Impediments during the compilation of a search and seizure warrant for digital information by forensic investigators in South Africa

Jacobus Gerhardus J. Nortje and Daniel Christoffel Myburgh
School of Accounting, North-West University, Potchefstroom, South Africa

Abstract

Purpose – The purpose of this paper is to identify and discuss impediments in the compilation of an application for a search and seizure warrant for digital evidence and the structure of such a warrant in South African criminal cases.

Design/methodology/approach – This paper provides a brief overview of international and local impediments, followed by a detailed discussion of the implications of these impediments and how it is approached in various jurisdictions. The methodology of this paper consists of a literature review.

Findings – Addressing the impediments in the compilation of the application and the warrant will be beneficial for forensic investigators, the South African Police Service (SAPS) and the administration of justice in South Africa.

Research limitations/implications – Search and seizures for digital evidence form part of civil, regulatory and criminal search and seizures. This study focuses on the search and seizure of digital evidence in criminal matters pursuant to mainly the provisions of the Criminal Procedure Act 51 of 1977 and the Cybercrimes Act 19 of 2020.

Originality/value – The originality of this paper lies in the approach to the drafting of applications for search and seizure warrants for digital information in South Africa. The contribution of the study is that, by using this approach, the SAPS can address the impediments during the application and compilation of the warrants, which would enhance the quality of investigations and contribute to the successful investigation and prosecution of crime in South Africa.

Keywords Search and seizure warrant, Application, Digital information, Authorising officers, Privilege information, Digital evidence

Paper type Literature review

1. Introduction

This is the first of two articles consisting of a literature review into impediments during the application, compilation (first article) and execution (second article) of a search and seizure warrant for digital information in South Africa (SA).

Journal of Financial Crime
Vol. 31 No. 3, 2024
pp. 476-488
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-05-2023-0106

The logic of the study commenced with an in-depth review of the current available literature, emphasising the different approaches, processes and best practices used as depicted in local and international case law and practices.

The missing knowledge is that no such research is known to have been conducted in SA. The shortcomings in this regard are emphasised by the number of successful court applications against the South African Police Service (SAPS) for defective contents and the execution of search and seizure warrants.

The following research question is key in addressing the identified impediments: Will the addressing of the impediments in the compilation of the application and the search and seizure warrant be beneficial for forensic investigators, the SAPS and the administration of justice in SA as a whole?

The purpose of this study is to identify and discuss impediments in the compilation of an application for a search and seizure warrant and a search and seizure warrant itself. To achieve the purpose of the study, the following four impediments, as identified in international and local case law, are discussed in Article 1: firstly, full disclosure with applications; secondly, the intelligibility of an application and search and seizure warrant; thirdly, search protocols and ex ante restrictions; and finally, privileged information. In Article 2, the following impediments during the execution of the search and seizure warrant will be discussed: overbroad seizures, the two-step search process including off-site searches, segregation of data, use of filter teams, retention of non-relevant data and plain-view discoveries.

Although much has been written on search and seizure warrants and the execution thereof, little attention has been paid to the contents of these warrants and their application, and therefore, regarding the mentioned impediments, specific to digital evidence. Various international case law identifies impediments that are relevant to SA. The international case law, law and guidelines of the following countries are the most notable and relevant to SA: Canada, New Zealand, the UK and America.

Related studies within a South African context are, *inter alia*, that of Basdeo, Nieman and Bouwer. Basdeo (2012) discussed the search and seizure powers of cyber inspectors in terms of the Electronic Communication and Transaction Act (25 of 2002) and the requirements of the Cybercrime Convention in Budapest (Council of Europe Treaty Office, 2001). Nieman (2006) is one of the most comprehensive discussions of the legal requirements of digital evidence, but does not address the application and the compilation of a search and seizure warrant. Bouwer, published in 2014, defines electronic evidence and explores the two-step search process as discussed by Kerr (2005a:533) and how the two-step search process can be implemented in SA.

The practical implication of this study is that if the SAPS addresses the impediments during the application and compilation of the search and seizure warrants, it would enhance the quality of investigations and contribute to the successful investigation and prosecution of crime in SA. Other main stakeholders are the Departments of Justice, Forensic Information Technology practitioners and lawyers when drafting and executing Anton Pillar orders, Investigation Directorate, Independent Police Investigation Directorate, Special Investigation Unit, South Africa Revenue Service, Financial Intelligence Centre and Competition Commission.

