Recommendations for safeguarding mobile users from violation by third party applications

LK Mphasane

orcid.org 0000-0002-3538-0608

Dissertation accepted in fulfilment of the requirements for the degree *Master of Science in Information Technology* at the North-West University

Supervisor: Dr V Malele

Co-supervisor: Dr T Mapayi

Graduation: November 2024

Student number: 44169434

ACKNOWLEDGEMENTS

I want to thank my mother for her support and encouragement. She never allowed me to let go or give up on my learning path. I also want to thank my supervisor, Dr Vusumuzi Malele, and my co-supervisor, Dr Temitope Mapayi, for their advice and support throughout this study. Without them, I could not have completed my research study. I want to express my appreciation to North-West University, especially the School of Computer Science and Information Systems, for giving me the opportunity to study and advance my education. Finally, I would like to express my gratitude to the Mighty God for consistently accomplishing the seemingly impossible for me.

DECLARATION

I, Letsholo Kagiso Mphasane, declare that the Master's dissertation titled: "Recommendations for safeguarding mobile users from violation by third-party applications" is my own work and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

Approval	Student Signature	Supervisor
Signature		
Date	10 August 2024	10 August 2024

ABSTRACT

While digital platforms have become indispensable to daily life, the ethical dimensions of user privacy remain under-researched. This study's principal goal was to offer recommendations for safeguarding mobile device users against violations by third-party applications or social engineering applications. The study looked at and formulated recommendations towards addressing the concerns like (i) the violation of mobile users' global privacy settings by third-party applications, and (ii) the repercussions under the South African Protection of Personal Information (POPI) Act.

The study employed the confidentiality, integrity and availability (CIA) framework to comprehensively assess privacy issues associated with the gathering and sharing of users' identifiable information by third-party apps, with or without consent or awareness. Furthermore, it examined the awareness among users of digital mass surveillance, the data extracted by third-party applications and the fate of this data once removed from mobile devices.

The major findings of the study were that (i) the downloaded applications used whatever they could gather on mobile users' activities to generate revenue, and (ii) the mobile users' data were neither adequately nor consistently protected, exposing users to all the risks associated with social engineering applications. Furthermore, the literature review findings provided some themes that were triangulated by collected data from participants. These themes were used to develop and contribute 10 recommendations to safeguarding mobile users from violation by third-party applications.

The study's recommendations emphasise enhancing data security, promoting transparency in data privacy practices and encouraging users to exercise caution when sharing personal data with mobile applications. These recommendations are aimed at improving user protection and privacy practices in the mobile app ecosystem and have the potential to positively impact the fields of cybersecurity, human-centred design and technology ethics. The future studies can aim at developing an application that could strictly safeguard the users.

Keywords: Personally identifiable information, Data privacy, Cybersecurity awareness, Confidentiality, Integrity, Availability.

ABBREVIATIONS AND ACRONYMS

Apps - Applications

CIA - Confidentiality, Integrity and Availability

COBIT - Control Objectives for Information and Related Technologies

DLP – Data Loss Prevention

DNS – Domain Naming Server

ERP - Enterprise resource planning

ESG - Environmental, Social and Governance

GDPR - General Data Protection Regulation

GPS - Global Positioning Service

IBM - International Business Machines

IMEI - International Mobile Equipment Identity

IP - Internet Protocol

KPI -Key Performance Indicators

PbD - Privacy-by-Design

PII - Personal Identifiable Information

PIN - Personal Identification Number

POPIA - Protection of Personal Information Act

SDK - Software Development Kit

SIM - Subscriber Identification Module

SLR - Systematic Literature Review

SPSS - Statistical Package for the Social Sciences

SSL - Secure Socket Layer

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1. BACKGROUND

In this digital economy era, mobile users depend on mobile platforms and applications (apps) for almost everything they do with their mobile devices. These mobile apps are provided by third-party organisations for business purposes or social interactions. Although the growth in mobile apps is good for the business and social ecosystem, it has brought privacy and security concerns to unprecedented levels (Awojobi & Ding, 2020). In most cases, mobile device users are unaware of both the type of information that is extracted from or downloaded to their devices and the apps that may be of threat to their mobile devices (i.e., by hacking information or installing viruses).

