothing in the South African mutual legal assistance framework prohibits consultation, as required under article 22(5) of the Cybercrime Convention, with a view to determining the most appropriate jurisdiction for prosecution(s), when more than one party claims jurisdiction over an offence. It is, however, recommended that explicit provision is made in the South African mutual legal assistance framework for the requirement of consultation with a view to determining the most appropriate jurisdiction for prosecution(s) when more than one party claims jurisdiction over an offence. This can be done under the regulations issued by the Minister of Justice and Constitutional Development in terms of section 33 of the International Cooperation in Criminal Matters Act.

(q) It is recommended that the Minister provides that South Africa must promptly inform a requesting party if a preservation order will not ensure the future availability of the required data, or will threaten the confidentiality of, or otherwise prejudice the investigation of the requesting party. This can be done by means of a direction or regulation under section 33 of the International Cooperation in Criminal Matters Act.

(r) It is advised that the Minister makes explicit provision for the spontaneous production of information, as provided for under article 26 of the Cybercrime Convention. This can be done by means of direction or regulation under section 33 of International Cooperation in Criminal Matters Act. There is no prohibition in South Africa against the spontaneous production of investigative information.

7.4 *Shutdown*[47]

From the output of this research, it is clear that the ubiquity of computer networks and information superhighways, and the connectivity of virtually every workstation to the global community that has been created as its default have ramifications that have yet to be worked out in more detail. To the researcher (at least), it is now equally clear that an attempt to address (some of) these legal ramifications is a truly humbling experience that requires enormous perseverance. This thesis aspires to be nothing more than an attempt made by a lawyer, bugged and/or blessed with the heart of a "techie", to contribute her "bit" [48] toward

---

47 The phrase or term "shut down", "shut-down" or "shutdown" means to quit all applications and to turn off the computer. Allow the researcher the indulgence of pertinently pointing out here that the phrase "shut up", as opposed to "shut-down", has quite different implications (such as to imprison, confine or enclose; to close completely, as in to "shut up shop"; to stop speaking or to cause someone else to stop speaking). Once again, the researcher does not subscribe to the pretence of modernist objectivity, and she concedes the possibility that in this thesis the distinction between the phrases "shut-down" and "shut-up" may have blurred/converged to some extent (once again, this perception is in the eye of the beholder – see paragraph 1.4 above). All criticisms, qualms and chuckles in this respect will be, if not co-entertained, at least tolerated by the author (see footnote 16 in paragraph 1.1 above). Answers.com "Shutdown" found on the Internet http://www.answers.com/topic/shutdown 2 and Answers.com "Shut up" found on the Internet http://www.answers.com/topic/shut-up 1.

48 See paragraph 2.2.1 above for explanations of the terms "bit" and "byte".

furthering South Africa's legal response to technological developments. New technologies challenge existing legal concepts, and there has always been a significant lag between the development of technology and a suitable response by the law:

> In respect of many technological developments the legal response can be divided into four stages. Step one could be taken from a Dickensian novel as elderly judges raise their eyes from the parchments littering the bench and, quill pen in quivering hand demand of counsel 'a **computer**, pray tell, what is that? Is it used by the Beatles?' Following denial comes a stage of grudging acceptance of the technology's existence but assertion that the application of general principles will suffice to resolve any disputes. ... This stage may last for a number of years. ... The attempt to remedy the situation brings us on to the third of our stages, where specific statutory provision is made for aspects of the new technology. ... Most legal systems are currently hovering between the second and third stages described above. However, whilst computer specific statutes have a valuable role to play in filling *lacunae* in existing legal provisions, making exceptional provision for the regulation of technology whose application is becoming the norm is often an unsatisfactory approach. The final stage differs perhaps only in degree, but sees recognition of the implications of the technology at the very core of the law.[49]

It is up to all the bold and beautiful and/or young and restless brothers and sisters in South Africa who happen to be born to the Third Wave to "byte" the bullet and do their "bit" in fast-tracking South Africa through the different stages of its legal response to technological developments. Despite the global digital divide,[50] the African continent in general, and South Africa in particular, could take their places with pride among the nations of the Information Age. After all, Africa carries much less baggage from the Second Wave of industrialism than some other continents. The fact that South Africa was one of the first signatories of the Cybercrime Convention can already be considered a large step in the right direction.[51]

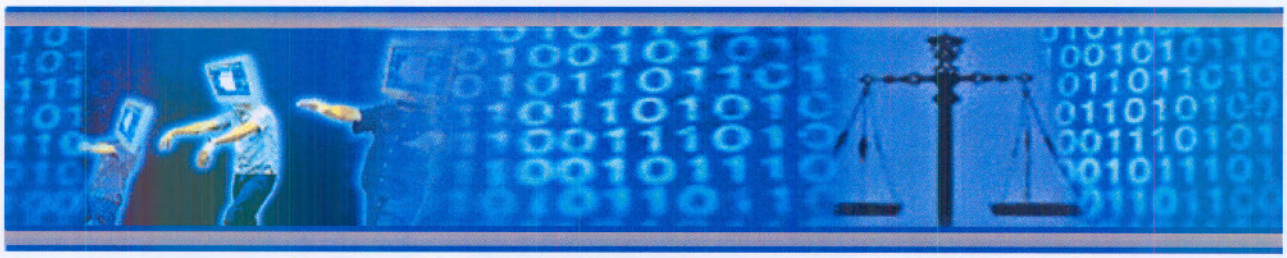
---

49 Lloyd *Information Technology Law* xlv-xlvi.

50 The "global digital divide" is a term used to describe disparities between developed and developing countries in respect of opportunities to access the Internet and the information, educational and business opportunities tied to this access. Unlike the traditional note of the "digital divide" between social classes, the "global digital divide" is essentially a geographical division. The notion of a digital divide resonates with scepticism about claims of the revolutionary power of the Internet and an emerging utopian Information Society. The Internet has been hailed as the great equaliser – a revolutionary technological tool that enables the efficient transfer of information on a global scale. See Answers.com "Global digital divide" found on the Internet http://www.answers.com/topic/gloabl-digital-divide 2 and Answers.com "Digital divide" found on the Internet http://www.answers.com/%22Digital%20Divide%22 3.

51 Van der Merwe 2003 *THRHR* 44.

BIBLIOGRAPHY



BIBLIOGRAPHY

BOOKS AND PERIODICALS

A

Acker JR and Brody DC	Criminal Procedure A Contemporary Perspective (2nd ed) (Jones and Bartlett New York 2004)
Adair Jr and David N	"Looking at the Law" 2001 Federal Probation 76 – 80
Aldesco Al	"Notes & Comments: The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime" 2002 Loyola of Los Angeles Entertainment Law Review 81 – 122
American Bankers Association	Computer Crime Participant's Manual National Seminar Program (American Bankers Association Washington 1985)
Anderson RJ	"Whither Cryptography?" 1994 Information Management & Computer Security 13 – 20
Anon	"Cybercrime Convention: One False Move, and you're a Hacker!" 2001 UNESCO Courier 33
Anon	"UK Will Lead IT Push In EU" 2005 Accountancymagazine.com 73 – 75
Anon	"Search and Seizure Order" 2002 Informa UK Ltd Intellectual Property Newsletter 1 – 3
Association of Chief Police Officers	Good Practice Guide for Computer-Based Electronic Evidence (Home Office United Kingdom 1999)
Atrens J not found	"A Comparison of Canadian and American Constitutional Law relating to Search and Seizure" 1994 Southwestern Journal of Law and Trade in the Americas 29 – 47
August R	"International Cyber-Jurisdiction: A Comparative Analysis" 2002 American Business Law Journal 531 – 573

B

Baron RMF	"Comment: A Critique of the International Cybercrime Treaty" 2002 The Catholic University of America CommLaw Conspectus 263 – 278
Bates TJ	"Computer Evidence – Recent Issues" 2000 Information Security Technical Report 15 – 22
Bayens SK	"The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology" 2000 Drake Law Review 239 – 278
Bharvada K	"Electronic Signatures, Biometrics and PKI in the UK" 2002 International Review of Law, Computers & Technology 265-275
Blanpain R (ed)	The Impact of the Internet and New Technologies on the Workplace (Kluwer Law International The Hague 2002)
Bohn RH and Muster LS	"The Dawn of the Computer Age: How the Fourth Amendment Applies to Warrant Searches and Seizures of Electronically Stored Information" 2003 Suffolk Journal of Trial & Appellate Advocacy 63 – 80
Bowrey K	Law and Internet Cultures (Cambridge University Press Cambridge 2005)
Bramwell A	"Data Retention" 2006 Privacy and Data Protection 9 -12

Brenner SW	"Distributed Security: Moving away from Reactive Law Enforcement" 2005 International Journal of Communications Law & Policy 1 – 43
Brenner SW and Frederiksen BA	"Computer Searches and Seizures: Some Unresolved Issues" 2001/2002 Michigan Telecommunications and Technology Law Review 39 – 113
Brill AE, Fletcher NB Jr and Munro RJ (ed)	Cybercrime & Security (Oceana Pubns New York 1998)
Bristows PW	"Anti-Terrorism Legislation – UK Big Brother Never Forgets – The Data Retention Provisions of the Anti-Terrorism, Crime and Security Act 2001" 2002 Computer Law & Security Report 205-207
Brooks CJ	A+ Certification Concepts & Practice Fourth Edition (Pearson Education Inc New Jersey 2004)
Burnes C	"Carnivore – Big Brother in the US" 2000 Privacy and Data Protection Ltd 8 – 10
Burnes C	"Email and Internet Usage Policies in the United States" 2002 Privacy and Data Protection 12
Buys R (ed)	Cyberlaw @ SA (Van Schaik Pretoria 2000)
Buys R (ed)	Cyberlaw @ SA II (Van Schaik Pretoria 2004)
Byrne JJ	I-Net Certification Study System (IDG Books Worldwide United States of America 2000)

C

Cachalia A et al	Fundamental Rights in the New Constitution (Juta Kenwyn 1994)
Carnelley M	"Interactive Gambling: A South African Comparative Perspective Part II – Regulatory Frameworks in Selected Jurisdictions" 2002 Obiter 1 – 26
Carr and Williams (eds)	Computers and Law (Intellect Books New York 1994)
Carstens J and Lucouw P	E-Commerce in Practice (Corals Publishers Vanderbijlpark 2004)
Case Note	R v Central Criminal Court, ex p. Bright, Alton and Rusbridger "Divisional Court – PACE Special Procedure Production Orders, the Official Secrets Act 1989 and the Public Interest in Disclosure" 2001 Journal of Criminal Law 1 – 10
Casey E (ed)	Handbook of Computer Crime Investigation (Academic Press London 2002)
Chellis J, Perkins C and Strebe M	MSCE Networking Essentials Study Guide Second Edition (SYBEX Inc Alameda 1998)
Chissick M and Kelman A	Electronic Commerce Law and Practice Third Edition (Sweet & Maxwell London 2002)
Coleman C and Sapte DW	"Cyberspace Security: Securing Cyberspace – New Laws and Developing Strategies" 2003 Computer Law & Security Report 131-136
Collier D	"Criminal Law and the Internet" in Buys R (ed) Cyberlaw @ SA II (Juta Pretoria 2004) 319-347
CSIR-Defencetek	CSIR FACTS Forensics Auditing Crime Technology Support (CSIR Pretoria 2003)

D

D'Oliveira J	"International Co-operation in Criminal Matters: The South African Contribution" 2003 SACJ 323 – 369

Davis C, Philipp A and Cowen D — Hacking Exposed Computer Forensics Secrets & Solutions (McGraw-Hill / Osborne California 2005)

Deveci HA — "Personal Jurisdiction: Where Cyberspace Meets the Real World – Part 1" 2005 Computer Law & Security Report 464 – 477

Deveci HA — "Personal Jurisdiction: Where Cyberspace Meets the Real World – Part II" 2006 Computer Law & Security Report 39 – 45

Du Toit E et al — Commentary on the Criminal Procedure Act (Juta Pretoria 2005)

E

Earnshaw C — "Search and Seize orders – The Role and Responsibility of the Forensic Computing Specialist" 2003 C & L Computer Forensics 11-13

Endeshaw A — "Admissibility of Evidence and Juristiction relating to Online Fraud" 1998 Computer Law and Security Report 29 – 33

Esen R — "Trusted Third Parties and Key Recovery" 2001 New Law Journal 340 – 341

Esen R — "Cybercrime: A Growing Problem" 2002 Journal of Criminal Law 269 – 284

F

Farmer D and Venema W — Forensic Discovery (Pearson Education Inc Upper Saddle River 2005)

FBI/CART — Conducting Searches in a Computer Environment (Rev 2/21/97) (FBI/CART Washington 1997)

Ferrera GR, Lichtenstein SD, Reder MEK, Bird RC and Schiano WT — Cyberlaw Text and Cases 2nd eds (Thomson South-Western West Ohio 2004)

Fisher J — "Cyber Rights, Protection, and Markets: Article The Draft Convention on Cybercrime: Potential Constitutional Conflicts" 2001 University of West Los Angeles Law Review 339 – 361

Flanagan A — "The Law and Computer Crime: Reading the Script of Reform" 2005 International Journal of Law and Information Technology 98 – 117

Forouzan BA with Fegan SC — TCP/IP Protocol Suite Second Edition (The McGraw-Hill Companies, Inc United States of America 2003)

Freedman W — "A Privilege for Members of the Clergy: Smit v Van Niekerk (reconsidered)" 1997 SACJ 74 – 85

Freeman EH — "Internet Service Providers and Search Warrants" 2003 Information Systems Security 6 – 9

Freeman EH — "Search and Seizure of Computer Equipment" 1999 Information Systems Security 10 – 15

G

Gahtan AM, Kratz MPJ and Mann JF — Internet Law A Practical Guide for Legal and Business Professionals (Carswell Ontario 1998)

Gibson W — Neuromancer (Phantasia Press Washington 1984)

Goemans C and Dumortier J — "Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-line Anonymity" 161-183 in Nicoll C, Prins JEJ and Van Dellen MJM Digital Anonymity and the Law (TMC Asser Press The Hague 2003)

Goodburn D and Ngoye M "Privacy and the Internet" in Buys R (ed) Cyberlaw @ SA II (Van Schaik Pretoria 2004)171-196

Goodwin B "Police Charter Will Boost Fight Against Cybercrime" 2002 Computer Weekly x

Goodwin B "Victory for Campaigners as Government Agrees to Update the Computer Misuse Act" 2003 Computer Weekly 12

Gordon LA et al "2005 CSI/FBI Computer Crime and Security Survey" 2005 Computer Security Institute 1 – 25

Grant I "Court and Spark" 1995 Intelligence Publication 40 – 43

Gruenwald J "Drafty Treaty" 2000 Interactive Week 18

Guidance Software "New Incident Response Mandates under Gramm-Leach-Bliley" 2005 Guidance Software 1 – 4

H

Haberle CA "Search and Seizure – Stop and Frisk – Evidence Seized Incident to an Arrest that is based upon a Police Officer's Computer Record that Failed to Indicate that the Arrest Warrant had been Quashed, due to an Error Committed by Court Personnel, is within the Scope of the Good Faith Exception to the Exclusionary Rule – Arizona v. Evans, 115 S. Ct 1185 (1995)" 1995/1996 Seton Hall Law Review 866 – 896

Hafner K Cyberpunk (Simon & Schuster New York 1992)

Hall KL (ed) The Oxford Companion to the Supreme Court of the United States (Oxford University Press Inc New York 1992)

Hannibal M and Mounteford L Criminal Litigation (Oxford University Press Inc New York 2005)

Harris S All in One CISSP Certification Exam Guide (McGraw-Hill / Osborne California 2002)

Hellums SD "Bits and Bytes: The Carnivore Initiative and the Search and Seizure of Electronic Mail" 2002 William & Mary Bill of Rights Journal 827 – 858

Herold R (ed) The Privacy Papers: Managing Technology, Consumer, Employee and Legislative Actions (Auerbach Publications London 2002)

Hiemstra VG Suid-Afrikaanse Strafproses Vierde Uitgawe (Butterworths Durban 1987)

Hiley E "Criminal Law – Production Orders under the Police and Criminal Evidence Act – Two Important Cases" 1987 Law Society's Guardian Gazette 3088 – 3090

Hiller J and Cohen R Internet Law & Policy (Prentice Hall New York- 2002)

Home Office Fraud and Technology Crimes Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources (Home Office Online Report London 2004)

Hopkins BR The Non-Profit's Guide to Internet Communications Law (John Wiley & Sons New Jersey 2003)

Hopkins SL "Cybercrime Convention: A Positive Beginning to a Long Road Ahead" 2003 Journal of High Technology Law 101 – 121

I

Itzikowitz A "Constitutional Validity of the Search and Seizure and Related Provision of the Exchange Control Regulations" 1995 11 SAJHR 281

J

Jackson DW — "Protection of Privacy in the Search and Seizure of Email: Is the United States doomed to an Orwellian Future?" 1999 Temple Environmental Law & Technology Journal 97 – 119

Jackson HA — "Arizona v. Evans: Expanding Exclusionary Rule exceptions and Contracting Fouth Amendment Protection" 1996 The Journal of Criminal Law & Criminology 1201-1227.