The article is structured as follows: Section 2 provides a background to the study, a conceptual scope of the study, followed by a literature review in Section 3. This is followed by conclusions and recommendations in Section 4.

2. Background

2.1 Relevance of this study

It is very difficult to determine where SA is regarding understanding and interpreting the internationally identified impediments that digital evidence poses to search and seizure

principles – if not in the beginning phase – and how prior experiences in other countries, such as Canada, the UK, New Zeeland and the USA can aid SA. It is, therefore, important to review the impediments that digital evidence poses to the application for and the compilation of a search and seizure warrant and how these complexities can be approached within a South African context.

2.2 Conceptual scope of the study

Although the contents of every application and search and seizure warrant will differ, general trends can be identified. The conceptual scope and context of the study are that the SAPS will compile an application for a search and seizure warrant in the form of an affidavit by the investigating officer as well as the search and seizure warrant itself. The compilation of a search and seizure warrant usually commences with the standard requirements as set out in Sections 20 and 21 of the Criminal Procedure Act (51 of 1977), read with Sections 28 and 29 of the Cybercrimes Act (19 of 2020). The items, which will include the digital information intended to be seized, need to be described in the warrant. The search and seizure warrant accompanied by the application will be presented to an authorised officer for consideration and authorisation. It was encountered that, in instances after the execution of the search and seizure warrant, a second application is made to the authorised officer for authorisation to access the digital information.

3. Literature review

3.1 Local and international impediments

Traditional search and seizures have developed with physical locations in mind and had the benefit of being refined during court cases over many years as opposed to digital evidence (Lowenstein, 2007, p. 6). Kerr (2005b, pp. 100–108) investigated several complexities that search and seizure procedures regarding digital evidence pose to traditional laws and identified the following aspects that should be considered:

- How should the articles, to be seized, be described and is data really seized if the forensic duplicate is seized as opposed to the original device? If the search and seizure warrant only describes computer equipment, these warrants can be considered too broad if the computer and all the data on it are seized – if warrants only describe the data, the seizure of the physical computers can be viewed as unconstitutional.
- When does the law regard a computer as being "searched" and what are the premises to be searched? If search and seizure warrants describe the premises of suspects, is the removal of computer equipment to digital forensic laboratories permissible to continue searching the data?

Additional technical complications were argued and considered in the case of the United States v Comprehensive Drug Testing Inc. (2009), where a full bench of judges directed authorised officers to enforce the following pre-emptive requirements (hereafter referred to as ex ante requirements):

- The State must waive reliance on the plain view doctrine. If investigators find anything that does not relate to the original warrant, they are not allowed to use or access it.
- Segregation of relevant and non-relevant data must be either done by specialised personnel or an independent third party.

- If segregation is done by the State, it must be specified in the warrant application that computer personnel may not disclose any information other than that which is the target of the warrant to the investigator.
- Search and seizure warrant applications must state the actual risks of the destruction of information and prior efforts to obtain the information by means of other legal routes.
- The search protocol of the State must be structured to only uncover information containing probable cause, and only that information may be examined by investigators.
- The State must destroy or return non-related data.

In September 2010, the Ninth Circuit Court issued a revised en-banc opinion and changed the requirements to guidelines. It should be noted that in the Matter of the United States of America's Application for a Search Warrant to Seize Electronic Devices from Edward Cunnius (2011, p. 12), the court stated that although the requirements were changed to guidelines, it does not mean that judges are prohibited from using or insisting on the State to comply with the ruling or that the guidelines are inappropriate.

In SA, the Criminal Procedure Act (51 of 1977) governed search and seizures by the State and was drafted before digital evidence becoming essential. Chapter 4 of the new Cybercrimes Act (19 of 2020) is the first attempt to give specific guidance to the search and seizure of digital evidence. Although a few SA court cases exist in which aspects of digital evidence were explored, no case was found where comprehensive consideration was given to the impediments that digital evidence poses to traditional search and seizure. It is considered that, as in the US v Comprehensive Drug Testing Inc. (2009) case, where the court warned that if rules are so relaxed to accommodate complications posed by digital evidence, there is a serious risk that every search and seizure warrant for digital evidence would become overbroad and that the Fourth Amendment becomes irrelevant, and this also applies to Section 14 of the South African Constitution (1996), if acceptable legal parameters of search and seizure warrants for digital evidence are not defined.