Social engineering refers to how cyber-attackers could manipulate mobile users to give them important information that they could use to gain access to confidential data (Rains, 2020). In this regard, users frequently examine permission requests for mobile apps, take security measures into account and scrutinise the data being gathered, despite formal privacy restrictions that may exist (O'Loughlin et al., 2019; Garg et al., 2021). There are several concerns regarding how these apps share the data they collect, including whether personally identifiable information (PII) has been acquired from users without their knowledge or consent (Garg et al., 2021). The latter relates to the users' third-party app privacy policy relations.

Many users entrust third-party apps with their most personal information, such as how they plan to tackle their weight reduction goals or the cost of that pretty garment viewed on some of the well-known online shopping sites such as Amazon, Shein and many more (O'Loughlin et al., 2019; Schechner, 2019). Furthermore, some third-party apps are aware of the user's PII such as menstrual cycle, body weight, heart rate and pregnancy status (Fowler, 2019). Data collected by third-party apps can be valuable to the owner of the data for gaining insight or for marketing companies which aim to tailor marketing strategies to user behaviour. In this regard, the issue of third-party apps raises the question of privacy and security, thereby touching on confidentiality and integrity.

The challenge of confidentiality and integrity leads to the investigation of issues of privacy presented by digital mass surveillance and the handling of mobile users' data by third-party organisations. In this study, mobile users' awareness of their PII, digital mass surveillance, information extraction and data usage, or what happens to users' data handled by third-party apps,

was investigated. Furthermore, mobile users' understanding of and consent to the extraction and usage of their data by third parties were explored. The findings were used to offer guidelines for safeguarding users against exploitation of their data by third-party apps.

1.2. SIGNIFICANCE OF THE STUDY

The concerns regarding the misuse of data by third-party organisations by utilising their apps need to be investigated. Users do not require risky permissions from third-party apps for them to fully operate their mobile devices; however, 60% of third-party apps demand risky permissions (Michael, 2019). The latter is against the users' privacy and increases the cyber-security threats that users might encounter, thereby creating complications for the user. To address such a challenge, this study adopted a Confidentiality, Integrity, and Availability (CIA) framework. The CIA Framework points to the fact that if users' privacy, threats, and intrinsic complications are not well managed; then they might cause data leakage.

The main aim of this study was to use the CIA theoretical framework to understand and assess privacy issues relating to third-party mobile apps' collection and sharing of mobile users' personal data with or without consent or awareness. The latter together with the literature reviewed was used to make recommendations for safeguarding mobile users from violation by third-party applications. This study differs from any search engine (e.g., Google) study or analytics because it examined how commercially motivated third-party apps infringed on mobile users' security and privacy rights by (i) conducting a systematic literature review, (ii) collecting empirical data from mobile users in different clusters, and (iii) corroborating the findings from the two analyses to provide recommendations for safeguarding mobile users against violations by third-party apps.

1.3. PROBLEM STATEMENT

Globally, cybercrime is spreading at an alarming rate, to the extent that it can now be classified as a digital plague. Due to the rise of digital links, all mobile device users' activity is now vulnerable to cyberattacks (Isa, 2019). The use of third-party data collection and publication apps is a key contributing cybersecurity factor (Isa, 2019). The installation of third-party apps on mobile devices by users has potential risks that most users might not be aware of, such as copying and storing mobile user data on third-party app servers at risk of being attacked (Fowler, 2019; Isa, 2019).

Third-party mobile apps have been found to be the primary contributors when it comes to the infringement of user privacy and data misuse (Fowler, 2019; Isa, 2019; Schechner, 2019). Third-

party agencies which are marketing organisations that make use of the data supplied by third-party apps obtain accurate and trustworthy information every week that they could utilise for marketing purposes; however, this has the potential of being misused. The information collected by the mobile apps should be used correctly and no other party should be able to access such information; furthermore, the information acquired should not be transformed either maliciously or accidentally (Hiza, 2022).

There are still difficulties related to the effective implementation of strategies to counter infringements by third-party apps which violate citizens' confidentiality (Hiza, 2022). In this regard, the misuse of data by third-party organisations needs to be investigated from the users' and technical perspectives.