Johnson CW — "Survey of Washington Search and Seizure Law: 2005 Update" 2005 Seattle University Law Review 467-503

Johnson MD and Gardner A E — "Access to Search Warrant Materials: Balancing Competing Interests Pre -Indictment" 2003 University of Arkansas at Little Rock Law Review 771 – 817

Jones N — "UK Cyber-cop Highlights Key Computer Crimes" 2003 Computer Fraud and Security 6

Jones R — "Your day in court – the role of the Expert Witness" 2004 Digital Investigation 18 – 20

Jones W — Jones 2001 Computer Fraud and Security 6.

Jordaan W — "Draadwerk! IT maak van die mens nog 'n dinosourus" 2006 Perspektief 1

Joubert CJ (ed) — Applied Law for Police Officials First Edition (Technikon SA Florida 1999)

Joubert JJ (ed) — Criminal Procedure Handbook Sixth Edition (Juta Lansdowne 2003)

Justice College — Search and Seizure (Justice College Pretoria 2004)

K

Kent J and Ghavalas B — "The Unique Challenges of Collecting Corporate Evidence" 2005 Digital Investigation 239 – 243

Kerr O — "Cybercrime Update: Tenth Circuit Sheds Light on Intermingling Rules for Search and Seizure Computers" 2003 Northwestern University Law Review 608 Journal of Internet Law 25 – 28

Keyser M — "The Council of Europe Convention on Cybercrime" 2003 Florida State University Journal of Transnational Law & Policy 287 – 326

Klang M — "A Critical Look at the Regulation of Computer Viruses" 2003 International Journal of Law and IT 162 – 184

Klosek J — "Convention on Cybercrime Raises Concern about Data Privacy" 2002 Cyberspace Lawyer 2 – 6

Koops BJ and Prins C — "Public ICT Policy" 2000 Computer Law & Security Report 311 – 316

Kreston SS — "Computer Search and Seizure issues in Internet Crimes against Children Cases" 2004 Rutgers Computer and Technology Law Journal 327 – 373

Kriegler J — Hiemstra Suid-Afrikaanse Strafproses (Butterworths Durban 1993)

Kruse II WG and Heiser JG — Computer Forensics Incident Response Essentials (Addison-Wesley Mexico City 2002)

Kuchta KJ — "Forensic Methodologies: A Computer Forensic Professional's Compass!" 2002 Information Systems Security 42 – 49

Kuras JH, Levy CK, Burns JL, Lowry SA — "Thirty-First Annual Review of Criminal Procedure: I. Investigation and Police Practices: Warrantless Searches and Seizures" 2002 Georgetown Law Journal 1130 – 1209

L

La Grand Wendell — "CNN Tapping is an Improper search" 1998 American Bar Association (ABA) Journal 39

Lawack-Davids — "The Cryptographic Dilemma: Possible Approaches to Formulating Policy in South Africa" 2001 Obiter 1-31

Lloyd IJ — Information Technology Law (Oxford University Press USA 2004)

Lo K not found — "Computer Forensics is key to Acquiring and Preserving Electronic Evidence" 2003 The Lawyers Weekly 22 – 24

Loundy DJ — Computer Crime, Information Warfare, and Economic Espionage (Carolina Academic Press United States of America 2003)

Lyon D — Surveillance After September 11 (Blackwell Oxford 2003)

M

Malan J and Venter JP — Cyber Inspectorate Research and Recommendations (CSIR Pretoria 2002)

Marler SL — "The Convention on Cybercrime: Should the United States Ratify?" 2002 New England Law Review 183 – 219

Mathieson SA — "UK Seeks All-EU Traffic Data Retention" 2005 Computer Fraud & Security 1 – 2

May C — "Computer Forensics – A Policy Decision" 2003 Computers & Law 8 – 10

Messick R — "IRS Computer Data Bank searches: An Infringement of the Fouth Amendment Search and Seizure Clause" 1985 Santa Clara Law Review 153 – 190

Meyers M and Rogers M — "Computer Forensics: The Need for Standardization and Certification" 2004 International Journal of Digital Evidence 1 – 11

Michael J — Privacy and Human Rights (Dartmouth Publishing Company Limited England 1994)

Michalson — "The Use of E-mail and the Internet in the Workplace" in Cyberlaw @ SA (Van Schaik Pretoria 2000)

Miquelon-Weismann MF — "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural due Process?" 2005 The John Marshall Journal of Computer & Information Law 329 – 360

Moore RE — Search and Seizure of Digital Evidence: An Examination of Constitutional and Procedural Issues (PhD-thesis University of Southern Mississippi 2003)

N

Nash J — Networking Essentials MCSE Study Guide (IDG Books Worldwide Inc Foster City 1998)

Neumann PG — 2000 "Inside Risks: Denial-of-Service Attacks" Association for Computing Machinery Communications of the ACM New York 136 – 140

Nicoll C, Prins JEJ and Van Dellen MJM — Digital Anonymity and the Law (TMC Asser Press The Hague 2003)

Note — Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication" 1996-1997 Harvard Law Review 1591 – 1608

Nykodym N and Taylor R "Control of Cybercrime : The world's current legislative efforts against Cybercrime" 2004 Computer Law & Security Report 390 – 395

O

O'Reilly C and Derting J "Electronic Disclosure – The Way Ahead" 2002 Computers and Law (C&L) Litigation Support 37-39

Oddis D "Combating Child Pornography on the Internet : The Council of Europe's Convention on Cybercrime" 2002 Temple International & Comparative Law Journal 477 – 518

Orwell G Orwell 1984 (Signet Classic New York1950)

P

Palfrey T "Surveillance as a Response to Crime in Cyberspace" 2000 Information & Communications Technology Law 173 – 193

Palmer GL Forensic Analysis in the Digital World (The MITRE Corporation)

Palmer M and Sinclair RB A Guide to Designing and Implementing Local and Wide Area Networks (Course Technology –ITP Canada 1999)

Paschke RT "Personal Use and Possession of Dagga: A Matter of Privacy or Prohibition" 1995 SACJ 109 – 126

Pattenden R "Litigation Privilege and Expert Opinion Evidence" 2000 International Journal of Evidence and Proof 213 – 245

Patzakis J "Computer Forensics as an Integral Component of the Information Security Enterprise" 2003 Guidance Software 1 – 5

Patzakis J "Digital Privacy Considerations" 2003 Guidance Software 1 – 8

Patzakis J and Limongelli V EnCase Legal Journal (Guidance Software Inc ??? 2005)

Patzakis J and Limongelli V "Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley" 2004 Guidance Software 1 – 8

Patzakis J, Limongelle V "Evidentiary Authentication within the EnCase Enterprise Process" 2003 Guidance Software 1 – 6

Peterson LL and Davie BS Computer Networks A Systems Approach (Morgan Kaufmann Publishers San Francisco 2003)

Plowden P and Stockdale M "A picture is worth a thousand words" 1998 New Law Journal 432

Prosise C and Mandia K Incident Response & Computer Forensics Second Edition (McGraw-Hill / Osborne California 2003)

Proust K "International Co-operation: A Commonwealth Perspective" 2003 SACJ 295 – 310

Q

Quinn K "Computer Evidence in Criminal Proceedings: Farewell to the Ill-Fated Section 69 of the Police and Criminal Evidence Act 1984" 2001 International Journal of Evidence and Proof 174-187

R

Rantala "Bureau of Justice Statistics Technical Report Pilot Test Results, 2001 Computer Security Survey – Cybercrime Against Businesses" 2004 NCJ 1 – 12

Rautenbach C "Polisie-padblokkades: 'n Grondwetlike Analise" 1999 SAPL 456 – 484

Rees P and Calleja R "Computers and Information Technology" 2002 International Journal of Electronic Commerce Law & Practice 47 – 57

Reetz RC	"Warrant Requirement for Searches of Computerized Information" 1987 BUL Review 1 – 13
Reith M, Carr C and Gunsch G	"An Examination of Digital Forensic Models" 2002 International Journal of Digital Evidence 1 – 12
Resseguie D	"Computer Searches and Seizure" 2000 Cleveland State Law Review 185 – 213
Reuter P	Introduction to the Law of Treaties Second Edition (Kegan Paul International London 1995)
Reynolds L	"Constitutional Law in the Electronic Age" 1992 Management Review 20 – 25
Rhoden, Carla	"Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruit of the Poisonous Tree and Beyond" 2002 American Journal of Criminal Law 107 – 134
Rittinghouse JW and Hancock WM	Cybersecurity Operations Handbook (Elsevier Digital Press Burlington 2003)
Room S	"Criminalising Cybercrime" 2004 New Law Journal 950 – 951
Rosen M	"The US – EU Convention on Cybercrime" 2002 UCLA Journal of Law and Technology 1 – 20
Rosenberg RS	The Social Impact of Computers Second Edition (Academic Press Inc California 1997)
Rosenblatt	"Machine of the Year" 1983 Time Magazine 46 – 52
Russell R (ed)	Stealing the Network How to Own a Continent (Syngress Publishing Inc Rockland 2004)
Rustad ML	"Private Enforcement of Cybercrime on the Electronic Frontier" 2001 Southern California Interdisciplinary Law Journal 63 – 116

S

Sadler RL	Electronic Media Law (Sage United States of America 2005)
Sammes T and Jenkinson B	Forensic Computing A Practitioner's Guide (Springer London 2000)
Schwikkard PJ and Van Der Merwe S	Principles of Evidence Second Edition (Juta Lansdowne 2002)
Seipel P	From Data Protection to Knowledge Machines (Deventer The Netherlands 1990)
Sharpe A and Russell C	Sharpe A and Russell C 2003 "The Data Retention Code – Will CSP's Jump or Will They Be Pushed?" Privacy and Data Protection 1 – 14
Sharpe S	Search and Surveillance: The Movement from Evidence to Information (Dartmouth Publishing Company Limited Aldershot 2000)
Shelly GB, Cashman TJ and Vermaat ME	Discovering Computers 2003 (Thomson Course Technology Boston 2002)
Shytov A	"Indecency on the Internet and International Law" 2005 International Journal of Law and Information Technology 260 – 280
Silvergate HA and Viles TC	"Constitutional, Legal and Ethical Considerations for Dealing with Electronic Files in the Age of Cyberspace" in Brill AE, Fletcher NB Jr and Munro RJ (ed) Cybercrime & Security (New York 1998)
Smith GJH	Internet Law and Regulation Third Edition (Sweet & Maxwell London 2002)

Sommer P	"Policing Cybercrime: The Future for the Policing of Cybercrime" 2001Computer Fraud & Security 8 – 12
South African Law Reform Commission	Discussion Paper 109 on Privacy and Data Protection (Pretoria 2003)
South African Law Reform Commission	Discussion Paper 99 on Computer-related Crime: Preliminary Proposals for Reform in respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects (Project 108) (Pretoria 2001)
South African Law Reform Commission	Project 98 International Cooperation in Criminal Prosecutions Pretoria 1995)
South African Law Reform Commission	Discussion Paper 78 Review of Security Legislation: The Interception and Monitoring Prohibition Act 127 of 1992 (Pretoria 1997)
South African Law Reform Commssion	Review of the Law of Evidence Project 6 (Pretoria October 1986)
South African Police Service	National Instruction 2/2002: Search and Seizure (SAPS Pretoria 2002)
Sprack J	A Practical Approach to Criminal Procedure 10th ed (Oxford University Press Oxford 2004)
Sprinkel SC	"Global Internet Regulation: The Residual effects of the "I Love You" computer virus and the Draft Convention on Cybercrime" 2002 Suffolk Transnational Law Review 491 – 514
Stahlman MR	"Military Justice Symposium – Volume II: New Developments in Search and Seizure: A Little Bit of Everything" 2001 Army Lawyer 20 – 34
Stavrou A	Mission Impossible? E-Security in South Africa's Commercial and Financial Sectors (Institute for Security Studies Pretoria 2002)
Stein AR	"The Unexceptional Problem of Jurisdiction in Cyberspace" 1998 The International Lawyer 1167 – 1191
Steytler N	Constitutional Criminal Procedure A Commentary on the Constitution of the Republic of South Africa, 1996 (Butterworths Durban 2004)
Stone R	The Law of Entry, Search, and Seizure (4th ed) (Oxford University Press New York 2005)
Strömer TH	Online-Recht Rechtsfragen im Internet (Dunkt.Verlag Heidelberg 2002)

T

Takach GS	Computer Law Essentials of Canadian Law (Irwin Law Toronto 1998)
Talleur T	"Digital Evidence: The Moral Challenge" 2002 International Journal of Digital Evidence 1 – 4
Tanenbaum AS	Computer Networks Fourth Edition (Prentice Hall PTR New Jersey 2003)
The P&DP Team	"Confidence and Data Protection: The United States Patriot Act" 2002 Privacy and Data Protection 12
Toffler A	The Third Wave (Bantam London 1980)

U

V

Vacca JR	Computer Forensics Computer Crime Scene Investigation Second

	Edition (Charles River Media Inc Massachusetts 2005)
Van der Berg	"Total Control TV" 2005 SA Computer Magazine 35 – 39
Van der Merwe D	Computers and the Law (2nd ed) (Juta Kenwyn 2000)
Van der Merwe DP	Computers and the Law (1st ed) (Juta Kenwyn 1986)
Van der Merwe DP	"Computer Crime" 2003 THRHR 30 – 44
Van der Merwe DP	"Computer Crime – Recent National and International Developments" 2003 THRHR 30 – 44
Van der Merwe DP	"Onlangse Ontwikkelinge op die Raakvlak tussen Rekenaars en die Reg" 1991 THRHR 95 – 105.
Van der Merwe DP	"Copyright and Computers, with Special Reference to the Internet" 1998 SALJ 180 – 201
Van der Merwe DP	"Die Regsimplikasies van Elektroniese Handeldryf" 1999 THRHR 226 – 240
Volonino L	"Electronic Evidence and Computer Forensics" 2003 Communications of the Association for Information Systems 1-24

W

Walden I	"Harmonising Computer Crime Laws in Europe" 2004 European Journal of Crime, Criminal Law and Criminal Justice 321 – 336
Walden I	"Data Security Law" 2005 Institute of Computer and Communications Law Studies 1 – 27
Wall DS	Cyberspace Crime (Ashgate Publishing Washington 2003)
Wasik M	Crime and the Computer (Clarenden Press Oxford 1991)
Watney MM	"Die Strafregtelike en Prosedurele Middele ter Bekamping van Kubermisdaad (Deel 1)" 2003 TSAR 56 – 74.
Watney MM	"Die Strafregtelike en Prosedurele Middele ter Bekamping van Kubermisdaad (Deel 2)" 2003 TSAR 241 – 257
Watney MM	"Identity Theft – The Dangerous Imposter" 2004 De Rebus 511 – 519
Watney MM	"Surgical Intervention and the Investigation of Crime" 2004 TSAR 587 – 594
Weber AM	"Annual review of Law and Technology: VIII. Foreign & International Law: A. Cyberlaw: Cybercrime: The Council of Europe's Convention on Cybercrime" 2003 Berkeley Technology Law Journal 425 – 446
Webster F	Theories of the Information Society (Routledge London 1995)
Webster F	Theories of the Information Society (Routledge London 1995)
Whitcomb CM	"A Historical Perspective of Digital Evidence: A Forensic Scientist's view" 2002 International Journal of Digital Evidence 1 – 9
Whitley EA and Hosein I	"Policy Discourse and Data Retention: The Technology Politics of Surveillance in the United Kingdom" 2005Telecommunications Policy 857-874
Wilding E	Computer Evidence A Forensic Investigations Handbook (Sweet & Maxwell London 1997)
Winick R	"Searches and Seizures of Computers and Computer Data" 1994 Harvard Journal of Law & Technology 75 – 128