3.1.1 Obligation to provide full disclosure with applications for search and seizure warrants. When considering the approval of a search and seizure warrant, the authorised officer should ensure that the search and seizure warrant is not too general or overbroad and that the terms are reasonably clear in such a way that the rights of the affected persons are protected as far as possible.

The study of Kessler (2010) into the level of understanding and awareness among judges in America concerning digital evidence identified that it is a requirement that a greater than usual explanation or description of what is requested regarding digital evidence should be provided. This is especially relevant to SA, if the case of Smith, Tabata and Van Heerden v the Minister of Law and Order (1989) is considered, where it was held that if the articles have been described in broad and general terms, the court will rule that the authorised officer did not apply his mind properly. The question can be asked whether authorised officers do not have sufficient knowledge concerning the unique complexities that digital evidence poses to traditional search and seizure operations; whether they are able to apply their minds sufficiently. Considering the custodial or the constitutional protector role that the court plays in assessing whether sufficient grounds exist to permit a breach in the constitutional rights of persons and to ensure that a breach is done in the least restrictive manner, a certain level of knowledge is required, or sufficient disclosure is made to place authorised officers in a position to apply their mind. This was the conclusion of the Supreme Court of Canada in

the case of R. v Vu (2013) when the court held that applications for search and seizure warrants must explicitly stipulate, and so also the search and seizure warrants, that a search of a computer is required and authorised due to the unique complications that computers pose to the privacy rights of a person. The court held that only then can the court be sure that authorised officers considered the full range of distinctive privacy concerns that computer searches raise, and having done so, the threshold has sufficiently been reached to permit infringements of the rights of persons.

The minority ruling in the Thint (Pty) Ltd v the National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others (2008) case also needs to be considered, where it was stated that applicants of search and seizure warrants should disclose all of the facts that "might be" regarded as reasonable and relevant, because these facts can influence the decisions of authorised officers. These officers cannot consider selected facts or edited versions of facts. Following the ruling in this case, the question arose whether the following aspects, as examples, should be mentioned in applications for search and seizure warrants for digital evidence, as it could be material:

- Should the application describe that computers containing all of the data – including non-relevant and potentially legal privileged documents – will be seized and that off-site searches will be conducted?
- Should the application indicate how long the computers will be removed before being returned and what impact these delays will have on the owner or a business?
- Should specific details of the search protocol and analysis process be defined in the application?

These also need to be considered in light of the ruling in the Canadian case of R. v Vu (2013) where the court required that the mere fact that computers will be searched should explicitly be stated in applications to ensure that authorised officers can consider whether sufficient grounds exist to breach the level of privacy that individuals have come to accept with computers, cellular phones and tablets.

3.1.2 Search protocol and ex ante restrictions. There are two approaches that can limit the invasiveness of search and seizure warrants: pre-emptive restrictions (hereafter referred to as *ex ante* restrictions), and after-the-fact scrutiny (hereafter referred to as *ex post facto* scrutiny). *Ex ante* restrictions are imposed on search and seizure warrants before approval and execution. These restrictions set out the process to be followed by investigators and what measures should be taken to limit invasiveness regarding search and seizure warrants (Kerr, 2005a, p. 566).

Lowenstein (2007, p. 13) states that most courts are rejecting *ex ante* restrictions. This was in 2007, before the US v Comprehensive Drug Testing, Inc. (2009) ruling, where *ex ante* restrictions were first set as requirements and thereafter changed to guidelines. In the case of United States v Vilar (2007), the court expressed the opinion that by specifying *ex ante* restrictions, authorised officers can place themselves in a position to tell the State how to run their investigations – something that authorised officers are not qualified to do.

Two aspects are relevant when considering *ex ante* restrictions. The first aspect is whether authorised officers are authorised or in a position to place restrictions on investigators *ex ante*; and secondly, what restrictions are in the interest of justice. Guzzi (2012, p. 305, 321) is of the opinion that it is impractical to have authorised officers impose restrictions who are not well equipped to understand the implications of these restrictions or to review them. Guzzi maintained that it is "potentially technologically inappropriate" and can be potentially unlawful for authorised officers to impose restrictions.

A search protocol sets out how digital forensic investigators should search through the content of computers (Welty, 2011, p. 9). Following a search protocol is not meant to determine the content of documents, but to determine whether documents are relevant to an investigation (Guzzi, 2012, p. 321). In SA, authorised officers historically did not set restrictions on search and seizure warrants or require search protocols. However, it is envisaged that Sections 29(2)(d)-(h), which stipulate "the extent set out in the warrant" of the Cyber Crimes Act (19 of 2020), in this situation may be changed and that it could be perceived that "the extent set out in the warrant" relates to the way the article will be searched and accessed and will not indicate the description of the article – thereby requiring *ex ante* restrictions and search protocols.