1.4. STUDY AIM

Users do not require risky permissions from third-party apps for them to fully operate their mobile devices; however, 60% of third-party apps demand them (Michael, 2019). This risky permissions compromise users' privacy and increase the cyber-security threats to users, thereby creating complications for the user. Most cybersecurity frameworks provide some policies and activities related to users' privacy issues.

The main aim of this study was to offer recommendations for protecting mobile users against being violated by third-party applications. It was achieved through the following goals:

(i). To use a literature review to analyse existing frameworks and highlight why the confidentiality, integrity and availability (CIA) triad framework (Mathur et al., 2019; Maroufkhani et al., 2019; Wong et al., 2019; Awojobi & Ding, 2020; Tode, 2023) is at the centre of this study.

(ii). To understand privacy issues relating to third-party mobile apps' collection and sharing of mobile users' data with or without consent or awareness.

(iii). To use the themes emerging from both (i) and (ii) to recommend guidelines for safeguarding mobile users against being violated by third-party applications.

Both primary and secondary research objectives assist to achieve the study goals. The primary objectives are directly aligned to the study's primary outcome (Kapoor & Goyal, 2023), while the secondary objectives, which are further categorised into empirical and theoretical objectives,

provide additional outcomes for the study. The following primary and secondary research objectives were adopted.

1.4.1. Primary objective and research question

The primary objective of this study was to collect primary and secondary data to understand and determine the trends and themes that could assist to recommend guidelines for safeguarding mobile users against violations by third-party organisations. The primary research question adopted in this study was phrased as follows: "How can mobile users be safeguarded from violation by third-party apps?"

1.4.2. Secondary objectives and research questions

The secondary objectives are subdivided into empirical and theoretical objectives. The theoretical objectives examine, measure, analyse, test and revise current theories and create new theoretical viewpoints (Kapoor & Goyal, 2023). Empirical objectives examine, measure, analyse, test and improve existing procedures and develop new ones (Kapoor & Goyal, 2023). Both empirical and theoretical objectives then lead to a practical and best practice that could bring some innovative solutions to the research problem. Table 1.1 illustrates this study's theoretical and empirical objectives with their underlying research questions.

Table 1.1: Empirical and theoretical objectives and their research questions.

Type of Objective	**Objectives**	**Research Questions**
Theoretical	a) To explore the concept of digital mass surveillance and how it impacts user privacy	(i). What is digital mass surveillance? (ii). How is digital mass surveillance used to target users?
	b) To identify the types, extent of data and routinely collected by third-party apps.	(iii). What kind of data is collected, why is it collected, and what is used for?
Empirical	c) To identifying the level of consent provided by users.	(iv). Are mobile device users aware of the level of consent they provide to third-party agencies? (v). How much of the data is collected beyond the user's consent? (vi). How can mobile device users be educated about the effect of online privacy and security?

A. Theoretical objectives

In this study the theoretical objectives (TO) refer to all study objectives that could be addressed by using existing literature. Two TOs were formulated to achieve the main research goal.

- **TO 1: To explore the concept of digital mass surveillance and how it impacts user privacy**

  The purpose of this objective was to determine the levels of transparency, oversight and accountability in surveillance practices, as well as the efforts to develop privacy-enhanced frameworks for safeguarding individual rights in the digital age (Huckvale et al., 2019). However, striking a balance between security imperatives and privacy rights remains a significant challenge in an increasingly interconnected and surveilled world. Digital mass surveillance can be used to target users online in various ways, leveraging the vast amount of data collected to identify, monitor and potentially influence individuals' online activities. To achieve this objective the following research questions were addressed:

  - RQ 1: How does digital mass surveillance impact user privacy?
  - RQ 2: How is digital mass surveillance used to target users?

- **TO 2: To identify the types and extent of data routinely collected by third-party apps**

  Any search engine (e.g., Google) or marketing report could point to the fact that third-party apps violate users' privacy (Hiza, 2022). This does not address the levels of transparency, oversight and accountability in surveillance practices, or the efforts to develop privacy-enhanced frameworks that could safeguard users' privacy. Thus, the quantity and extent of data typically gathered by third-party apps and whether that violates the users' privacy and security form the crux of this objective. Equally important are the level of understanding of the user about collected data and the level of consent that users give to third-party app organisations. To achieve this objective the following research question was addressed:

  - RQ 3: What kind of data is collected by third-party apps? Why is it collected?