X

Y

Young JM "Surfing while Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation: A Critical Analysis of the Council of Europe Convention on Cybercrime & the Canadian Lawful Access Proposal" 2004 International Journal of Communications Law and Policy available at SSRN: http://ssrn.com/abstract=653962

Z

Zeffert DT, Paizes AP and Skeen A St Q The South African Law of Evidence (LexisNexis Butterworths Durban 2003)

Zetter K, McLeod RG "New Technologies, Laws Threaten Privacy" 2002 PC World 22

CASE LAW

A

A M & S Europe Ltd v Commission of the European Communities [1983] QB 878

A v B and C [2002] EWCA Civ 337 [2003] QB 195

Agnello v US 269 US 20 (1925)

Alana Shoars v Epson America Incorporated Cal Lexis 3670 (1994)

Alex Cartage (Pty) Ltd v Minister of Transport 1986 (2) SA 838 (E)

American Postal Workers Union Columbus Area Local AFL-CIO v United States Postal Service 871 F 2d 556 (6TH Cir 1989)

Andersen Consulting LLP v UOP and Bickel & Brewer 991 F Supp 1041 (ND Ill 1998)

Andresen v Minister of Justice 1954 (2) SA 473 (W)

Anton Pillar KG v Manufacturing Processes Ltd [1976] Ch 55 [1976] 1 All ER 779

Arizona v Hicks 480 US 321 (1987)

Attorney-General Transvaal v Kader 1991 (4) SA 727 (A)

B

Baily v Wilson [1968] Crim LR 617

Barclays Bank plc v Taylor; Trustee Savings Bank of Wales and Border Counties v Taylor [1989] 3 All ER 563 [1989] 1 WLR 1066

Barnes v State of Missouri 960 F 2d 63 (8TH Cir 1992)

Beheersmaatschappij Helling I NV v Magistrate Cape Town 2005 JOL 13758 (C)

Berglund v City of Maplewood 173 F Supp 2d 935 (D Minn 2001)

Bernstein v Bester NO 1996 (4) BCLR 449 (CC)

Black v United States 172 FRD 511 (SD Fla 1997)

Blue Chip Consultants (Pty) Ltd v Shamrock 2002 (3) SA 231 (W)

Bogoshi v Van Vuuren NO; Bogoshi v Director Office for Serious Economic Offences 1993 (2) SACR 98 (T)

Bohach v City of Reno 932 F Supp 1232 (D Nev 1996)

Booi v Minister of Safety and Security 1995 (2) SACR 465 (O)

Botha v Botha 1972 (2) SA 559 (N)

Boyd v United States 116 US 616 (1886)

Brazil v Chief Constable of Surrey [1983] 3 All ER 537 77 Cr App Rep 237

Brinegar v US 338 US 160 (1949)

British Steel Corporation and Granada Television Ltd [1981] AC 1096

Brown v Waddell 50 F 3d 285 (4TH Cir 1995)

Bumper v North Carolina 391 US 543 (1968)

C

Cales v Howell 635 F Supp 454 1985

California v Greenwood 486 US 35 (1988)

Callis v Gunn [1964] 1 QB 495 [1963] 3 All ER 677

Case v Minister of Safety and Security; Curtis v Minister of Safety and Security 1996 (5) BCLR 609 (CC)

Cave v Johannes NO 1949 (1) SA 72 (T)

Chapman v United States 365 US 610 (5TH Cir 1960)

Chappell v The United Kingdom [1989] ECHR 4 [1990] 12 EHRR 1

Cheadle, Thompson & Haysom v Minister of Law and Order 1986 (2) SA 279 (W)

Chic Fashions (West Wales) Ltd v Jones [1968] 2 QB 299 [1968] 1 All ER 229

Chimel v California 395 US 752 (1969)

Choonara v Minister of Law and Order 1992 (1) SACR 239 (W)

Cine Films (Pty) Ltd v Commissioner of Police 1971 (4) SA 574 (W)

Cine Films (Pty) Ltd v Commissioner of Police 1972 (2) SA 254 (A)

Coetzee v Attorney-General KwaZulu-Natal 1997 (1) SACR 546 (D)

Colorado v Bertine 479 US 367 (1987)

Columbia Picture Industries v Robinson [1986] 3 All ER 338

Commonwealth v Georgia 310A 2d 334 (1973)

Community Repeater Services CC v Minister of Justice 2000 (2) SACR 592 (SE)

Concalves v Minister of Law and Order 1993 (1) SA 161 (W)

Connally v Georgia 429 US 245 (1977)

Control Magistrate Durban v Azanian Peoples Organisation 1986 (3) SA 394 (A)

Coolidge v New Hampshire 403 US 443 (1970)

Coppolino v State 223 So 2d 68 (FLA Dist Ct App 1968)

Costello v Chief Constable of Derbyshire Constabulary [2000] QB 427 [2001] EWCA Civ 381

Couch v United States 409 US 322 (1972)

Cremieux v France [1993] IIHRL 8 (1993) 16 EHRR 357

Cresto Machines (Edms) Bpk v Die Afdeling Speur-offisier SA Polisie Noord-Transvaal 1972 (1) SA 376 (A)

Crowley v Cybersource Corporation and Amazon.com Inc 166 F Supp 2d 1263 (ND Cal 2001)

D

Dabelstein v Hildebrandt 1996 (3) SA 42 (C)

Dallison v Caffery [1965] 1 QB 348 [1984] 2 All ER 610

Darbo v DPP [1992] Crim LR 56

Datnis Motors (Midlands) (Pty) Ltd v Minister of Law and Order 1988 (1) SA 503 (N)

Daubert v Merrell Dow Pharmaceuticals 509 US 579 (1993)

Davis v Tip NO 1996 (1) SA 1152 (W)

Davis v Additional Magistrate Johannesburg 1989 (4) SA 299 (W)

Davis v Gracey 111 F 3d 1472 (10TH Cir 1997)

Davis v State 497 So 2d 1344 (Fla 5d DCA 1986)

De Reuck v Director of Public Prosecutions, Witwatersrand Local Division 2003 (12) BCLR 1333 (CC) [SACR 445 (CC)

De Wet v Willers NO 1953 (4) SA 124 (T)

DeMassa v Nunez 747 F 2d 1283 (9TH Cir 1984)

DePugh v Sutton 917 F Supp 690 (WD Mo 1996)

Divisional Commissioner of SA Police Witwatersrand Area v SA Associated Newspapers Ltd 1966 (2) SA 503 (A)

Dookie v Minister of Law and Order 1991 (2) SACR 153 (D)

Douglas v Hello! Ltd (No 3) [2005] EWCA Civ 595 [2006] QB 125 [2003] EWHC 786 [2003] All ER 996

DPP v McKeown and Jones [1997] 1 All ER 737

Dumbell v Roberts [1944] 1 All ER 326

Dyani v Minister of Safety and Security 2001 (1) SACR 634 (Tk)

E

Eiser v Vuna Health Care (Pty) Ltd (1998) JOL 1736 (W)

Entick v Carrington (1765) 19 How St Tri 1030 95 ER 807

Equisec (Pty) Ltd v Rodriques 1999 (3) SA 113 (W)

Ex Parte Dabelstein v Hildebrandt 1996 2 All SA 17 (C)

Ex Parte Jackson 96 US 727 (1877)

Ex Parte Minister of Safety and Security: In Re S v Walters 2002 (4) SA 613 (CC)

Extra Dimension v Kruger NO 2004 (2) SACR 493 (T)

F

Faulkner v Willetts [1982] RTR 159 [1983] Crim LR 453 DC

Federal Trade Commission v Netscape Communications Corp 196 FRD 559 (ND Cal 2000)

Fedics Group (Pty) Ltd v Matus 1997 (9) BCLR 1199 (C)

Ferreira v Levin NO and Vryenhoek v Powell NO 1996 (1) BCLR 1 (CC)

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 (2) SA 451 (A)

Fitt v UK App No 29777/96

Florida v Hammonds 557 So 2d 179 (Fla Ed DCA 1990)

Florida v Jimeno 500 US 248 (1991)

Florida v Wells 495 US 1 (1990)

Francis & Francis (a firm) v Central Criminal Court [1988] 3 All ER 775 88 Cr App Rep 213

Frank Truman Export Ltd v Metropolitan Police Commissioner [1977] QB 952 [1977] 3 All ER 431 64 Cr App Rep 248

Fraser v Nationwide Mutual Insurance Co 135 F Supp 2d 623 (ED Pa 2001)

Frazier v State 172 F 3d 1268 (10TH Cir 1999)

French v Hay 89 US 231 (1874)

Frye v US 293 F 1013 (DC Ct App 1923)

Funke v France [1993] ECHR 7 16 EHRR 297

G

Ghani v Jones [1970] 1 QB 693 [1969] 3 ALL ER 1700

Goncalves v Minister of Law and Order 1993 (1) SA 161 (W)

Goodwin v The United Kingdom 17488/90 [1996] ECHR 16 (1996) EHRR 123

Gosschalk v Rossouw 1996 (2) SA 476 (C)

Graham v Peat (1801) 1 East 244 102 ER 95

Guest v Leis 255 F 3d 325 (6TH Cir 2001)

H

H Heiman, Maasdorp & Barker v Barker v Secretary for Inland Revenue 1968 (4) SA 160 (W)

Hako v Minister of Safety and Security 1996 (2) SA 891 (TkS)

Halford v The United Kingdom [1997] ECHR 32 (1997) 24 EHRR 523

Hammonds v State 1999 WL 669383 (Alabama 1999)

Harksen v Attorney-General of the Province of the Cape of Good Hope 1998 (2) SACR 681 (C)

Haynes v Commissioner for Inland Revenue 2000 (6) BCLR 596 (Tk)

Haysom v Additional Magistrate Cape Town; S v Haysom 1979 (3) SA 155 (C)

Heads v Chief Constable of Humberside Police CO/250/86 12 May 1986 DC

Hessel v O'Hearn 977 F 2d 299 (7TH Cir 1992)

Highstead Entertainment (Pty) Ltd t/a 'The Club' v Minister of Law and Order 1993 (2) SACR 625 (C)

Hill v MCI Worldcom Communications Inc 120 F Supp 2d 1194 (SD Iowa 2000)

Hodes v Deputy Commissioner of Police 1959 (4) SA 650 (C)

Hoffa v United States 385 US 293 (1966)

Horton v California 496 US 128 (1990)

Howe v Mabuya 1961 (2) SA 635 (D)

Hyundai Motor Distributors (Pty) Ltd v Smit NO 2000 (1) SACR 503 (T)

I

Illinois v Gates 462 US 213 (1983)

Illinois v Lafayette 462 US 640 (1983)

Illinois v McArthur 531 US 326 (2000)

Illinois v Rodriguez 497 US 177 (1990)

In re Doubleclick Inc Privacy Litigation 154 F Supp 2d 497 (SDNY 2001)

In Re Grand Jury Proceedings: Subpoenas Duces Tecum, Larry Danbom and Western Union v United States 827 F 2d 301 (8th Cir 1987)

In re Grand Jury Subpoena Duces Tecum 846 F Supp 11 (SDNY 1994)

In Re Grand Jury Subpoena Served upon Simon Horowitz 482 F 2d 72 (2d Cir 1973)

In Re Search Warrant for Law Offices Executed on March 19 1992 153 FRD 55 (SDNY 1994)

In re: Grand Jury Investigation Concerning Solid State Devices v United States 130 F 3d 853 (9TH Cir 1997)

In the Matter of Search Warrant for K-Sports Inc 163 FRD 594 (CD Cal 1995)

In the Matter of the Application of the United States of America for an Order Authorising an In-Progress Trace of Wire Communications Over Telephone Facilities v Mountain States Telephone & Telegraph Company 616 F 2d 1122 (9TH Cir 1980)

In the Matter of the Application of Lafayette Academy Inc. v United States 610 F 2d 1 (1ST Cir 1979)

In the matter of the Application of the United States of America for an order Authorising the Installation of a Pen Register or Touch-Tone Decoder and a Terminating Trap, Bell Telephone Company of Pennsylvania 610 F 2d 1148 (3RD Cir 1979)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Limited; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO 2001 (1) SA 545 (CC)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2000 (2)

SACR 349 (CC)

Ismael v Durban City Council 1973 (2) SA 362 (N)

J

Jackelson 1926 TPD 685

Jeffrey v Black [1978] QB 490 [1978] 1 All ER 555

Jimenez v State of Florida 643 So 2d 70 (Fla 2d DCA 1994)

JL Foti Construction Co Inc v Donovan Secretary of Labor Occupational Safety and Health Review Commission 786 F 2d 1165 (6TH Cir 1986)

Jones & Jones v Lloyd [1981] Crim LR 637

K

Katz v United States 389 US 347 (1967)

Kent Pharmaceutical Ltd v Director of the Serious Fraud Office [2002] EWHC 3023

Key v Attorney-General Cape of Good Hope Provincial Division 1996 (6) BCLR 788 (CC)

Kiggen v Burger (2002) JOL 9444 (C)

Klass v Federal Republic of Germany (1978) 2 EHRR 214 5029/71 [1978] ECHR 4

Klein v Attorney-General Witwatersrand Local Division 1995 (2) SACR 210 (W)

Knox v Anderton [1983] 76 Cr App Rep 156

Kostovski v The Netherlands (1989) 12 EHRR 434[1990] ECHR 8

Kumho Tire Co et al v Carmichael et al 526 US 137 (1999)

Kuruma v The Queen [1955] AC 197

Kyllo v United States 533 US 27 (2000)

L

Lamb v Director of Public Prosecutions [1990] Crim LR 58 154 JP 381

Lambert and Palmer Communications Incorporated v Polk County Iowa The City of Des Moines 723 F Supp 128 (SD Iowa 1989)

Lambert v Roberts [1981] 2 All ER 15 72 Cr App Rep 223

Laurence v Verhoef NNO 1993 (1) SACR 552 (W)

Lavers v Hein & Far BK 1998 (3) SA 195 (SCA)

Lenz Township Co (Pty) Ltd v Munnick 1959 (4) SA 567 (T)

Levack v The Regional Magistrate Wynberg 1999 (2) SACR 151 (C)

Lindley v Rutter [1981] QB 128

Lorse v The Netherlands [2003] ECHR 59 (2003) 37 EHRR 3

LSD Ltd v Vachell 1918 WLD 127

M

Magajane v North West Gambling Board Case 2006 CCT 49/05

Magmoed v Janse van Rensburg 1993 (1) SACR 67 (A)

Mahlangu v S [1999] JOL 4784 (W)

Mahomed v Attorney-General of Natal 1998 (1) SACR 73 (N)

Mahomed v NDPP 2005 JDR 1004 (W)

Malone v Metropolitan Police Commissioner [1979] Ch 344

Mandela v Minister of Prisons 1983 (1) SA 938 (A)

Mandela v Minister of Safety and Security 1995 (2) SACR 397 (W)

Mapp v Ohio 367 US 643 (1961)

Marcel v Commissioner of Police of the Metropolis [1992] Ch 225 [1992] 1 All ER 72

Mary Beth G v City of Chicago 723 F 2d 1263 (7TH Cir 1983)

Masokanye v Additional Magistrate Stellenbosch 1994 (1) SACR 21 (C)

Massachusetts v Sheppard 468 US 981 (1984)

Matisonn v Additional Magistrate Cape Town 1980 (2) SA 619 (C)

Mbutuma v The MEC for Safety and Security of the Eastern Province 1998 (1) SACR 367 (Tk)

McArdle v Egan [1933] All ER Rep 611 150 LT 412

McGann v Northeast Illinois Regional Commuter Rail Road Corporation D/B/A Metra/Metropolitan Rail 8 F 3d 1174 (7TH Cir 1993)