Welty (2011, p. 9) reported that because digital evidence on computers is intermingled, investigators should demonstrate how they plan to search for relevant information to minimise an invasion of privacy. The South African Constitution, Section 36(1)(e), stipulates that the least restrictive means should be followed to achieve a specific purpose. In the case of the United States v Mann (2010), it was emphasised that search and seizure warrants to obtain digital evidence should be detailed and tailored to only allow access to files in question and to nothing more. Search protocols can involve a myriad of possibilities and can include, but are not limited to, a specification of keywords that will be searched, the types of files that will be accessed, and search processes that will be followed. Metadata and hash values can be searched, or other more sophisticated approaches or newer available technology can be applied, such as predictive coding, content analytics and auto-categorisation (Guzzi, 2012, p. 319). Although it was stated in the case of the United States v Mann (2010) that search and seizure warrants should be detailed and exact to only discover related files, this is easier said than done. The court held in the case of the United States v Burgess (2009) that there may be no practical alternative to the State looking in many of the folders or files on a computer or in all of them. The court, however, held that to protect the rights of suspects, investigators should first look in the most obvious places and then – when necessary – progressively move from the obvious to the obscure. It was argued that by following search protocols, investigators can demonstrate their intent to limit the invasiveness of search and seizure warrants.

Search protocols are susceptible to both *ex ante* and *ex post facto* judicial reviews. These protocols are, therefore, subject to more stringent and greater judicial reviews. Not only is the description of sought objects evaluated, but also the proposed methodology that will be followed in locating these articles and ultimately, the actions that were taken during the search. The United States Department of Justice (2009, pp. 79–82) warned that placing prior search parameters on analyses can seriously impair the ability of the State to locate evidence and prosecutors should oppose these restrictions. One proposed restriction is to limit analyses to keyword searches. However, very few digital forensic investigations will be complete and accurate by only conducting a keyword search. Files are often scanned and these scanned files, or documents saved as pictures on a computer, are unresponsive to a keyword search. Suspects can also make use of encryption or passwords. It is further advised by the United States Department of Justice (2009, p. 82) that if search protocols are included in applications, it should be clearly stated that these protocols are illustrations of likely strategies and not "specification of the exact manner that will be followed".

The Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners of the British Attorney General (2013, pp. 24–25) provide clear guidance that lead investigators should develop a strategy setting out how data should be analysed.

In the Canadian Supreme Court case, R. v Vu (2013), it was argued that *ex ante* search protocols should be a requirement of all search and seizure warrants and that search

protocols were required to limit the scope of digital searches to ensure that the State only discovers information in relation to the reasonable grounds stipulated in search and seizure warrants. The Canadian Supreme Court did not accept this argument in its entirety and was of the opinion that search protocols are not always required in every case.

3.1.3 Intelligibility. One of the basic requirements for search and seizure warrants is that it should intelligibly define, to both the searchers and suspects, the ambit of the search and seizure.

The expectations of individuals about privacy on their computers and mobile devices were recognised in the Canadian case of R. v Vu (2013), where the court set aside a search and seizure warrant because it did not explicitly mention that computers would be searched and seized and held that computers are very different to filing cabinets. After exploring the unique aspects of computers, the court held that the search for digital evidence search and seizure warrants is a distinctive treatment under Section 8 of the Canadian Charter of Rights and Freedoms and that specific prior authorisation must be obtained for searches where computers are involved and, as such, search and seizure warrants must specifically specify the authority to search computers. The complexity of computers often leads to individuals comparing computers to familiar physical world objects and the unique nature of computers is completely ignored – individuals are trying to fit a square peg in a round hole (McLain, 2007, p. 1072). When computers are considered in the same light as filing cabinets, not enough attention or consideration is given to the unique privacy concerns that computers pose.

In SA, the requirements to take into consideration concerning the intelligibility of search and seizure warrants were defined in Thint (Pty) Ltd v the National Director of Public Prosecutions and Others, Zuma and Another v the National Director of Public Prosecutions and Others (2008) and confirmed by the Constitutional Court in Minister for Safety and Security v Van Der Merwe and Others (2011) case, as:

- the authority under which search and seizure warrants are issued should be clearly stated;
- searchers should be identified;
- the authority bestowed upon searchers should be clearly defined;
- persons, containers or premises to be searched should be clearly identified; and
- suspected offences, which triggered a criminal investigation, should be clearly listed.