B. Empirical objectives

In this study the empirical objective (EO) refers to all study objectives that could be addressed by collecting and analysing empirical data. Two EOs were formulated to achieve the main research goal.

- **EO 1: To identify the level of consent provided by users**

The purpose of this objective was to determine the level of permission granted by users to third-party apps by evaluating the transparency, specificity and voluntariness of the consent process. Third-party apps collect a wide range of data from users, often with the goal of providing personalised services, improving user experience and monetising user information (Huckvale et al., 2019). While some mobile device users are aware of the level of consent they grant to third-party agencies, others may be unaware or may not completely comprehend the ramifications of their consent. The research question was created to increase transparency and encourage user education.

- RQ 4: Do users understand why third-party app organisations collect their data? Do users consent to such data collection?

Users with a higher degree of technological literacy may be more aware of the consequences of giving consent to third-party agencies and may actively adjust their privacy settings. Users with poorer technical literacy, on the other hand, may be less aware of these difficulties and hence more inclined to accept default settings without fully comprehending the implications. The purpose of this objective was to use TO 1, TO 2 and EO 1 to identify themes that could lead to safeguarding mobile users against violations by third-party apps. In this regard, the following research question was addressed:

- RQ 5: How can mobile device users be educated about the effect of online privacy and security?

1.5. STUDY CONTRIBUTION

The concerns pertaining to misuse by third-party organisations through their apps need to be investigated. The fact that 60% of third-party apps demand risky permissions for their devices to function optimally compromises users' right to privacy and increases cybersecurity threats. Unlike most pieces of information based on a Google search, this paper provides a highly structured, academic analysis of privacy issues associated with third-party apps.

While past studies outline privacy and security concerns, they often lack viable and affordable strategies rooted in robust theoretical frameworks such as the CIA triad. This study addressed this existing gap by utilising the CIA framework to examine privacy risks inherent in the collection and

sharing of personal data belonging to third-party application users. Chapter 5 offers recommendations for safeguarding mobile users' privacy and security.

1.6. CHAPTER LAYOUT

This dissertation comprises six chapters, which are briefly summarised below.

Chapter 1: Introduction

- This chapter presents the study background, problem statement, aims and goals. It motivates the investigation and provides a concise description of the study's objectives. Furthermore, it summarises the dissertation layout.

Chapter 2: Literature review

- This chapter briefly describes the theoretical framework adopted in the dissertation. It identifies areas of earlier research, similar study gaps, discrepancies between studies and unresolved questions within the literature.

Chapter 3: Methodology

- The research design, data collection and analysis are covered in this chapter. The study paradigms and methodology are described, followed by a discussion of the adopted paradigm. Furthermore, this chapter sets out how to collect and analyse data. It also highlights relevant variables to produce the necessary information.

Chapter 4: Findings and discussion

- This section summarises the study findings as well as the growing complexities of mobile users and the online environment. It emphasises the importance of regular ongoing training programmes for basic internet security and the development of a security culture among smart mobile device users.

Chapter 5: Contribution

- An important part of the analysis step is covered in this chapter. The contribution of the dissertation to the body of knowledge is discussed. The recommendations deal with the research findings and propose ways to address the problems and limitations thereof.

Chapter 6: Conclusion and future work

- This chapter summarises the dissertation and suggests areas for further research.

1.7. CONCLUSION

This chapter introduced the study by setting out the research background, research aims and objectives. The research questions were presented to give a framework for how the study's primary aim could be achieved. The study's objectives help to differentiate it from a mere search engine (e.g., Google search) or marketing report. The next chapter provides this study's literature framework.

CHAPTER 2

LITERATURE REVIEW

2.1. INTRODUCTION

A literature review is given in this section with an emphasis on cybersecurity frameworks and models or strategies for safeguarding mobile users' privacy, especially against third-party apps. Furthermore, it focuses on the types and extent of the data being gathered by the third-party apps as well as the overall level of consent given by the users to the third-party apps. In this regard, the literature review technique was used to source the necessary knowledge (Malele, 2023).

This chapter begins by analysing users' behaviour regarding application privacy by setting out the data issues in the third-party app ecosystem, followed by frameworks that could assist this ecosystem to protect the rights of the users. Thereafter, the models that are used to implement the frameworks are presented and the necessary themes emerging from the implementation are identified as indicators leading towards recommendations. The established literature gaps and how this study addresses such gaps are presented.