McGrath v Chief Constable of the Lancashire Constabulary; R v Crown Court at Preston Ex parte cGrath The Times 27 October 1992 CO/1176/92

McLeod v Commissioner of Police of the Metropolis [1994] 4 All ER 553

McLeod v The United Kingdom 24755/94 [1998] ECHR 92 (1999) 27 EHRR 493

McLorie v Oxford [1982] QB 1290

Mendes v Kitching NO 1995 (2) SACR 634 (E)

Minister of Justice v Desai 1948 (3) SA 473 (W)

Minister of Justice v Desai NO 1948 (3) SA 395 (A)

Minister of Safety and Security v Gaqa 2002 (1) SACR 654 (C)

Minister of Safety and Security v Xaba 2003 (2) SA 703 (D)

Minister van Polisie v Gamble 1979 (4) SA 759 (A)

Mistry v Interim National Medical and Dental Council of South Africa 1997 (7) BCLR 933 (D)

Mitchell v Hodes NNO 2003 (1) SACR 524 (C)

Mohamed v President of the Republic of South Africa 2001 (2) SA 1145 (C)

Moore PCC (NS) 463 17 ER 462)

Munusamy v Hefer NO 2004 (5) BCLR 508 (O)

N

Naidoo v Minister of Law and Order 1990 (2) SA 158 (W)

Narlis v South African Bank of Athens 1976 (2) SA 573 (A)

Natal Law Society v N 1985 (4) SA 115 (N)

National Director of Public Prosecutions v Carolus 1999 (2) SACR 27 (C)

National Director of Public Prosecutions v Tam 2004 (1) SACR 126

National Media Limited v Jooste 1996 (3) SA 262 (A)

National Transport Commission v Chetty's Motor Transport (Pty) Ltd 1972 (3) SA 726 (A)

National Union of South African Students v Divisional Commissioner South African Police Cape Western Division 1971 (2) SA 553 (C)

Ndabeni v Minister of Law and Order 1984 (3) SA 500 (D)

Ndlovu v Minister of Police Transkei 1993 (3) SA 91 (TK)

Nedcor Bank Limited v Behardien 2000 (1) SA 307 (C)

Nel v Deputy Commissioner of Police Grahamstown 1953 (1) SA 487 (E)

Nel v Le Roux NO 1996 (1) SACR 572 (CC) 1996 (4) BCLR 592 (CC)

New Jersey v TLO 469 US 325 1984

Newfields v Ryan; Ballentine v Florida Tex Oil Co 91 F 2d 700 (5TH Cir 1937)

Ngubani v Divisional Commissioner South African Police Witwatersrand Division 1963 (1) SA 316 (W)

Nicholls v Ely Beet Sugar Factory Limited [1931] 2 Ch 84 [1931] All ER Rep 154

Niemietz v Germany 13710/88 [1992] ECHR 80 (1993) 16 EHRR 97

Nombembe v The Minister of Safety and Security 1998 (2) SACR 160 (Tk)

North v Russell 427 US 328 (1976)

NTL Group and Ipswich Crown Court [2002] EWHC 1585

Ntoyakhe v Minister of Safety and Security 1993(2) SASV 625 (OK)

Ntoyakhe v Minister of Safety and Security 2000 (1) SA 257 (E)

Ntoyakhe v The Minister of Safety and Security 1999 (2) SACR 349 (E)

NUSAS v Divisional Commissioner South African Police 1971 (2) SA 533 (C)

O

O'Hara v The United Kingdom 37555/97 [2001] ECHR 598

O'Hara v United Kingdom (2002) 34 EHRR 32

O'Connor v Ortega 480 US 709 (1986)

O'Hara v Chief Constable of the Royal Ulster Constabulary [1997] 1 All ER 129 [1997] 1 Cr App Rep 447

Ohio v Robinette 519 US 33 (1996)

Oliver v United States 466 US 170 (1984)

Olmstead v US 277 US 438 (1928)

Organizacion JD LTDA and Manufacturers JD LTDA v United States Department of Justice and United States Drug Enforcement Administration 124 F 3d 354 (2ND Cir 1997)

P

Parbhoo v Getz NO 1997 (4) SA 1095 (CC)

Parkhurst v Trapp 77 F 3d 707 (3RD Cir 1996)

Park-Ross v Director: Office for Serious Economic Offences 1995 (2) SA 148 (C) 1995 (1) SASV 530 (K) 1995 2 BCLR 198 (C)

Payton v New York 445 US 573 (1980)

People v Marx 54 126 Cal Rptr 350 (1975)

Powell NO v Van Der Merwe NO 2005 (1) SACR 317 2005 (5) SA 62 (SCA)

Powell v Tordoff 911 F Supp 1184 (ND Iowa 1995)

Preston v UK [1997] 6 EHRLR 695

Pretoria Portland Cement Co Ltd v The Competition Commission [2002] JOL 9808 (A)

Prinsloo v Newman 1975 (1) SA 481 (A)

Protea Technology Limited v Wainer 1997 (9) BCLR 1225 (W)

Pullen, NO, Bartman, NO & Orr, NO v Waja 1929 TPD 838

Q

R

R (on application of H) v Inland Revenue Commissioners [2002] EWHC 2164 (Admin)

R (on application of Paul Da Costa & Co) v Thames Magistrates' Court [2002] EWHC 40 (Admin)

R (on the application of Kent Pharmaceuticals Limited) v Director of the Serious Fraud Office [2003] EWHC 3002 (ADMIN) [2003] All ER (D) 298 (Dec)

R (on the application of Kent Pharmaceuticals Limited) v Director of the Serious Fraud Office [2004] EWCA Civ 1494

R (on the application of Rottman) v Commissioner of Police of the Metropolis [2002] UKHL 20 [2002] 2 All ER 865 [2002] 2 WLR 1315

R v Atkinson [1976] Crim LR 307

R v Badham [1987] Crim LR 202

R v Bagas 1952 (1) SA 437 (A)

R v Baker [1996] Crim LR 55

R v Baker [1997] Crim LR 497 The Times 26 November 1996

R v Beckford [1992] 94 Cr App R 43

R v Beghin 1933 EDL 24

R v Borden [1994] (119) DLR (4^{TH}) 74 (SCC)

R v Boyes [1861] 121 ER 730

R v Camane 1925 AD 570

R v Canale [1990] 2 All ER 187 [1990] Crim LR 329

R v Central Criminal Court and ex parte AJD Holdings [1992] Crim LR 669

R v Central Criminal Court ex parte Adegbesan [1986] 3 All ER 113

R v Central Criminal Court ex parte Bright [2001] 2 All ER 244

R v Central Criminal Court ex parte Brown [1992] The Times 7 September 1992 CO/0881/92

R v Central Criminal Court ex parte Francis & Francis [1988] 1 All ER 677 87 Cr App Rep 104

R v Chalkley; R v Jeffries [1998] QB 848 [1998] 2 All ER 155

R v Chesterfield Justices ex parte Bramley [2000] QB 576 [2000] 1 All ER 411 [2000] 1 Cr App Rep 486 [2000] Crim LR 385

R v Chief Constable of Lancashire ex parte Parker and McGrath [1993] 2 All ER 56

R v Chief Constable of Warwickshire ex parte Fitzpatrick [1998] 1 All ER 65 [1998] Crim LR 290

R v Coote [1861-1873] All ER 1113

R v Crown Cour of Manchester ex parte Taylor [1988] Crim LR 386 DC

R v Crown Court at Acton ex parte Layton [1993] Crim LR 458

R v Crown Court at Bristol ex parte Bristol Press and Picture Agency Limited [1987] Crim LR 329

R v Crown Court at Guildford ex parte Director of Public Prosecutions; R v Crown Court at Southwark ex parte Bowles [1998] QB 243 [1996] 4 All ER 961 [1997] 1 Cr App Rep 436 [1997] 2 WLR 936

R v Crown Court at Inner London Sessions ex parte Baines & Baines (a firm) [1988] 1 QB 579 [1987] 3 All ER 1025 57 Cr App Rep 111

R v Crown Court at Leicester ex parte Director of Public Prosecutions [1987] 3 All ER 654

R v Crown Court at Lewes ex parte Hill [1991] 93 Cr App Rep 60

R v Crown Court at Liverpool ex parte Wimpey plc [1991] Crim LR 635

R v Crown Court at Manchester ex parte Rogers [1999] 4 All ER 35 [1999] 1 WLR 832 [1999] 2 Cr App Rep 267 [1999] Crim LR 743

R v Crown Court at Northampton exparte DPP [1991] 93 Cr App Rep 376

R v Crown Court at Snaresbrook ex parte Director of Public Prosecutions [1988] 1 All ER 315

R v Crown Court at Southwark ex parte Bowles [1998] 2 All ER 193 [1998] 2 Cr App R 187

R v Crown Court at Southwark ex parte Customs and Excise Commissioners [1990] 1 QB 250 [1989] 3 All ER 673

R v Davies [2002] EWCA Crim 85

R v Debele 1956 (4) SA 570 (A)

R v Guildhall Magistrate's Court ex parte Primlaks Holdings Co. (Panama) Inc [1990] 1 QB 261

R v Heap 13 October 1994 (Transcript: John Larking)

R v Heard [1937] CPD 401

R v Hubbard [1921] TPD 433

R v Hunt 16 Cr App R (S) 87 [1994] Crim LR 747

R v Inland Revenue Commissioners ex parte Rossminster Limited [1980] AC 952 [1979] 3 All ER 385 70 Cr App Rep 159

R v Jamba 1947 (4) SA 228 (C)

R v Jones R v Smith [1976] 3 All ER 54 63 Cr App Rep 47

R v Justice of the Peace for Peterborough ex parte Hicks [1978] 1 All ER 225

R v Keane [1994] 2 All ER 478 [1995] Crim LR 225

R v Khan [1996] 3 All ER 289

R v Kuyper 1915 TPD 308

R v Kuzwayo 1949 (3) SA 761 (A)

R v Leeds Crown Court ex parte Switalski [1991] Crim LR 559

R v Leeds Magistrates' Court ex parte Dumbleton [1993] Crim LR 866 CO/2129/92

R v Liverpool Crown Court Ex parte Wimpy plc [1991] Crim LR 635 The Times 24 April 1991 The Independent 11 April 1991 CO/595/91

R v Longman [1998] 1 WLR 619

R v Maidstone Crown Court ex parte Rogers [1999] 1 WLR 832

R v Maidstone Crown Court ex parte Waitt CO/1420/87 [1988] Crim LR 384

R v McMillan 1958 (4) SA 461 (A)

R v Mkwayi 1956 (3) SA 406 (E)

R v Nani 1930 EDL 12

R v Parker 1966 (2) SA 56 (RA)

R v Quinn Lexis UK CD 510 [1995] 1 Cr App Rep 480

R v R [1994] 4 All ER 260 [1995] 1 Cr App Rep 183

R v Reading Justices Chief Constable of Avon and Somerset and Intervention Board for Agricultural Produce ex parte South West Meat Limited [1992] Crim LR 672 CO/1605/1991

R v Rorke [1915] AD 145

R v Rudolf 1950 (2) SA 522 (C)

R v Sang [1980] AC 402 [1979] 2 All ER 1222

R v Sas [1918] CPD 346

R v Shephard [1991] Lexis UK CD 179 93 Cr App Rep 139

R v Sole 2004 (2) SACR 599 (Les)

R v South Western Magistrate's Court ex parte Cofie [1997] 1 WLR 885

R v Southampton Crown Court ex parte J & P [1993] Crim LR 962 CO/1421/92

R v Southwark Crown Court ex parte Sorsky Defries [1996] Crim LR 195 CO/283/95

R v Sulski [1935] TPD 292

R v Thames Magistrates' Court ex parte Hormz [1983] 163 JP 19

R v Thornley [1981] 72 Cr App R 302 [1981] Crim LR 637

R v Turner [1995] 2 Cr App R 94

R v Van Heerden 1958 (3) SA 150 (T)

R v Wright [1994] Crim LR 55

R v Zawele 1937 AD 342

Rabie v Minister of Police 1984 (1) SA 786 (W)

Rademeyer v Attorney-General 1955 (1) SA 444 (T)

Rakas v Illinois 439 US 128 (1978)

Regina v Christou Regina v Wright (Christopher) [1992] QB 979

Regina v Guildhall Magistrates' Court ex parte Primlaks Holdings Co (Panama) Inc [1990] 1 QB 261

Reuters Group PLC v Viljoen NNO 2001 (12) BCLR 1265 (C)

Rex v Jackelson 1926 TPD 685

Rex v Makanyaka 1948 (3) SA 1225 (O)

Rex v Nani 1930 EDL 12

Rex v Rudolf 1950 (2) SA 522 (C)

Reynolds v Commissioner of Police of the Metropolis [1984] 3 All ER 649

Richards v Wisconsin 520 US 385 (1997)

Robson v Hallett [1967] 2 All ER 407

Roman v Williams NO 1997 (9) BCLR 1267 (K)

Rotary Sealing Services CC v National Prosecuting Authority 2005 JOL 15492 (T)

Rowe and Davis v UK App No 28901/95

Rudolph v Commissioner for Inland Revenue 1996 (7) BCLR 889 (CC) 11

Rudolph v Commissioner for Inland Revenue 1997 (4) SA 391 (SCA)

Rukwira v Director of Public Prosecutions [1993] 158 JP 65 [1993] Crim LR 882

Rumping v Director of Public Prosecutions [1964] AC 814 [1962] 3 All ER 256 [1962] 3 WLR 763 46 Cr App Rep 398

S

S v Khanyapa 1979 (1) SA 824 (A)

S v Adams 1993 (1) SACR 611 (C)

S v Agnew 1996 (2) SACR 535 (C)

S v Baleka (1) 1986 (4) SA 192 (T)

S v Bekesi 1992 (1) SACR 39 (C)

S v Boshoff 1981 (1) SA 393 (T)
S v Bosma, S v Kleinschmidt 1980 (1) SA 852 (A)
S v Bosman 1978 (3) SA 903 (O)
S v Bosman; S v Kleinschmidt 1979 (1) SA 277 (O)
S v Botha (1) 1995 (2) SACR 598 (W)
S v Botha (2) 1995 (2) SACR 605 (W)
S v Carneson 1962 (3) SA 437 (T)
S v Coetzee 1997 (4) BCLR 437 (CC)
S v Cornelissen; Cornelissen v Zeelie NO 1994 (2) SACR 41 (W)
S v De Blom 1977 (3) SA 513 (A)
S v Desai 1997 (1) SACR 38 (W)
S v Diale 1994 (1) SACR 221 (BG)
S v Dlamini 1973 (1) SA 144 (A)
S v Dlamini 1978 (4) SA 917 (N)
S v Dlamini; S v Dladla; S v Joubert; S v Schietekat 1999 (2) SACR 51 (CC)
S v Du Toit 2004 (1) SACR 341 (T)
S v Dzukuda 2000 (2) SACR 443 (CC)
S v Forbes 1970 (2) SA 594 (C)
S v Govender 1967 (2) SA 121 (N)
S v Groesbeeck 1969 (4) SA 383 (O)
S v Gumede 1998 (5) BCLR 530 (D)
S v Hammer 1994 (2) SACR 496 (C)
S v Harper 1981 (1) SA 88 (D)
S v Haysom 1979 (3) SA 155 (C)
S v Hendrix 1979 (3) SA 816 (D)
S v Heyman 1966 (4) SA 598 (A)
S v Hlangothe 1979 (4) SA 199 (B)
S v Huma 1995 (2) SACR 411 (W)
S v Jackelson 1926 TPD 685
S v Johardien 1990 (1) SA 1026 (C)
S v Khan 1997 (2) SACR 611 (SCA)
S v Kheswa 1997 (2) SACR 638 (D)
S v Kidson 1999 (1) SACR 338
S v Kumalo 1992 (2) SASV 411 (N)
S v Lange 1963 (4) SA 941 (N)
S v Leepile 1986 (2) SA 352 (W)
S v Leepile 1990 (3) SA 988 (W)
S v Lottering 1999 (12) BCLR 1478 (N)
S v Louw 2000 (2) SACR 714 (T)