A further conclusion was made in the Goqwana v the Minister of Safety NO and Others (2016) case – supported in the Heaney v S (2016) case in that the suspected crime should be accurately described. In digital evidence, this ruling is important, as terminology such as *hacking* should not be colloquially used terms; when the correct description should be *unlawful access* in terms of the Cybercrimes Act (19 of 2020) and can lead to search and seizure warrants being found unintelligible.

Computers always contain relevant and non-relevant information and, therefore, it is even more likely that differences of opinion can occur regarding the seizure of computers. In the case of Polonyfis v the Minister of Police and Others (2011), the court held that it is ultimately the discretion of searchers to decide whether articles fall within the scope of a search and seizure warrant or not, but decisions made by searchers are subject to *ex post facto* scrutiny.

The advantage of conventional search and seizure warrants is that the issuing authorised officers can evaluate the level of intrusion and can limit such intrusion. Suspects

can also easily evaluate that law enforcement is staying inside the ambit of a search and seizure warrant. However, with search and seizure warrants for digital evidence, the technical level of understanding of authorised officers, suspects and investigators cannot be ignored. The question is then asked, if the authority to seize computers is not mentioned at all in a search and seizure warrant, will the reasonable person understand that the State is permitted to remove computers containing all of the data, create forensic duplicates and search through the data off-site? Secondly, will a reasonable person understand that the scope of forensic duplicates entails that all files – even deleted files – are duplicated and not only relevant files? Computers have become such an integral part of our lives and in the commissioning of crime (SALRC, 2010, p. 7) that it seems logical for investigators to clearly state and request the seizure of the computers, if it is reasonably believed that these computers contain evidence.

In SA, traditionally, search and seizure warrants are not required to specify which containers or filing cabinets will be searched. Section 21 of the Criminal Procedure Act (51 of 1977) only states that search and seizure warrants authorise police officials to enter premises and search for identified articles. Search and seizure warrants do not require the investigators to specify how each room will be entered and how each cupboard will be searched. In a literal way, it can be argued that the same applies to computers – if computers are specified as articles to be seized, the investigators can search every folder and file as they see fit.

Section 29 (2)(h) of the Cybercrimes Act (19 of 2020) additionally makes provision for the methodology needed by police officials during a search of digital evidence by specifying "use or obtain and use any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent set out in the warrant".

The aspect of intelligibility equally applies to both searchers and suspects. For the purpose of this article, a practical distinction is made between the use of the term "search", meaning *locating* and *analysis*, or *interpreting*. This distinction is required to point out that data can be searched automatically to locate relevant information without the content becoming known, and secondly, once relevant information is located, it can be read, analysed or interpreted as part of an investigation. This is the basis of an exposure-based approach, which proposes that data is only considered searched when data is exposed to human observation (Kerr, 2005a, p. 547). If search and seizure warrants, therefore, allow investigators to locate computers on a scene and the seizure thereof and an off-site search of data is permitted, it can be argued that a search has not yet been concluded when devices are removed from a scene. The search for specified devices is completed, but the search for relevant data on these devices has not yet been performed (Kerr, 2005b, pp. 100–108). This raises two aspects, namely, at what point do search and seizure warrants expire, i.e. are additional searches for relevant data on devices part of "on-going" search and seizure warrants? Secondly, if a search for computers is performed by investigators on a scene while a search through the data is performed by digital forensic investigators away from the scene, who is the "searcher" referred to in terms of intelligibility? A strong argument can be made that the investigators and the digital forensic investigators can both be perceived as the "searcher". Although it was found in the Goqwana v the Minister of Safety NO and Others (2015) case that the searcher should be identified in search and seizure warrants, it was also held that, in many situations, the searcher will have to be assisted by other investigators, the court was silent on the fact of identifying the other police officials, but stated that at least one of the police officials responsible for a search should be identified

as such. It is, however, advised in the Practical Guide of the SAPS (SAPS, 2016, p. 10) that the name of digital forensic investigators should be included in search and seizure warrants, but only for purposes of their presence on the scene. If a digital forensic investigator is recognised as the searcher, it can be further argued that the search and seizure warrant is the only document from which the digital forensic investigators should determine what is included or excluded for his "search" through the data and no other "external sources" should be used. This approach is in line with the ruling in the Thint (Pty) Ltd v the National Director of Public Prosecutions and Others, Zuma and Another v the National Director of Public Prosecutions and Others (2008) case that "it may therefore be said that the warrant should itself define the scope of the investigation".