2.2. THIRD-PARTY APPS

No-one can deny the importance of smartphones and third-party apps in today's world (Kim, 2017). People's lives have been made much easier because of how varied and modern their applications are. Mobile device users can install third-party apps from various sources, and these apps typically require a range of permissions to function (Awojobi & Ding, 2020). To safeguard sensitive user data and stop privacy breaches, most contemporary mobile devices especially smartphones adopt the permission-based paradigm (Reardon et al., 2019). For example, connections to the system API, databases or message-passing mechanisms may require permission. The public API defines 8648 methods, some of which are restricted by permissions (Lenarduzzi et al., 2019). If a third-party app wants to access resources or user information, it will request permission from the user. The developer must define the application's permissions by specifying them in the patent file and demanding that the user approves them at runtime. When an app requests significant data from a user or device, developers must design a valid privacy policy.

The privacy policy included in the app comprehensively outlines how the app can gather, use and share data, including the types of third-party apps and who will receive the data. Furthermore, it is the user's sole responsibility to decide whether to allow an app that requests specific permissions on

his or her device, because most apps on the market request data that are irrelevant to the app's main feature, which could result in the leakage of private information or inefficient use of mobile resources. This situation is concerning for those with low literacy who cannot make their own decisions about the legality of apps. Even among literate smartphone users, the majority ignore privacy permissions when installing programmes on their devices. In this way users become victims of data theft, which can lead to more significant concerns for them (Zou et al., 2019).

The fundamental issue is that most users do not read or comprehend the purpose of the permissions asked by the apps they install, allowing programmes to gain illegal access to and misuse their devices (Alshomraniet et al.,2023). One of the major challenges is privacy concerns, such as data leakage (Baddar, 2017) and superfluous permissions (Zou et al., 2019), which could result in the release of personal information. While some of the flaws may be related to the system's liberty, portability and ease of use, others are caused by a lack of awareness and technical talent among mobile application developers (Alshomraniet al.,2023).

Many mobile app developers do not prioritise privacy and are unaware of the potential harm caused by third-party advertisements and analytics technologies (Appel et al., 2020). A detailed survey of mobile app security concerns showed that up to 70% of Android applications gained permissions that were not required for the programme to function (Alshomraniet al.,2023). These superfluous permissions are bad in terms of increased resource consumption and private data leaking. The threats have been classified into five general categories: information leakage, privilege escalation, repackaging, denial of service (DoS) attacks and collusion (Alshomraniet al.,2023). In recent years, mobile apps have had a major impact on business, society and lifestyles. Various app markets provide a diverse choice of apps for entertainment, business, health care and social life.

2.3. APP ECOSYSTEM

With the increase in social media use in day-to-day lives, the individual’s digital presence has expanded significantly. Kollnig et al. (2021) determined that the present app marketplace was centred around two major ecosystems of apps and that there was a vast range of sources in the app store from where the users could easily install the apps. These would include the official app stores of various platform providers, and the range of stores offered by the device manufacturers as well as various third parties. While the underlying objective of the stores is rather similar in terms of serving as the distribution channel for hosted apps, there is considerable variation in the linked security and protection of privacy. This would include both guidance and the controls for

safeguarding the users of the apps, and the procedures plus policies implemented for guiding and reviewing the activities of the developers.

Many users are concerned about the overall advisability of trusting the apps as well as the linked utilisation of the data (Huckvale et al., 2019). Due to this, the users find themselves hugely dependent on the processes implemented by the organisations for checking the overall credibility of all apps being hosted. However, in reality the practices might vary greatly across the providers, ranging from the stores having clear review processes and attempting to ensure that the developers communicate the methods by which the apps are collecting and using user data to situations where the apps are made available even though the characteristics which could put the devices as well as the data of the users at risk are known.

An investigation into the types of data collected by third-party apps and the extent of the data collected by third-party apps showed that various types of apps were released by third-party developers (Gordon et al., 2020). These apps are used to help improve users' daily lives and tasks. Some researchers have determined that in the present interconnected world, mobile apps are becoming an integral part of the daily lives of people. With increasing dependence on the applications, the quantity of the data being collected and stored, as well as the processes, has become of major concern.