S v Lubbe 1981 (2) SA 854 (C)
S v Lunngile 1999 (2) SACR 597 (SCA)
S v Lwane 1966 (2) SA 433 (A)
S v M 2000 (2) SACR 474 (N)
S v Madiba 1998 (1) BCLR 38 (D)
S v Maduna 1978 (2) SA 777 (D)
S v Mahlangu 2000 (1) SACR 565 (W)
S v Makwanyane 1995 (6) BCLR 665 (CC)
S v Maluleke 1993 (1) SACR 649 (T)
S v Maphumulo 1996 (2) SACR 84 (N)
S v Mataung 1962 (3) SA 611 (O)
S v Mathebula 1997 (1) SACR 10 (W)
S v Matison 1981 (3) SA 302 (A)
S v Matsane 1978 (3) SA 821 (T)
S v Maunye 2002 (1) SACR 266 (T)
S v Mayekiso 1996 (9) BCLR 1168 (C)
S v Mbuli 2003 (1) SACR 97 (SCA)
S v Melani 1996 (2) BCLR 174 (E)
S v Mnanzana 1966 (3) SA 38 (T)
S v Mnyamana 1990 (1) SACR 137 (A)
S v Mokoena 2003 (1) SACR 74 (T)
S v Molobi 1976 (2) SA 301 (W)
S v Moloto 1991 (1) SACR 617 (T)
S v Mongale 1979 (3) SA 669 (B)
S v Motloutsi 1996 (1) SACR 78 (C)
S v Mpetha (1) 1982 (2) SA 253 (C)
S v Mpetha (2) 1983 (1) SA 576 (C)
S v Mpumlo 1986 (3) SA 485 (E)
S v Mqubasi 1993 (1) SACR 198 (SE)
S v Mthenjane 1979 (2) SA 105 (A)
S v Nader 1963 (1) SA 843 (O)
S v Naidoo 1974 (4) SA 574 (N)
S v Naidoo 1998 JOL 1804 (D)
S v Ncube 1976 (1) SA 798 (RA)
S v Nell 1967 (4) SA 489 (SWA)
S v Nkosi 1990 (1) SACR 509 (N)
S v Nombewu 1996 (2) SACR 396 (E)
S v Nyengane 1996 (2) SACR 520 (E)
S v Phohlo 1987 (3) SA 27 (O)

S v Pogrund 1961 (3) SA 868 (T)
S v Pogrund 1974 (1) SA 244 (T)
S v Ramaligela 1983 (2) SA 424 (V)
S v Ramgobin 1986 (4) SA 117 (N)
S v Russell 1977 (4) SA 291 (C)
S v Safatsa 1988 (1) SA 868 (A)
S v Schoor 1993 (1) SACR 202 (E)
S v SE Mbongwa Unreported Case No 1/2001 delivered on 28 June 2001 (OPD)
S v Seals 1990 (1) SACR 38 (C)
S v Sebejan 1997 (1) SACR 626 (W)
S v Seseane 2000 (2) SACR 225 (O)
S v Sheehama 1991 (2) SA 860 (A)
S v Sihlobo [2004] JOL12831 (TK)
S v Singh 1975 (1) SA 330 (N)
S v Sithole 1991 (4) SA 94 (W)
S v Smith 1984 (1) SA 583 (A)
S v Taylor 1991 (2) SACR 69 (C)
S v Toubie 2004 (1) SACR 530 (W)
S v Van Schoor 1993 (1) SACR 202 (E)
S v Vengetsamy 1972 (4) SA 351 (D)
S v Waite 1978 (3) SA 896 (O)
S v Weinberg 1966 (4) SA 660 (A)
S v Zondi 1968 (1) SA 709 (N)
S v Zuma 1995 (4) BCLR 401 (SA)
SA Police v SA Associated Newspapers 1966 (2) SA 503 (A)
SASOL III (Edms) Bpk v Minister van Wet en Orde 1991 (3) SA 766 (T)
Scarborough Borough Council v Adams and Adams [1983] JPL 673 (1983) 47 P&CR 133 DC
Schmerber v State of California (1966) 348 US 757
Schmid v State of Alaska (1980) 615 P 2d 565
Schneckloth v Bustamonte 412 US 218 (1973)
Schwimmer v United States 232 F 2d 855 (8th Cir 1956)
Sea Point Computer Bureau Pty Ltd v McLoughlin and De Wet NNO 1997 (2) SA 636 (W)
Seccombe v Attorney General 1919 TPD 270
Securities and Law Enforcement Employees, District Council 82 v Carey 737 F 2d 187 (2ND Cir 1984)
Sega Enterprises Limited Sega of America Inc v MAPHIA 948 F Supp 923 (ND Cal 1996)
Semanye's Case [1558-1774] All ER Rep 62
Senior v Holdsworth ex parte Independent Television News Limited [1976] 1 QB 23
Shaabin Bin Hussien and Chong Fook Kam on Appeal from the Federal Court of Malaysia [1970] AC 942
Shadwick v City of Tampa 407 US 345 (1972)

Shenton v Tyler [1939] 1 All ER 827 (CA)

Shoba v Officer Commanding Temporary Police Camp Wagendrift Dam; Maphanga v Officer Commanding South African Police Murder and Robbery Unit Pietermaritzburg 1995 (4) SA 1 (A)

Sigwebedlana v Minister of Police (1999) JOL 1756 (Tk)

Silverman v US 365 US 505 (1961)

Silwana v Magistrate District of Piketberg 2003 (2) SACR 310 (C)

Skinner Secretary of Transportation v Railway Labor Executive Association 489 US 602 (1988)

Slade v Guscott [1981] 72 Cr App R 302 No 78/06556

Smacsoft (Pty) Ltd v Schindler (1997) JOL 1770 (C)

Smit & Maritz Attorneys v Lourens NO 2002 (1) SACR 152 (W)

Smit v Van Niekerk NO 1976 (4) SA 293 (A)

Smith v Maryland 442 US 735 (1979)

Smith, Tabata & van Heerden v Minister of Law and Order 1989 (3) SA 627 (E)

Snook v Mannion [1982] RTR 321 [1982] Crim LR 601 DC

South African Rugby Football Union v President of the Republic of South Africa 1998 (4) SA 296 (T)

South Dakota v Opperman 428 US 364 (1976)

Stanford v Texas 379 US 476 (1965)

State ex rel Macy v One (1) Pioneer CD-ROM Changer 891 P2d 600 (Okla Civ App 100 1994)

State Wide Photocopy v Tokai Financial Services Inc 909 F Supp 137 (SDNY 1995)

Steve Jackson Games Inc v United States Secret Service 36 F 3d 457 (5TH Cir 1994)

Steve Jackson Games Inc v United States Secret Service 816 F Supp 432 (WD Tex 1993)

Stoner v California 376 US 483 (1964)

Supreme Gaming CC v Minister of Safety and Security 2000 (3) SA 608 (SCA)

Swain v Spinney 117 F 3d 1 (1ST Cir 1997)

T

Terry v Ohio 392 US 1 (1968)

The National Director of Public Prosecutions v Carolus 1999 (2) SACR 27 (C)

The State v Carneson 1962 (3) SA 437 (T)

The State v Chamane 1962 (2) SA 428 (A)

The State v Mataung 1962 (3) SA 611 (O)

Thomas v Sawkins [1935] 2 KB 249

Trulock v Freeh 275 F 3d 391 (4TH Cir 2001)

Trupiano v US 70 F Supp 764 (1947)

U

United States v New York Tel Co 434 US 159 (1977)

United States v Abbell 914 F Supp 519 (SD Fla 1995)

United States v Abbell 963 F Supp 1178 (SD Fla 1997)

United States v Alfonso 759 F 2d 728 (9TH Cir 1985)

United States v Allen 106 F 3d 695 (6TH Cir 1997)

United States v Allen 53 MJ 402 (CAAF 2000)
United States v Bach 400 F 3d 622 (8TH Cir 2005)
United States v Bach Criminal No 01-221 (PAM/ESS) US District LEXIS 22109 (2001)
United States v Ball 90 F 3d 260 (8TH Cir 1996)
United States v Balon 384 F 3d 38 (2004)
United States v Barr 605 F Supp 114 (SDNY 1985)
United States v Barry 853 F 2d 1479 (8TH Cir 1988)
United States v Barth 26 F Supp 2d 929 (WD Tex 1998)
United States v Bilanzich 771 F 2d 292 (7TH Cir 1985)
United States v Bizier 111 F 3d 214 (1ST Cir 1997)
United States v Blas 1990 US Dist LEXIS 1996 (ED Wis 1990)
United States v Block 590 F 2d 535 (4TH Cir 1978)
United States v Blok 188 F 2d 1019 (DC Cir 1951)
United States v Bradshaw 102 F 3d 204 (6TH Cir 1996)
United States v Buettner-Janusch 646 F 2d 759 (2ND Cir 1981)
United States v Buitrago Pelaez 961 F Supp 64 (SDNY 1997)
United States v Campos 221 F 3d 1143 (10TH Cir 2000)
United States v Carey 172 F 3d 1268 (10TH Cir 1999)
United States v Castro 596 F 2d 674 (5TH Cir 1979)
United States v Cervini 16 Fed Appx 865 (10TH Cir 2001)
United States v Chan 830 F Supp 531 (ND Cal 1993)
United States v Charbonneau 979 F Supp 1177 (SD Ohio 1997)
United States v Christine 687 F 2d 749 (3RD Cir 1982)
United States v Clarke 2 F 3d 81 (4TH Cir 1993)
United States v Couch 409 US 322 (1973)
United States v Cox 190 F Supp 2d 330 (NDNY 2002)
United States v David 756 F Supp 1385 (D Nev 1991)
United States v Denman 100 F 3d 399 (5TH Cir 1996)
United States v Dionisio 410 US 1 (7TH Cir 1972)
United States v Doe 61 F 3d 107 (1ST Cir 1995)
United States v Donnes 947 F 2d 1430 (10TH Cir 1991)
United States v Duran 957 F 2d 499 (7TH Cir 1992)
United States v Durham 139 F 3d 1325 (10TH Cir 1998)
United States v Elliot 50 F 3d 180 (2ND Cir 1995)
United States v Ellis 547 F 2d 863 (5TH Cir 1977)
United States v Flores 122 F Supp 2d 491 (SDNY 2000)
United States v Ford 184 F 3d 566 (6TH Cir 1999)
United States v Fregoso 60 F 3d 1314 (8TH Cir 1995)
United States v Freitas 800 F 2d 1451 (9TH Cir 1986)

United States v Galante 94 Cr 633 LMM (1995)
United States v Gargiso 456 F 2d 584 (2ND Cir 1972)
United States v Gawrysiak 972 F Supp 853 (DNJ 1997)
United States v Gomez-Soto 723 F 2d 649 (9TH Cir 1984)
United States v Gorshkov WL 1024026 at 2 (WD Wash 2001)
United States v Grant 218 F 3d 72 (1ST Cir 2000)
United States v Gray 78 F Supp 2d 524 (ED Va 1999)
United States v Grosenheider 200 F 3d 321 (5TH Cir 2000)
United States v Hall 142 F 3d 988 (7TH Cir 1998)
United States v Hambrick 55 F Supp 2d 504 (W D Va 1999)
United States v Hargus 128 F 3d 1358 (1997)
United States v Hay 231 F 3d 630 (9TH Cir 2000)
United States v Hill 19 F 3d 984 (5TH Cir 1994)
United States v Hill 322 F Supp 2d 1081 (2004)
United States v Horn 187 F 3d 781 (8TH Cir 1999)
United States v Horowitz 806 F 2d 1222 (4TH Cir 1986)
United States v Hunter 13 F Supp 2d 574 (D Vt 1998)
United States v Jacobsen 466 US 109 (1984)
United States v Jenkins 46 F 3d 447 (5TH Cir 1995)
United States v Johnson 846 F 2d 279 (5TH Cir 1988)
United States v Kahan 350 F Supp 784 (SDNY 1972)
United States v Kennedy 81 F Supp 2d 1103 (D Kan 2000)
United States v Kow 58 F 3d 423 (9TH Cir 1995)
United States v Lacy 119 F 3d 742 (9TH Cir 1997)
United States v Lam Muk Chiu 522 F 2d 330 (2ND Cir 1975)
United States v Lamb 945 F Supp 441 (NDNY 1996)
United States v Lambert 771 F 2d 83 (6TH Cir 1985)
United States v Lavin 92 Cr 326 JFK (1992)
United States v Leary 846 F 2d 592 (10TH Cir 1988)
United States v Leon 468 US 897 (1984)
United States v Licata 761 F 2d 537 (9TH Cir 1985)
United States v London 66 F 3d 1227 (1ST Cir 1995)
United States v Long 524 F 2d 660 (9TH Cir 1975)
United States v Longo 70 F Supp 2d 225 (WDNY 1999)
United States v Lynch 908 F Supp 284 (DVI 1995)
United States v Lyons 992 F 2d 1029 (10TH Cir 1993)
United States v Malbrough 922 F 2d 458 (8TH Cir 1990)
United States v Martin 157 F 3d 46 (2ND Cir 1998)
United States v Matlock 415 US 164 (1974)

United States v Maxwell 45 MJ 406 CAAF LEXIS 116 (1996)
United States v McAllister 18 F 3d 1412 (7TH Cir 1994)
United States v McConney 728 F 2d 1195 (9TH Cir 1984)
United States v McNally 473 F 2d 934 (3RD Cir 1973)
United States v Meriwether 917 F 2d 955 (6TH Cir 1990)
United States v Milian-Rodriguez 759 F 2d 1558 (11TH Cir 1985)
United States v Miller 152 F 3d 813 (8TH Cir 1998)
United States v Miller 425 US 435 (1976)
United States v Miller 688 F 2d 652 (9TH Cir 1982)
United States v Molinaro 877 F 2d 1341 (7TH Cir 1989)
United States v Montoya De Hernandez 473 US 531 (1985)
United States v Moorehead 57 F 3d 875 (9TH Cir 1995)
United States v Morton Salt Co 338 US 632 (7TH Cir 1948-1949)
United States v Most 876 F 2d 191 (DC Cir 1989)
United States v Mullins 992 F 2d 1472 (9TH Cir 1993)
United States v Murphy 506 F 2d 529 (9TH Cir 1974)
United States v Musson 650 F Supp 525 (D Colo 1986)
United States v Neill 952 F Supp 834 (DDC 1997) FN 142(5)
United States v O'Razvi 1998 WL 405048 (SDNY 1998)
United States v Oriakhi 57 F 3d 1290 (4TH Cir 1995)
United States v Ortiz 176 US 422 (1900)
United States v Ortiz 84 F 3d 977 (7TH Cir 1996)
United States v Paige 136 F 3d 1012 (5TH Cir 1998)
United States v Pena 143 F 3d 1363 (10TH Cir 1998)
United States v Pervaz 118 F 3d 1 (1ST Cir 1997)
United States v Place 462 US 696 (1983)
United States v Poulsen 41 F 3d 1330 (9TH Cir 1994)
United States v Prandy-Binett 995 F 2d 1069 (DC Cir 1993)
United States v Presler 610 F 2d 1206 (4TH Cir 1979)
United States v Price 599 F 2d 494 (2ND Cir 1979)
United States v Procopio 88 F 3d 21 (1ST Cir 1996)
United States v Rahme 813 F 2d 31 (2ND Cir 1987)
United States v Ramirez 523 US 65 (1998)
United States v Reed 15 F 3d 928 (9TH Cir 1994)
United States v Reyes 798 F 2d 380 (10TH Cir 1986)
United States v Reyes 922 F Supp 818 (SDNY 1996)
United States v Rith 164 F 3d 1323 (10TH Cir 1999)
United States v Roberts 86 F Supp 2d 678 (SD Texas 2000)
United States v Robinson 414 US 218 (1973)