3.1.4 Privileged information. It is well accepted that computers contain a multitude of data (Lowenstein, 2007, p. 10) and some of the data may be privileged. South African law recognises two types of privileged information, namely, matrimonial privilege and legal privilege, which is protected by the Law of Criminal Procedure.

Matrimonial privileged information, as contained in Section 198 of the Criminal Procedure Act (51 of 1977), states that a spouse shall not be obligated in criminal proceedings to disclose any communication that the other spouse made to him. This privilege can only be claimed by a spouse receiving communication (Schwikkard and Van der Merwe, 2002, p. 142). Because communication also relates to email communication, as defined in the Regulation of Interception of Communication and Provision of Communication-Related Information Act (70 of 2002), it can have a huge impact on the ability of investigators to freely analyse email communication of persons if they should constantly guard against matrimonial privileged information.

Legal privilege is probably the type of privilege that is most focused on in court cases. It is well documented that legal, privileged information may not be seized under a search and seizure warrant as was confirmed in the case of Thint (Pty) Ltd v the National Director of Public Prosecutions and Others, Zuma and Another v the National Director of Public Prosecutions and Others (2008).

Historically, the practice of seizing legally privileged information entailed the sealing of documents when persons claimed privilege and these documents were then handed to a neutral person, such as the Registrar of the High Court (Heiman, Maasdorp and Barker v Secretary of Inland Revenue, 1968). In the case of Bogoshi v Van Vuuren NO and Bogoshi v the Director Office of Serious Economic Offences (1993), the court held that the person who claims the privilege should be given the opportunity to remove privileged documents after these documents were seized.

In the Minister of Safety and Security v Bennett (2007) case, the SAPS seized a large number of documents and kept them sealed. After the seizure, the suspect raised the aspect of legal privilege. All documents were sealed and could not be accessed by the SAPS. It was argued that because the SAPS seized privileged documents, the seizure of even one document containing privileged information would "render the whole execution of the warrant invalid". The court rejected this and that there was no prejudice towards the suspect due to the manner in which the SAPS handled the documents, by using an independent advocate to identify privileged information. This action is in line with the requirement, as discussed below, of a filter team who independently segregates privileged, relevant and non-relevant data.

In the New Zealand case, Director of Serious Fraud Office v A Firm of Solicitors (2006), the court commented that "extensive conditions" were needed to protect privileged material and that it might "even be appropriate" for independent lawyers to be present during search processes.

Section 54 of the United Kingdom Criminal Justice and Police Act (16 of 2001) and the Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (2011, p. 23) prescribe that legally privileged information may only be seized if there is not a reasonable practical way of separating privileged information from other information on a scene and if privileged information is seized, it should be kept separate from other seized articles/data. Independent lawyers should review privileged information. This information may only be retained if the information is inextricably linked to relevant information, and it cannot be separated in a practical manner from the rest of the information. In this situation, independent filter teams must be used to analyse the documents and they may only provide relevant information that does not contain legally privileged data to the investigation team.

In the Lavallee, Rackel and Heintz v Canada (2002) case, the Supreme Court set a number of search protocols or rules when a search was conducted on law offices. Investigators should indicate to authorised officers that:

- no reasonable alternative existed;
- unless warrants stipulate that no examination may take place immediately, all of the documents should be sealed;
- lawyers and/or clients should be contacted at the time of execution and if they cannot be present, a member of the Bar should be allowed to observe the search; and
- independent lawyers should examine the documents to determine whether they contain privileged information.

Although case law recognises that privileged information may not be seized, but sealed and kept separate – this cannot happen when computers are seized. Once a forensic duplicate is created, no piece of the data can be removed from the forensic duplicate. If suspects are given the opportunity to delete information from their computers, forensic tools can very easily recover the deleted data. Similarly, suspects could have deleted privileged information before a seizure and their computer can, therefore, contain no active privileged information at the time of a seizure. If the SAPS performs data recovery, deleted privileged information is recovered. It is, therefore, impractical for persons to identify privileged information in only active data, and this means that privileged information can only be identified after a seizure and after data recovery was performed.