United States v Rodriguez 961 F 2d 1089 (3RD Cir 1992)
United States v Rodriguez 968 F 2d 22 (10TH Cir 1992)
United States v Rodriguez 995 F 2d 776 (7TH Cir 1993)
United States v Romero-Garcia 991 F Supp 1223 (D Or 1997)
United States v Ross 456 US 798 (1982)
United States v Rossby 81 Fed Appx 109 (2003)
United States v Runyan 275 F 3d 449 (5TH Cir 2001)
United States v Sassani 139 F 3d 895 (4TH Cir 1998)
United States v Schwimmer 232 F 2d 855 (1956)
United States v Scott 83 F Supp 2d 187 (2000)
United States v Simons 206 F 3d 392 (4TH Cir 2000)
United States v Skeddle 989 F Supp 890 (ND Ohio 1997)
United States v Slanina 283 F 3d 670 (5TH Cir 2002)
United States v Smith 27 F Supp 2d 1111 (CD Ill 1998)
United States v Smythe 84 F3d 1240 (10TH Cir 1996)
United States v Sumlin 567 F2d 684 (6TH Cir 1977)
United States v Taketa 923 F2d 665 (9TH Cir 1991)
United States v Tamura 694 F2d 591 (9TH Cir 1982)
United States v Tank 200 F3d 627 (9TH Cir 2000)
United States v Thomas 114 F3d 403 (3RD Cir 1997)
United States v Trost 152 F3d 715 (7TH Cir 1998)
United States v Turner 169 F3d 84 (1ST Cir 1999)
United States v Upham 168 F3d 532 (1ST Cir 1999)
United States v Ventresca 380 US 102 (1965)
United States v Villarreal 963 F2d 770 (5TH Cir 1992)
United States v Villegas 899 F2d 1324 (2ND Cir 1990)
United States v Walker 20 F Supp 2d 971 (1998)
United States v Walker (3RD Cir 2000)
United States v Walser 275 F3d 981 (10TH Cir 2001)
United States v Walters 558 F Supp 726 (D Md 1980)
United States v Whitfield 939 F2d 1071 (DC Cir 1991)
United States v Word 806 F2d 658 (6TH Cir 1986)
United States v Zimmerman 277 F3d 426 (3RD Cir 2002)
US v Frazier (1988) 856 F2d 196
US v On Lee 343 US 757(1952)
US v Weir (1981) 657 F2d (8TH Cir) 1005

V

Van Der Merwe v Minister van Justisie 1995 (2) SACR 471 (O)
Van Vuuren v Esterhuizen NO 1996 (2) SACR 322 (A)

Van Vuuren v Esterhuizen NO 1996 (4) SA 603 (A)

Vaughn v Baldwin 950 F2d 331 (6TH Cir 1991)

W

Waddell v Eyles NO and Welsh NO 1939 TPD 198

Wainwright v Home Office [2003] UKHL 53 [2003] 4 All ER 969

Walter v United States 447 US 649 (1980)

Warden v Hayden 387 US 294 (1967)

Washington v Chisman 455 US 1 (1982)

Waterhouse v Shields 1924 CPD 155

Webb v Chief Constable of Merseyside Police; Porter v Chief Constable of Merseyside Police [2000] QB 427 [2000] 1 All ER 209

Wessels NO v Van Tonder 1997 (1) SA 616 (O)

West Virginia v Joseph T (1985)

Wikes v Wood (1763) 19 How St Tri 1153 98 ER 489

Wilson v Arkansas 514 US 927 (1995)

Wisconsin v Shroeder 2000 WL 675942 (Wisconsin Supreme Court Decision)

Wolpe v Officer Commanding South African Police Johannesburg 1955 (2) SA 87 (W)

World Wide Film Distributors(Pty) Ltd v Divisional Commissioner SA Police Cape Town 1971 (4) SA 312 (C)

X

Xola v Minister of Safety and Security 2005 JOL 14770 (Tk)

Y

Young v Minister of Safety and Security 2005 (2) SACR 437 (SE)

Yu v United States 1997 WL 423070 (SDNY Jul 29 1997)

Z

Zubulake v. UBS Warburg [S.D.N.Y May 13, 2003]

Zuma v NDPP [2006] JOL 16755 (D)

Zurcher v Stanford Daily 436 US 547 (1978)

STATUTES AND INTERNATIONAL DOCUMENTS

A

Adjustment of Fines Act 101 of 1991

Adoption and Children Act of 2002

African Charter on Human Rights and People's Rights of 1981

Alcoholic Liquor Duties Act of 1979

American Convention of Human Rights of 1969

Animals (Scientific Procedures) Act of 1986

Anti-Terrorism, Crime and Security Act of 2001

Anti-Terrorism, Crime and Security Act of 2003

Arms and Ammunition Act 75 of 1969

Aviation and Maritime Security Act of 1990

Aviation Security Act of 1982

B

Bankers' Books Evidence Act of 1879

Banking Act of 1987

Betting, Gaming and Lotteries Act of 1963

Biological Weapons Act of 1974

Businesses Act 71 of 1991

C

Cable and Broadcasting Act of 1984

Channel Tunnel (Security) Order of 1994 No 570

Child Care Act 74 of 1983

Child Protection and Sexual Predator Punishment Act of 1998

Children Act of 1989

Children and Young Persons (Harmful Publications) Act of 1955

Children and Young Persons Act of 1933

Civil Aviation Offences Act 10 of 1972

Civil Procedure Act of 1997

Civil Proceedings Evidence Act 25 of 1965

Close Corporations Act 69 of 1984

Community Development Act 3 of 1966

Companies (Northern Ireland) Order of 1986

Companies Act 61 of 1973

Companies Act of 1985

Competition Act of 1998

Computer Evidence Act 57 of 1983

Computer Misuse Act of 1990

Constitution of the Republic of South Africa 108 of 1996

Constitution of the Republic of South Africa 200 of 1993

Constitutional Court Complementary Act 13 of 1995

Contempt of Court Act of 1981

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation of 1988

Convention on the Physical Protection of Nuclear Materials of 1979

Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents of 1973

Convergence Bill GN 3382 Government Gazette 25806 3 December 2003

Copyright, Designs and Patents Act of 1988

Correctional Services Act 111 of 1998

Correctional Services Act 8 of 1959

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981

Criminal Investigations Act of 1996

Criminal Justice (International Cooperation) Act of 1990

Criminal Justice Act of 1987

Criminal Justice Act of 1988

Criminal Justice and Police Act of 2001

Criminal Justice and Public Order Act of 1994

Criminal Law Amendment Act 105 of 1997

Criminal Procedure Act 51 of 1977

Criminal Procedure Act 56 of 1955

Criminal Procedure Amendment Act 33 of 1975

Criminal Procedure and Amendment Act 29 of 1955

Criminal Procedure and Evidence Act 31 of 1917

Crossbows Act of 1987

Customs and Excise Act 91 of 1964

Customs and Excise Management Act of 1979

D

Dangerous Dogs Act of 1991

Data Protection Act of 1998

Deer Act of 1991

Defence Act 44 of 1957

Disaffection Act of 1934

Documentary Evidence from Countries in Africa Act 62 of 1993

Dogs Act of 1906

Drug and Drug Trafficking Act 140 of 1992

Drug Trafficking Act of 1994

E

Electronic Communications Act of 2000

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications Bill [B9B-2005]

Electronic Communications Privacy Act of 1986

Emergency Laws (Re-enactments and Repeals) Act of 1964

Enforcement of Foreign Civil Judgments

English Criminal Evidence Act of 1898

Estate Duty Act 45 of 1955

European Convention on Extradition of 1957

European Convention on Mutual Assistance in Criminal Matters of 1959

European Convention on the Protection of Human Rights and Fundamental Freedoms of 1950

European Council Regulation 1/2003

European Treaty

European Union Data Protection Directive 95/46 of 2000

European Union Directive 95/46/EC

European Union Directive 97/66/EC

European Union EC Directive 97/66/EC

European Union's Convention on Mutual Assistance in Criminal Matters between States adopted in 2000

Evidence (Proceedings in Other Jurisdictions) Act of 1975

Exhibitions of Hypnotism Act of 1952

Explosive Substances Act of 1883

Explosives Act of 1875

Extradition Act of 2003

Extradition Agreement between the Government of the Republic of South Africa and the Government of the United Kingdom of Swaziland of 1968

F

Federal Rules of Criminal Procedure

Federal Rules of Evidence

Finance Act of 1993

Finance Act of 1994

Finance Act of 1997

Finance Act of 2000

Financial Intelligence Centre Act 38 of 2001

Financial Services Act of 1998

Firearms (Amendment) Act of 1997

Firearms Act of 1968

Firearms Control Act 60 of 2000

Food and Environment Protection Act of 1985

Foreign Courts Evidence Act 80 of 1962

Forgery and Counterfeiting Act of 1981

Freedom of Information Act of 1966

G

Gambling Act 51 of 1965

Game Laws (Amendment) Act of 1960

Game Theft Act 105 of 1991

Gaming Act of 1968

General Law Amendment Act 62 of 1955

Government Gazette 23195 of 1 March 2002

Government Gazette 28 November 2005 No 28271 3 by General Notice 1325 of 2005

Government Notice 292 of 1968 in *Government Gazette* 2179 (Regulation Gazette 1026)

Government Notice R1411 in *Government Gazette* 19435 of 30 October 1998

H

Hague Convention on the Unlawful Seizure of Aircraft of 1970

Hague Convention on the Unlawful Seizure of Aircraft of 1970

Human Rights Act of 1998

Hydrocarbon Oil Duties Act of 1979

I

Immigration Act of 1971

Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002

Incitement to Disaffection Act of 1934

Income and Corporation Taxes Act of 1970

Income Tax Act 58 of 1962

Indecent Displays Control Act of 1981

Inheritance Tax Act of 1984

Insolvency Act 24 of 1936

Inspection of Financial Institutions Act 38 of 1984

Inspector General Act

Insurance Act 27 of 1943

Insurance Companies Act of 1982

Intelligence Services Act 38 of 1994

Intelligence Services Act 38 of 1994

Interception and Monitoring Prohibition Act 127 of 1992

Interception and Monitoring Prohibition Bill of 1999

International Convention Against the Taking of Hostages of 1979

International Convention for the Suppression of Terrorist Bombings of 1987

International Convention for the Suppression of Terrorist Financing of 1999

International Convention for the Suppression of Terrorist Financing of 1999

International Convention on the Elimination of All Forms of Racial Discrimination of 1965

International Cooperation in Criminal Matters Act 75 of 1996

International Covenant on Civil and Political Rights of 1996

International Labour Organisation Worst Forms of Child Labour Convention of 1999

Investigation of Serious Economic Offences Act 117 of 1991

J

Justices of the Peace and Commissioners of Oaths Act 16 of 1963

K

Knives Act of 1997

L

Law of Evidence Amendment Act 45 of 1988

Licensing Act of 2003

Liquor Act 27 of 1989

Local Government (Miscellaneous Provisions) Act of 1982

Local Government: Municipal Structures Act 117 of 1998

Lotteries and Amusement Parks Act of 1976

M

Magistrate's Courts Act 32 of 1944

Maintenance and Promotion of Competition Act 96 of 1979

Marketable Securities Act 32 of 1948

Medicines and Related Substances Control Act 101 of 1965

Mental Health Act of 1983

Misuse of Drugs Act of 1971

Montreal Convention on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation of 1971

N

National Prosecuting Authority Act 32 of 1998

O

Obscene Publications Act of 1959

Offences against the Person Act of 1861

Offensive Weapons Act of 1996

Official Secrets Act of 1911

Official Secrets Act of 1989

Omnibus Crime Control and Safe Streets Act of 1968

P

Pen Register and Trap and Trace Devices Statute

Performing Animals (Regulation) Act of 1925

Poaching Prevention Act of 1862

Police and Criminal Evidence Act and its Code of Practice B: Searches of Premises by Police Officers and the Seizure of Property Found by Police Officers on Persons and Premises

Police and Criminal Evidence Act Code of Practice A: Exercise by Police Officers of Statutory Powers of Stop and Search

Police and Criminal Evidence Act of 1984 (PACE)

Prevention and Combating of Corrupt Activities Act 12 of 2004

Prevention of Organised Crime Act 121 of 1998

Prevention of Organised Crime Act 140 of 1998

Prevention of Terrorism (Additional Powers) Act of 1996

Prevention of Terrorism (Temporary Provisions) Act of 1989

Privacy Protection Act 42 USC

Proceeds of Crime Act 76 of 1996

Proceeds of Crime Act of 2002

Promotion of Access to Information Act.

Protection of Animals Act of 1911

Protection of Badgers Act of 1992

Protection of Businesses Act 99 of 1978

Protection of Children Act of 1978

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

Protection of Personal Information Bill

Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms on the Continental Shelf of 1988

Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms on the Continental Shelf of 1988

Public Order Act of 1936

Public Order Act of 1986

Public Service Act of 1994 (Proclamation No. 103 of 1994)

Public Stores Act of 1875

Public Stores Act Offences against the Person Act of 1861

Q

R

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICPCIA)

Regulation of Investigatory Powers (Communications Data) Order of 2003 Chap 6

Regulation of Investigatory Powers Act of 2000 (RIPA)

Restriction of Offensive Weapons Act of 1959

Road Traffic Act of 1988

S

Scrap Metal Dealers Act of 1964

Sexual Offences Act 23 of 1957

Sexual Offences Act of 2003

South African Police Services Act 68 of 1995

Southern African Development Community on Mutual Legal Assistance

Special Investigating Units and Special Tribunals Act 74 of 1996

Sporting Events Act of 1985

Stamp Act of 1891

Statute of the Council of Europe of 1949 ETS No 001

Stock Theft Act 57 of 1959

Supreme Court Act 59 of 1959

T

Taking of Hostages Act

Taxes Management Act of 1970

Telecommunications Act 103 of 1996

Telecommunications Act of 1984

Telecommunications Data Directive (97/66/EC)

Telecoms Privacy Directive 97/66

Terrorism Act of 2000

Terrorism Act of 2006

Theatres Act of 1968

Theft Act of 1968

Title 18 of the United States Code Collection

Title III of the Omnibus Crime Control and Safe Streets Act of 1968

Tokyo Convention on Offences and Certain Other Acts committed on Board Aircraft of 1962

Town and Country Planning Act 1971

Transfer Duty Act 40 of 1949

Transport and Works Act of 1992

Treaty between the Government of the Republic of South Africa and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters of 2000

Treaty of London of 1949

U

Uncertified Securities Tax Act 31 of 1998

UNCITRAL Model Law on Electronic Commerce

United Kingdom Central Authority Guidelines for Judicial and Prosecuting Authorities

United Kingdom Computer Misuse Act of 1990

United Kingdom Police and Evidence Act of 1984

United Nations Charter

United Nations Convention against Corruption

United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (Vienna Convention)

United Nations Convention against Transnational Organised Crime of 2000

United Nations Convention on the Rights of the Child of 1989

United Nations Security Council Resolution 1373 of 2001

United States Constitution

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001

USA PATRIOT Act Additional Reauthorising Amendments Act of 2006

USA PATRIOT Improvement and Reauthorisation Act of 2005

V

Value-Added Tax Act 89 of 1991

Vehicles (Crime) Act of 2001

Video Recordings Act of 1984

Vienna Convention on the Law of Treaties of 1969

Vienna Convention United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances)

W

Wildlife and Countryside Act of 1981

Wireless Telegraphy Act of 1949

X

Y

Youth Justice and Criminal Evidence Act of 1999

Z

INTERNET

A

Adviceguide (2006) "Civil Rights – In England" found on the Internet http://www.adviceguide.org.uk/index/your_rights/the_european_union.htm [Date of use 3 March 2006] 1-6

Aldesco (2002) "Notes and Comments – The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime" found on the Internet http://elr.lls.edu/issues/v23-issue1/aldesco.pdf [Date of use 23 May 2005] 87 – 90

Altini (2003) "Commentary on the Electronic Communications and Transactions Bill, 2002" found on the Internet http://www.cliffedekker.co.za/literature/commentary/index.htm [Date of use 18 March 2004] 1 – 14

American Civil Liberties Union (2003) "Seven Reasons the Senate should Reject the International Cybercrime Treaty" http://www.aclu.org//privacy/internet/14861res20031218.html [Date of use 31 January 2006] 1 – 4

Anon (2001) "The Black Hole of Search and Seizure" found on the Internet http://www.vogon-international.co.uk/forensic-bulletin/volume3/issue6/black-hole.htm [Date of use 04 February 2006] 1 – 16

Anon (2004) "Digital Evidence Collection & Handling" found on the Internet http://faculty.ncwc.edu/toconnor/426/426lect06.htm [Date of use 24 February 2004] 1 – 25

Anon (2004) "Procedural Law" found on the Internet http://www.mobrien.com/computer_crime4.htm [Date of use 03 February 2006] 1 – 32

Anonymous (2004) "Digital Evidence Collection and Handling 2004" found on the Internet http://faculty.ncwc.edu/toconnor/426/426lect06.htm [Date of use 24 June 2004] 1 – 12

Answers.com (2006) "The Show Must Go On" found on the Internet http://www.answers.com/The%20Show%20Must%20Go%20On#after_ad1 [16 January 2006] 1 – 3

Answers.com (2006) "Biometrics" found on the Internet http://www.answers.com/biometrics [Date of use 14 March 2006] 1 – 4

Answers.com (2006) "Bios" found on the Internet http://www.answers.com/topic/bios?method=6 [Date of use 28 February 2006] 1 – 7

Answers.com (2006) "Boot" found on the Internet http://www.answers.com/boot [Date of use 7 June 2006] 1 – 13

Answers.com (2006) "Brouter" found on the Internet http://www.answers.com/brouter [Date of use15 May 2006] 1 – 2

Answers.com (2006) "Core Dump" found on the Internet http://www.answers.com/topic/core-dump [Date of use 6 June 2006] 1 – 4

Answers.com (2006) "Council of Europe" found on the Internet http://www.answers.com/topic/council-of-europe [Date of use 26 May 2006] 1 – 6

Answers.com (2006) "Cursor" found on the Internet http://www.answers.com/topic/cursor [Date of use 16 January 2006] 1 – 4

Answers.com (2006) "Digital divide" found on the Internet http://www.answers.com/%22Digital%20Divide%22 [Date of use 15 June 2006] 1 – 15

Answers.com (2006) "European Union Law" found on the Internet http://www.answers.com/topic/european-union-law [Date of use 29 March 2006] 1 – 45

Answers.com (2006) "European Union" found on the Internet http://www.answers.com/European%20Union [Date of use 17 June 2006] 1 – 33

Answers.com (2006) "Global digital divide" found on the Internet http://www.answers.com/topic/gloabl-digital-divide [Date of use 12 May 2006] 1 – 13

Answers.com (2006) "Globalization" found on the Internet http://www.answers.com/globalisation [Date of use 22 May 2006] 1 – 11

Answers.com (2006) "Handheld device" found on the Internet http://www.answers.com/topic/handheld-device?method=22 [Date of use 10 June 2006] 1 – 3

Answers.com (2006) "Hit" found on the Internet http://www.answers.com/topic.hit [Date of use 16 January 2006] 1 – 11

Answers.com (2006) "Hits" found on the Internet http://www.answers.com/topic/hits-pulp-album [Date of use 15 January 2006] 1 – 3

Answers.com (2006) "ICANN" found on the Internet http://www.answers.com/ICANN [Date of use 31 March 2006] 1 – 5

Answers.com (2006) "Internet Governance" found on the Internet http://www.answers.com/topic/internet-governance [Date of use 6 July 2006] 1 – 5

Answers.com (2006) "Metadata" found on the Internet http://www.answers.com/main/ntquery?method=e&dsid=1512&dekey=meta-data&curtab=1512_1&linktext=meta-data [Date of use 14 April 2006] 1 – 5

Answers.com (2006) "Pointer" found on the Internet http://www.answers.com/pointer [Date of use 16 January 2004] 1 – 10

Answers.com (2006) "Real-time" found on the Internet http://www.answers.com/topic/real-time-1?method=6 [Date of use14 April 2006] 1- 4

Answers.com (2006) "Server" found on the Internet http://www.answers.com/server 1 [Date of use 10 June 2006] 1 – 9

Answers.com (2006) "Star Chamber Historical Site, England (In Government) found on the Internet http://www.answers.com/Star%20Chamber [Date of use 1 March 2006] 1 – 6

Answers.com (2006) "Surf" found on the Internet http://www.answers.com/topic/surf?method=6 [Date of use 31 March 2006] 1 – 5

Answers.com "Root Domain" found on the Internet http://www.answers.com/main/ntquery?method=4&dsid=1512&dekey=root+domain... [Date of use 28 February 2006] 1– 3

Answers.com "Search engine" found on the Internet http://www.answers.com/topic/search-engine [Date of use 10 June 2006] 1 – 7

Answers.com "Shut up" found on the Internet http://www.answers.com/topic/shut-up [Date of use 10 June 2006] 1 – 2

Answers.com "Shutdown" found on the Internet http://www.answers.com/topic/shutdown [Date of use 7 June 2006] 1 – 3

Aus CERT (2006) "Australian Computer Crime and Security Survey" found on the Internet http://www.auscert.org.au/images/ACCSS2006.pdf [Date of use 18 April 2006] 1 – 40

B

Bacard 2006 "Anonymous Remailer FAQ" found on the Internet http://www.andrebacard.com/remail.html [Date of access 14 May 2006] 1-7

Banisar D (2000) "Love Letter's Last Victim" found on the Internet http://www.securityfocus.com/news/39 [Date of use 31 January 2006] 1 – 3

Best J (2006) c/Net News.com "EU Data Retention Directive Gets Final Nod" found on the Internet http://news.com.com/2100-7348_3-60423032.html [Date of use 7 March 2006] 1 – 4

Best J (2006) c/Net News.com "Europe Passes Tough New Data Retention Laws" found on the Internet http://news.com.com/Europe+passes+though+new+data+retention+laws/2100-7350_3- [Date of use 26 March 2006] 1 – 4

Burney B (2001) "The Concept of Cybercrimes – Is it right to analogize a physical crime to a cybercrime?" found on the Internet http://www.cybercrimes.net/Virtual/Burney/page3.html [Date of use 19 August 2003] 1 – 45

C

CCIPS (2001) "Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001" found on the Internet http://www.cybercrime.gov/searchmanual.htm [Date of use 22 May 2006] 1 – 10

CNET News.com (2003) "Bush pushes for Cybercrime Treaty" found on the Internet http://news.com.com/2100-1028_3-5108854.html [Date of use 31 January 2006] 2

CNN.com/Law Center (2003) "Can Europe Block Racist Web sites from its borders" found on the Internet http://www.cnn.com/2003/LAW/02/06/findlaw.analysis.ramasastry.cyberlaw/index.ht... [Date of use 31 January 2006] 1 – 4

Computer Security Institute (2005) "2005 CSI/FBI Computer Crime and Security Survey" found on the Internet http://www.p4performance.com/pdfs/whitepapers/FBI2005.pdf [Date of use 19 November 2005] 1 – 25

Computer Security Institute "2005 CSI/FBI Computer Crime and Security Survey" found on the Internet http://www.p4performance.com/pdfs/whitepapers/FBI2005.pdf

Confucius (2006) "Quote DB" found on the Internet http:///.quotedb.com/quotes/1482 [Date of use 31 March 2006] 1 – 2

Council of Europe (1950) "Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol No 11 Rome, 4X.I. 1950" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm [Date of use 18 March 2005] 1 – 50

Council of Europe (1950) Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol No 11 Rome, 4X.I. 1950" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm. [Date of use 28 April 2006] 1 – 40

Council of Europe (1995) "Explanatory Memorandum to Recommendation 1995(13) on Problems of Criminal Procedural Law connected with Information Technology" found on the Internet http://cm.coe.int/stat/E/Public/1995/ExpRep(95)13.htm [Date of use 24 Feb 2004] 1 – 47

Council of Europe (1995) "Recommendation No R(95)13 of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology" found on the Internet http://cm.coe.int/ta/rec/1995/95r13.htm [Date of use 24 Feb 2004] 1– 4

Council of Europe (2001) "Convention on Cybercrime CETS No.: 185" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [Date of use 10 November 2005] 1 – 8

Council of Europe (2001) "Convention on Cybercrime: List of declarations made with respect to treaties" found on the Internet http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=&D.. [Date of use 10 November 2005] 1 – 15

Council of Europe (2001) "Cybercrime Convention Budapest 23.XI.2001" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [Date of use 8 March 2004] 1 – 28

Council of Europe (2001) "Explanatory Report to the Convention on Cybercrime (ETS No 185) found on the Internet http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [Date of use 13 Jan 2004] 1 – 68

Council of Europe (2002) "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems Strasbourg, 28.I.2003" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/189 [Date of use 13 Jan 2004] 1 – 8

Council of Europe (2003) "Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems Strasbourg, 28.I.2003" found on the Internet http://conventions.coe.int/Treaty/en/Treaties/Html/189 [Date of use 10 November 2005] 1 – 8

Council of Europe (2003) "Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS No. 189)" found on the Internet http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=10/11/2005&CL=ENG [Date of use 13 January 2004] 1 – 8

Crown Copyright (2000) "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm [Date of use 27 Feb 2006] 1 – 15

CSI/FBI (2003) "CSI/FBI Computer Crime and Security Survey 2003" found on the Internet http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf [Date of use 23 August 2004] 1 – 18

CSI/FBI (2004) "CSI/FBI Computer Crime and Security Survey 2004" found on the Internet http://i.cmpnet.com.gocsi.db_area/pdfs/fbi/FBI2004.pdf [Date of use 23 August 2004] 1 – 20

CSO, Carnegie Mellon and CERT® Coordination Center (2004) "*E*-Crime watch™ survey" found on the Internet http://www.csoonline.com/releases/ecrimewatch04.pdf [Date of use 23 August 2004] 1 – 20

Cyber-Rights & Cyber Liberties (UK) Palermo Statement (2000) "Cyber-rights vs Cyber-Crimes" found on the Internet http://www.cyber-rights.org/reports/palermo.htm [Date of use 31 January 2006] 1 – 3

Cyber-Rights & Cyber-Liberties (??) "February 2002 – CoE Published the First Draft Version of the First Additional Protocol" found on the Internet http://www.cyber-rights.org/cybercrime/coe_archieve.htm [Date of use 23 March 2003] 1 – 8

Cyber-Rights & Cyber-Liberties (2002) "The Council of Europe Fights Against Racism and xenophobia on the Internet" found on the Internet http://www.cyber-rights.org/cybercrime/coe_archieve.htm [Date of use 31 January 2006] 1 – 15

D

E

Ernst & Young "Global Information Security Survey 2003" found on the Internet http://www.securitymanagament.com/library/EY_Survey1103.pdf [Date of use 24 February 2006] 1 – 18

Espiner T (2006) "Give us Tools to Fight Cybercrime" found on the Internet http://news.com.com/Interpol+Give+us+tools+to+fight+cybercrime/2100-7348_3-605 [Date of use 29 March 2006] 1 – 4

EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data found on the Internet http://www.cdt.org/privacy/eudirective/EU-Directive_html 1 – 4

F

Feldman (2003) "The essentials of Computer Discovery" found on the Internet http://www.forensics.com/pdf/Essentials_of_Discovery.pdf [Date of use 18 March 2003] 1 – 23

G

Goeman C (2002) "Law Enforcement and Data Privacy: Difficulties to Accommodate" found on the Internet http://www.law.kuleuven.ac.be/icri/publications/367ISSEconf.0212002.lawenforcementprivacy.pdf?where=itl [Date of use 29 May 2006] 1 – 13

Google (2004) "Definitions of Binary" found on the Internet http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3Abinary [Date of use 24 June 2004] 1 – 4

Google (2004) "Definitions of Convergence on the Web" found on the Internet http://www.google.com/search?hl=en&lr-&ie=UTF-8&oi-defmore&q=define:Convergence [Date of use 24 June 2004] 1 – 4

Google (2004) "Definitions of Cyberspace on the Web" found on the Internet http://www.google.com/search?hl=en&ie=ISO-8859-1&q=define%3A+cyberspace [Date of use 8 February 2005] 1 – 3

Google (2004) "Definitions of Data Hiding on the Web" found on the Internet http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3A+data+hiding [Date of use 24 June 2004] 1 – 7

Google (2004) "Definitions of Digital on the Web" found on the Internet http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3Adigital [Date of use 24 June 2004] 1-3

Google (2004) "Definitions of Hex on the Web" found on the Internet http://www.google.com/search?hl+en&lr+ie+ISO-8859-1&q=define%3A+hex [Date of use 23 August 2004] 1 – 3

Google (2004) "Definitions of Mainframe on the Web" found on the Internet http://www.google.com/search?hl=en&lr=&ie-ISO-8859-1&q=define%3A+mainframe [Date of use 24 June 2004] 1 – 3

Google Search (2005) "Define: Convergence" found on the Internet http://www.google.com/search?hl=en&lr-&ie=UTF%20-8&oi-defmore&q=de..:Convergenc [Date of use 8 February 2005] 1 – 4

Google Search (2005) "Define: Cyberspace" found on the Internet http://www.google.com/search?hl=en&ie=ISO=8859-1&q=define%3A+cyberspace [Date of use 28 July 2005] 1 – 7

Google Search (2005) "Define: Data Hiding" found on the Internet http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3A+data+hiding [Date of use 28 July 2005] 1 – 5

Greene TC (2001) "Cybercrime Justifies World Government" found on the Internet http://www.theregister.co.uk/2001/0531cybercrime_justifies_world_government/pri [Date of use 31 January 2006] 1 – 4

Guidance Software (2005) "EnCase Forensic Edition" found on the Internet http://www.guidancesoftware.com [Date of use 20 January 2006 1 – 120

H

Holder (2000) Statement of Eric Holder, Deputy Attorney General of the United States before the subcommittee on crime of the house committee on the judiciary and the subcommittee on criminal oversight of the senate committee on the judiciary on Internet denial of service attacks and the federal response on 29 February 2000" found on the Internet http://www.usdoj.gov/criminal/cybercrime/dag0229.htm [Date of use ?] 4, 6 FN11(1) 14(1)

Home Office's website (2005) "Police and Criminal Evidence Act" found on the Internet www.homeoffice.gov.uk [Date of use 18 Novemeber 2005] 1 – 78

Hosein G (2005) "Privacy and Cyberspace: Questioning the Need for Harmonisation" found on the Internet http://www.itu.int/osg/spu/cybersecurity/docs/Hosein_Privacy_and_Cyberspace.pdf [Date of use 28 March 2005] 1 – 15

HSE Enforcement Guide (England & Wales) (2006) "Evidence That May Assist in Your Investigation" found on the Internet http://www.hse.gov.uk/enforce/enforcementguide/investigation/physical/evidence.htm [Date of use 4 February 2006] 1 – 3

I

J

JISC Legal Information Service (2002) "*E*-Security Encryption and the Law – Overview" found on the Internet http://www.jisclegal.ac.uk/esecurity/escurity.htm [Date of use 3 February 2006] 1 – 18

Jones CW (2005) "Council of Europe Convention on Cybercrime: Themes and Critiques" found on the Internet http://www.sims.berkeley.edu/~cjones/FullTextPapers/CouncilofEuropeConventionon Cybercrime-ThemesandCritiques.pdf [Date of use 10 November 2005] 1-14

Judicial Studies Board (2006) "District Judge's (Magistrates' Court) Benchbook" found on the Internet www.jsboard.co.uk/magistrates [Date of use 16 May 2006] 1 – 89

K

Kaspersen HWK (2003) "Cyber Racism and the Council of Europe's reply" found on the Internet http://www.hreoc.gov.au/racial_discrimination/cyberracism/kaspersen.html [Date of use 30 November 2005] 1 – 11

Kennedy DC (2002) "In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty" found on the Internet http://law.richmond.edu/JOLT/v9i1/article3.pdf [Date of use 27 April 2006] 1 – 59

Koenig D (2001) "Meeting Law Enforcement's Responsibilities: Solving the Serious Issues of Today" found on the Internet http://www.neiassocaites.org.seriousissues.pdf [Date of use 28 September 2005] 1 – 137

KPMG "2002 Global Information Security Survey" found on the Internet http://www.kpmg.com/microsite/informationsecurity/pdf/giss.pdf [Date of use 20 May 2006] 1 – 40

Left S (2001) "Government launches Cybercrime Unit" found on the Internet http://www.guardian.co.uk/internetnews/story/0,7369,474518,00.html [Date of use 31 January 2006] 1 – 3

M

McConnell International (2000) "Cyber Crime ... and Punishment?" found on the Internet http://www.mcconnellinternational.com/services/cybercrime.htm [Date of use 2 May 2003] 1-3

McConnell International (2000) "Cybercrime... and Punishment? Archaic Laws Threaten Global Information" found on the Internet http://www.mcconnellinternational.com/services/cybercrime.htm [Date of use 2 May 2003] 1 – 10

McConnell International (2000) "Risk *e*-Business: Seizing the Opportunity of Global *e*-Readiness" found on the Internet http://www.mcconnellinternational.com/ereadiness/EreadinessReport.htm [Date of use 2 May 2003] 1 – 19

McLean JJ (1999) "14th Bileta Conference: Cyberspace 1999: Crime, Criminal Justice and the Internet" found on the Internet http://www.bilete.ac.uk/99papers/maclean.html [Date of use 02 April 2005] ??