4. Conclusions and recommendations

Authorised officers should guard against allowing the rules for search and seizures to be so relaxed to accommodate the impediments and fact that evidence is intermingled with non-relevant information, that all search and seizures for digital evidence become overbroad, thereby allowing the constitutional rights of suspects to become irrelevant. The information contained in the application and the search and seizure warrant should, therefore, be carefully assessed to consider whether enough grounds exist to authorise the infringement of the heightened expectation of privacy that individuals hold in relation to their computers and mobile phones by authorising the search and seizure thereof.

In SA, authorised officers historically did not set restrictions on search and seizure warrants or require search protocols; however, it is envisaged that Sections 29(2)(d)-(h) in regard to "the extent set out in the warrant" of the Cyber Crimes Act (19 of 2020) may influence this. The opinion of the court in the case of United States v Vilar (2007) is that, by specifying *ex ante* restrictions, authorised officers can place themselves in a position to tell

the State how to run their investigations – something that authorised officers are not qualified to do.

It is recommended that:

- A qualified digital forensic investigator, who has sufficient knowledge in this field, unlike a normal forensic investigator who does not have sufficient knowledge in this field, must provide a statement that provides a greater-than-usual explanation or description of the unique complexities of digital evidence and the methodology to address it to such an extent that authorised officers shall be able to apply their mind sufficiently. Investigators are advised to address how the discussed impediments will be managed in their application, the search and seizure warrant and by their conduct, as a self-regulatory measure to ensure that search and seizure warrants are not overturned during *ex post facto* scrutiny. The investigator must attach this statement to the application and state that, insofar digital information is concerned, reliance is given to the statement of the digital forensic investigator.
- It is not recommended that authorised officers set ex ante restrictions, but that digital forensic investigators are required to, after a seizure, define and document search protocols that can be subjected to ex post facto scrutiny.
- The application and search and seizure warrant should show and the authorised officer should assess the following in each individual situation:
  - the description of the articles in terms of Section 1(1) of the Cybercrimes Act (19 of 2020);
  - the names of the forensic investigators and digital forensic investigators who will conduct the search and seizure;
  - the level as set out in the application and search and seizure warrant to which the SAPS will conduct a search on the scene to establish whether the device contains relevant information before seizing it;
  - the risk that the impediments pose to the interest of justice and the requirements to seize the whole computer and conduct an off-site search, if relevant information, or a forensic duplicate, cannot be created on the scene;
  - how claims of privilege, and privileged data will be managed;
  - how relevant information will be identified while minimising or preventing an invasion of privacy and access to privileged information; and
  - how access to and the segregation of relevant and non-relevant data will be managed.
- The search and seizure warrant must be the only document from which the digital forensic investigator should determine what is included or excluded for his *search* through the data and no other *external sources* must be used – it should therefore be sufficiently detailed, or else it can be found that the warrant is not intelligible in terms of permitting the digital forensic investigator to properly perform his functions.

References

Basdeo, V. (2012), "The legal challenges of search and seizure of electronic evidence in South African criminal procedure: a comparative analysis", *South African Journal of Criminal Justice*, Vol. 25 No. 2, pp. 195-212.

Bouwer, G.P. (2014), "Search and seizure of electronic evidence: division of the traditional one-step process into a new two-step process in a South African context", *South African Journal of Criminal Justice*, Vol. 27 No. 2, pp. 156-171.

British Attorney General (2013), "Attorney general's guidelines on disclosure for investigators, prosecutors and defence practitioners", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf (accessed 23 January 2023).

Canada (2002), "Lavallee, Rackel & Heintz v", *Canada (Attorney General)*, No. 3, S.C.R. 209.

Canada (2013), R v. Vu, S.C.J. No. 60, 2013 (3) S.C.R. 657, at para. 22 (S.C.C.).

Council of Europe Treaty Office (2001), "Convention on cybercrime (ETS no. 185)", available at: www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185# (accessed 27 January 2023).

Guzzi, S. (2012), "Digital searches and the fourth amendment: the interplay between the plain view doctrine and search-protocol warrant restrictions", *American Criminal Law Review*, Vol. 49 No. 1, pp. 301-329.

Kerr, O.S. (2005a), "Searches and seizures in a digital world", *Harvard Law Review*, Vol. 119 No. 2, pp. 531-585.

Kerr, O.S. (2005b), "Search warrants in an era of digital evidence", *Mississippi Law Journal*, Vol. 75 No. 1, pp. 85-108.

Kessler, G.C. (2010), "Judges' awareness, understanding, and application of digital evidence", PhD thesis, Nova Southeastern University, Graduate School of Computer and Information Sciences, Fort Lauderdale, FA.