Millar S (2001) "Blunkett will not limit Scope of Measure to Terrorist Cases" found on the Internet http://www.guardian.co.uk/Archive/Article/0,4273,4293489,00.html [Date of use 31 January 2006] 1 – 3

Mobile Computing Definitions (2006) "Enhanced Messaging Service" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,290660,sid40_gci785459,... [Date of use 28 February 2006] 1 – 2

Mobile Computing Definitions (2006) "Multimedia Messaging Service" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,290660,sid40_gci943702,... [Date of use 28 February 2006] 1 – 2

Mobile Computing Definitions (2006) "Short Message Service" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci213660,00.html 1 [Date of use 28 February 2006] 1 – 2

Mobrien.com (2006) "Computer Crime" found on the Internet http://www.mobrien.com/computer_crime4.htm [Date of use 22 March 2006] 1 – 8

Money Laundering Alert (2001) "Cyberlaundering threats should put all bankers on alert, FATF warns" found on the Internet http://www.moneylaundering.com/MLAarticles/01Apr5.htm [Date of use 15 October 2003] 1 – 3

N

Naughton J (2001) "Cybercrime Treaty's a secret Policemen's ball" found on the Internet http://www.guardian.co.uk/internetnews/story/0,7369,489920,00.html [Date of use 31 January 2006] 1 – 2

Net Definitions (2006) "Static IP address/ dynamic IP address" found on the Internet http://searchvb.techtarget.com/sDefinition/0,290660,sid8_gci520967,00.html [Date of use 24 April 2006] 1 – 3

Networking Definitions "File transfer protocol" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,290660,sid7_gci213976,00.html 1

Networking Definitions "URL" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,290660,sid7_gci213251,00.html 1

O

Out-Law News (2001) "Final Form of the Cybercrime Convention Wins Approval" found on the Internet http://www.out-law.com/page-1751 [Date of use 8 November 2005] 1 – 2

P

Paul, Weiss, Rifkind, Wharton & Garrison LLP (2005) "District Court Addresses Presumption of Discovery of Metadata" found on the Internet http://www.internationallawoffice.com/Newsletters/Detail.aspx?r=80004&i=59884&... [Date of use 15 December 2005] 1 – 18

Perera R (2000) "Internet Business Group Calls for Delay in Cybercrime Treaty" found on the Internet http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,53469,00... [Date of use 31 January 2006] 1

Perrin S (2001) "An Analysis of International Initiatives on High-Tech Crime A Review of Implications for the Canadian Policy Environment" found on the Internet http://www./exinformatica.org/cybercrime/pub/perrin.pdf [Date of use 13 January 2006] 1 – 98

Poulsen K (2004) "US Defends Cybercrime Treaty" found on the Internet http://www.securityfocus.com/news/8529 [Date of use 31 January 2006] 1

Poulsen K (2006) T0rn'Arrest Alarms White Hats, Advocates" found on the Internet http://www.businessweek.com/technology/content/sep2002/tc20020925_0548.htm [Date of use 31 January 2006] 1 - 3

Privacy International (2003) "Silenced – Europe Profile" found on the Internet http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-103799 [Date of use 9 November 2005] 1 – 6

Privacy International (2004) "Overview – Not really about Cybercrime" found on the Internet http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65424 [Date of use 31 January 2006] 1

Privacy International (2004) "The Group of 8" found on the Internet http://www.privacyinternational.org/article.shtml?cmd[347]=347-65438 [Date of use 31 January 2006] 1 – 2

Q

Quintessenz (2006) "EU Data Retention – Doqu/Base" found on the Internet http://www.quintessenz.at/cgi-bin/index?id=000100002986 [Date of use 7 March 2006] 1 – 6

R

Rantala 2004 *NCJ*; Home Office "Fraud and Technology Crimes: Findings from the 2003/2004 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources" found on the Internet http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf [Date of use 7 March 2006] 1 – 6

Reno J (1997) "Keynote Address by U.S. Attorney General Janet Reno on High-tech and Compuate Crime" found on the Internet http://www.usdoj.gov/criminal/cybercrime/agfranc.htm [Date of use 23 May 2006] 1 – 4

Rizvi H (2004) "Bush Pushes Plan to Permit Internet Surveillance" found on the Internet http://www.commondreams.org/headlines04/0121-01.htm [Date of use 30 November 2005] 1 – 3

Rosen (2003) "The US – EU Convention on Cybercrime" found on the Internet http://www.lawtechjournal.com/notes/2002/19_020819_rosen.php 1 [Date of 19 March 2006] 1 – 13

S

Scheeres J (2002) "EU Law Turns ISPs Into Spies?" found on the Internet http://www.wired.com/news/politics/0,1283,52829,00.html [Date of use 22 May 2006] 1 – 3

Screenshot (2006) "Screenshot Utility, a Screen Capture Program" found on the Internet http://www.screenshot-utility.com/ [Date of use 9 February 2006] 1 – 3

Search390.com Definitions (2003) "Mainframe" found on the Internet http://search390.techtarget.com/sDefinition/0,,sid10_gci212516,00.html [Date of use 19 August 2004] 1 – 2

SearchExchange.com Definitions (2004) "File Allocation Table" found on the Internet http://searchexchange.techtarget.com/sDefinition/0,,sid43_gci213956,00.html [Date of use 17 August 2004] 1

SearchMobileComputing.com Definitions (2003) "Memory" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212546,00.html [Date of use 22 June 2004] 1 – 2

SearchMobileComputing.com Definitions (2003) "Peripheral" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212774,00.html [Date of use 16 August 2004] 1

SearchMobileComputing.com Definitions (2003) "RAM" found on the Internet http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci214255,00.html [Date of use 22 June 2004] 1 – 3

SearchMobileComputing.com Definitions (2003) "Storage" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214465,00.html [Date of use 22 June 2004] 1

SearchNetworking.com Definitions (2004) "Client/Server" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci211796,00.html [Date of use 19 August 2004] 1 – 2

SearchNetworking.com Definitions (2004) "Peer-to-Peer" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html [Date of use 19 August 2004] 1 – 2

SearchSmallBizIT.com Definitions (2000) "Read-only Memory" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci214271,00.html [Date of use 22 June 2004] 1 – 2

searchSmallBizIT.com Definitions (2001) "Motherboard" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci212594,00.html [Date of use 17 August 2004] 1 – 2

searchSmallBizIT.com Definitions (2002) "Hardware" found on the Internet http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44)gci212228,00.html [Date of use 17 August 2004] 1

SearchSQLServer.com (??) "Drilldown" found on the Internet http://searchsqlserver.techtaget.com/sDefinition/0,290660,sid87_gci212001,00.html [Date of use ??] 1 FN8(5)

SearchStorage.com Definitions (2001) "Flash Memory" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212130,00.html [Date of use 17 August 2004] 1 – 2

SearchStorage.com Definitions (2001) "Memory Stick" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214628,00.html [Date of use 19 August 2004] 1 – 2

SearchStorage.com Definitions (2001) "Storage" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci214465,00.html [Date of use 22 June 2004] 1

SearchStorage.com Definitions (2003) "Cache Memory" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211730,00.html [Date of use 3 August 2004] 1 – 3

SearchStorage.com Definitions (2003) "Diskette" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211964,00.html [Date of use 17 August 2004] 1 – 2

SearchStorage.com Definitions (2003) "Hard Disk Drive" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci213993,00.html [Date of use 17 August 2004] 1 – 2

SearchStorage.com Definitions (2003) "Hard Disk" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212227,00.html [Date of use 17 August 2004] 1 – 2

SearchStorage.com Definitions "Storage Snapshot" found on the Internet http://searchstorage.tehctarget.com/sDefinition/0,290660,sid5_gci1008820,00.html [Date of use 09 February 2006] 1

SearchWebServices.com Definitions (2003) "Middleware" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212571,00.html [Date of use 17 August 2004] 1 – 2

SearchWin2000.com Definitions (2003) "Computer" found on the Internet http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci211829,00.html [Date of use 16 August 2004] 1 – 2

Shawl "Breaking News – Bush Signs Partriot Act Renewal" found on the Internet http://www.jurist.law.pitt.edu/paperchase/2006/03/breking-news-bush-signs-patriot-act.php 1

Sieber U (1998) "Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-STUDY (Version 1,0)" found on the Internet http://www.jura.uni-muenchen.de/sieber/article/article.htm [Date of use 4 February 2003] 1 – 238

SMB Definitions (2006) "Bootstrap" found on the Internet http://searchsmb.techtarget.com/sDefinition/0,290660,sid44_gci214479,00.html [Date of use 7 June 2006] 1 – 2

SMD Definitions (2006) "Internet appliance" found on the Internet http://searchsmb.terchtarget.com/sDefinition/0,190660,sid44_gci914561,00.html [Date of use 10 June 2006) 1 – 2

Sterling B (1993) "Mondo.184: Bruce Sterling Live at Mondo, Part II" found on the Internet http://www.eff.org.Misc/Publications/William_Gibson/sterling_gibson_nas.speeches.1 [Date of use 22 May 2006] 1 – 5

Sussmann MA (1997) "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium" found on the Internet http://www.law.duke.edu/journals/djcil/articles/djcil9p451.htm [Date of use 3 February 2006] 1 – 30

T

Taylor G (2001) "The Council of Europe Cybercrime Convention: A Civil Liberties Perspective" found on the Internet http://www.austlii.edu.au/au/other/CyberLRes/2001/30/ [Date of use 8 February 2005] 1 – 9

Taylor G (2004) "The Council of Europe Cybercrime Convention A Civil Liberties Perspective" found on the Internet http://www.crime-research.org/articles/CoE_Cybercrime/ [Date of use 08 November 2005] 1 – 5

TreatyWatch.org (2001) "Eight Reasons the International Cybercrime Treaty should be Rejected" found on the Internet http://www.treatywatch.org/about.html [Date of use 08 November 2005] 1 – 4

U

UK Home Office (2000) "Explanatory Notes to Regulation of Investigatory Powers Act" found on the Internet http://www.opsi.gov.uk/acts/en2000/2000en23.htm [Date of use 27 February 2006] 1 – 15

UK Home Office (2004) "Findings from the 2003/2004 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources" found on the Internet http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf [Date of use 23 April 2006] 1 – 23

UNCITRAL "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 *bis* as adopted in 1998" found on the Internet http://www.uncitral.org/pdf/english/text/electom/05-89450_Ebook.pdf 1 - 90

United States Department of Justice, the President's Working Group (2000) "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet" found on the Internet http://www.usdoj.gov/criminal/cybercrime/unlawful.htm [Date of use 31 January 2006] 1 – 90

USA CCIPS (2002) "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" found on the Internet http://www.cybercrime.gov/s&smanual2002.htm [Date of use 28 July 2005] 1-140

V

Vatis (??) "Statement of Michael A Vatis, Director, National Infrastructure Protection Center & Federal of Investigation on Cybercrime Before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee, Washington, DC, February 29, 2000" found on the Internet http://www.cybercrime.gov/vatis.htm [Date of use?] 2 FN26(1)

W

Ward M (2001) "Treaty Could Stifle Online Privacy" found on the Internet http://news.bbc.co.uk/1/hi/sci/tech/1378482.stmm [Date of use 31 January 2006] 1 – 3

Webopedia (2004) "Cluster" found on the Internet http://www.pcweopedia.com/TERM/C/cluster.html [Date of use 24 June 2004] 1 – 4

Webopedia (2004) "Memory" found on the Internet http://www/pcwebopedia.com/TERM/m/memory.html [Date of use 24 June 2004] 1 – 5

Webopedia (2004) "Slack Space" found on the Internet http://www.pcweopedia.com/TERM/s/slack_spcae.html [Date of use 24 June 2004] 1 – 2

Webopedia (2006) "Brouter" found on the Internet http://www.webopedia.com/TERM/B/brouter.html [Date of use 15 May 2006] 1 – 3

Webopedia (2006) "Look-and-feel" found on the Internet http://www.webopedia.com/TERM/l/look_and_feel.html [Date of use 20 February 2006] 1 – 2

Webopedia (2006) "User Interface" found on the Internet http://www.webopedia.com/TERM/U/user_interface.html [Date of use 20 February 2006] 1 – 3

Whatis.com (2001) "Target Search" ™ found on the Internet http://whatia.techtarget.com/definition/0,,sid9_gci211837,00.html [Date of use 24 June 2004] 1

Whatis.com SearchCIO.com Definitions (2003) "Raw data" found on the Internet http://searchcio.techtarget.com/sDefinition/0,,sid19_gci878172,00.html [Date of use 15 June 2004] 1 – 2

Whatis.com SearchCIO.com Definitions (2004) "Convergence" found on the Internet http://searchcio.techtarget.com/definition/0,,sid9_gci211837,00.html [Date of use 24 June 2004] 1 – 3

Whatis.com searchDatabase.com Definitions (??) "Information" found on the Internet http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci212343,00.html [Date of use 15 June 2004] 1

Whatis.com searchNetworking.com Definitions (2006) "Metropolitan area network" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214083,00.html [Date of use 19 August 2004] 1 – 2

Whatis.com SearchNetworking.com Definitions (2006) "Wide area network" found on the Internet http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214117,00.html [Date of use 19 August 2004] 1 – 2

Whatis.com searchSecurity.com Definitions (2006) "Extranet" found on the Internet http://searchsecurity.techtarget.com/sDefinition/0,,sid_gci212089,00.html [Date of use 19 August 2004] 1 – 2

Whatis.com searchSMB.com Definitions (2006) "Real time" found on the Internet http://searchsmb.techtarget.com/sDefinition/0,290660,sid44_gci214344,00.html [Date of use 14 April 2006] 1 – 2

Whatis.com SearchSQLServicer.com Definitions (2003) "Meta" found on the Internet http://searchsqlserver.techtarget.com/sDefinition/0,290660,sid87_gci212555,00.html [Date of use 24 June 2003] 1 – 17

Whatis.com searchStorage.com Definitions (2001) "Data" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211894,00.html [Date of use 15 June 2004] 1 – 2

Whatis.com searchStorage.com Definitions (2006) "Storage Area Network" found on the Internet http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212937,00.html [Date of use 19 August 2004] 1 – 2

Whatis.com SearchWebServices.com Definitions (2001) "Intranet" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212377,00html [Date of use 19 August 2004] 1 – 2

Whatis.com searchWebservices.com Definitions (2003) "Internet" found on the Internet http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212370,00.html [Date of use 19 August 2004] 1 – 3

Whatis.com(2006) "Mailing list" found on the Internet http://whatis.techtarget.com/definition/0,289893,sid9_gci212515,00.htrml [Date of use 10 June 2006] 1 – 3

Wikipedia (2005) "Metadata" found on the Internet http://en.wikipedia.org.wiki/Metadata [Date of use 25 November 2005] 1 – 7

Wired News (2002) "Beefed-Up Global Surveillance?" found on the Internet http://www.wired.com/news/politics/0,1283,50529,00.html [Date of use 31 January 2006] 2

X

Y

Young (2004) "Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation: A Critical Analysis of the Council of Europe Convention on Cyber-Crime & the Canadian Lawful Access Proposal" found on the Internet http://www.ijclp.org/Cy_2004/pdf/Young_ijclp-paper.pdf [Date of use 15 February 2006] 1 – 28

Z