Lowenstein, A.S. (2007), "Search and seizure on steroids: united states v", *Comprehensive Drug Testing and Its Consequences for Private Information Stored on Commercial Electronic Databases*, University of CA, Los Angeles.

McLain, G.R. (2007), "United States v. Hill: a new rule, but no clarity for the rules governing computer searches and seizures", *George Mason Law Review*, Vol. 14 No. 4, pp. 1071-1104.

New Zealand (2006), Director of Serious Fraud Office v A Firm of Solicitors 2006 (1) NZLR 586.

Nieman, A. (2006), "Search and seizure, production and preservation of electronic evidence", PhD thesis, North-West University, Potchefstroom.

SAPS (South African Police Service) (2016), *Practical Guide to Apply for Search Warrants in Terms of Section 21 of the Criminal Procedure Act 51 of 1977*, Pretoria.

Schwikkard, P.J. and Van der Merwe, S.E. (2002), *Principles of Evidence*, 2nd ed., Cape Town, Juta.

South Africa (1968), Heiman, Maasdorp and Barker v Secretary for Inland Revenue 1968 (4) SA 160 (W).

South Africa (1977), "Criminal procedure act 51 of 1977".

South Africa (1993), Bogoshi v. Van Vuuren NO; Bogoshi v Director Office of Serious Economic Offences 1993(3) SACR 98.

South Africa (1996), "Constitution of the republic of South Africa".

South Africa (2002), "Regulation of interception of communication and provision of communication-related information act 70 of 2002".

South Africa (2007), Minister of Safety and Security and Others v. Bennett and Others (302/06) 2007 ZASCA 136; 2007 SCA 136 (RSA); 2008 (2) All SA 26 (SCA); 2009 (2) SACR 17 (SCA).

South Africa (2008), "Thint (Pty) Ltd v. National Director of Public Prosecutions and Others, Zuma and Another v. National Director of Public Prosecutions and Others (CCT 89/07, CCT 91/07) 2008 ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC); 2008 (12) BCLR 1197 (CC)".

South Africa (2011), "Minister for Safety and Security v. Van Der Merwe and Others (CCT90/10) 2011 ZACC 19; 2011 (5) SA 61 (CC); 2011 (9) BCLR 961 (CC); 2011 (2) SACR 301 (CC)".

South Africa (2011), Polonyfis v. Minister of Police and Others (64/10) 2011 ZASCA 26; 2012 (1) SACR 57 (SCA).

South Africa (2016), Goqwana v. Minister of Safety NO & Others (20668/2014) 2015 ZASCA 186; 2016 (1) All SA 629 (SCA); 2016 (1) SACR 384 (SCA).

South Africa (2016), Heaney v. S (A464/2015) 2016 ZAGPPHC 257.

South Africa (2020), "Cybercrimes act 19 0f 2020".

South Africa (1989), "Smith", Tabata and Van Heerden v Minister of Law & Order 1989 (3) SA 627 (E) 249.

South Africa (2002), "Electronic communication and transaction act 25 of 2002".

South African Law Reform Commission (2010), "Review of the law of evidence electronic evidence in criminal and civil proceedings: Admissibility and related issues", Issue Paper 27, Project 126, Pretoria, 7.

United Kingdom (2001), "Criminal justice and police act 16 of 2001".

United States of America (2007), "United States v. Vilar, 2007 U.S. Dist. LEXIS 26993, 124-25 (S.D.N.Y.) 2007".

United States of America (2009), "United States v. Burgess, 576 F.3d 1078, 1082 (10th cir. 2009)".

United States of America (2009), "United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006-07 (9th cir. 2009) (en banc)".

United States of America (2010), "United States v. Mann, 592 F.3d 779, 786 (7th cir. 2010)".

United States of America (2011), "United States district court (USDC) (2011). the matter of the United States of America's application for a search warrant to seize electronic devices from Edward Cunnius".

United States of America Department of Justice (2009), "Searching and seizing computers and obtaining electronic evidence in criminal investigations", US Department of Justice.

Welty, J. (2011), "Warrant searches of computers", available at: https://nccriminallaw.sog.unc.edu/wp-content/uploads/2011/05/2011-05-11-PDF-Continuously-Updated-Handout-re-Warrant-Searches.pdf (accessed 22 March 2023).

Corresponding author
Jacobus Gerhardus J. Nortje can be contacted at: Koos.Nortje@nwu.ac.za