2.4. TYPES OF COLLECTED AND DISTRIBUTED PERSONAL DATA

Mobile devices are now widely used around the world and their popularity is rapidly expanding. Globally, it was expected that there would be approximately 7.34 billion mobile users by 2021, up from about 4 billion in 2011 (Wamba et al., 2015; Turner, 2021). This increase signifies the level of demand for good mobile services. Parallel to this, mobile app development has become a thriving industry, particularly the use of artificial intelligence in mobile apps, which has led to an increase in mobile device users downloading and using apps for purchasing services and products for their daily lives (Furletti et al., 2017). The interaction of the mobile device users with the apps produces personal identifiable information (PII) and the profiling of each user.

The issues regarding PII as acquired by third-party agencies beyond what is specified in the privacy and security policy have been gradually growing (Moreno et al., 2016). This means the growing user numbers lead to the growth, collection and capturing of PII data, stored in large amounts through mobile apps (Trabucchi et al., 2017). As a result, mobile users are concerned about how

personally identifiable information (PII) is collected by mobile apps (Wijesekera et al., 2015). In the discussion of PII data, CIA constitutes three basic cybersecurity concerns (Taherdoost, 2012; Tipton et al., 2016; Yin et al., 2020). Hence, it was adopted as this dissertation's theoretical framework.

Currently various types of apps are being released by third-party developers to improve users' daily tasks. Mobile apps are becoming an integral part of people's daily lives (Gordon et al., 2020). With increasing dependence on apps, the major stakeholders for whom the data hold great value are the app providers, advertisers and researchers. In this regard, through the analysis of user data the app providers could easily gain insight into the users' preferences and behaviour (Talal et al., 2019).

Several app providers depend on third-party services plus tools for functions like advertisement targeting, analytics and payment processing (Talal et al., 2019). Due to the variety of app providers and adherence to similar security standards, these third-party integrations leave the field wide open for additional risks to the security of the apps that mobile device users download.

2.5. PERSONALLY IDENTIFIABLE INFORMATION EXPOSURE

Personally identifiable information (PII) refers to any data that can be used to identify, contact or locate an individual. It encompasses a range of data, both direct and indirect, that can pinpoint a specific person. Based on their use and specificity, these identifiers can be generally divided into several classes. For instance, people's passport numbers can be used to uniquely identify them, along with other details like race and date of birth (Garg et al., 2021). PII is crucial in contexts such as cybersecurity, data protection and privacy regulations, as unauthorised access to or misuse of this information can lead to identity theft, fraud and other privacy breaches (Garg et al., 2021).

The sensitivity of personally identifiable information (PII) varies based on how it can be used and the potential consequences of its exposure. Here is a hierarchy of PII, according to a study by Garg et al (2021), which ranges from generally less sensitive to more sensitive, with reasons why certain types are deemed more critical:

A. Less sensitive PII:

- Name: While important, names alone generally aren't enough to commit fraud but can be combined with other data for identity theft.

- Email address: Useful for contact but not inherently dangerous without additional information.

B. Highly sensitive PII:

- Bank account and credit card information: Directly linked to financial accounts and can lead to significant financial loss if exposed.
- Medical records: Health information is highly sensitive due to privacy concerns and potential misuse for insurance fraud or discrimination.

C. Most sensitive PII:

- Biometric Data: Fingerprints, facial recognition and other biometric identifiers are unique and difficult to change if compromised.
- Passport number: Can be used for identity theft and fraudulent activities, particularly for international travel.

More sensitive PII can lead to great harm if exposed or misused, including identity theft, financial loss and severe privacy violations. Data like biometric identifiers can't be easily changed if compromised, unlike a password or email address. Financial, medical and biometric data can be used in more damaging ways than less sensitive information like a name or phone number. Mobile apps can pose significant risks to personally identifiable information (PII) due to various factors related to their design, functionality and data handling practices. Here are some of the primary ways in which mobile apps can be a risk to PII:

- Insecure storage: If PII is stored locally on the device without encryption, it can be vulnerable to unauthorised access if the device is lost or stolen.
- Unencrypted transmission: Data transmitted over the internet without encryption (e.g., through unsecured HTTP connections) can be intercepted and accessed by malicious actors.
- Third-party integrations: Apps that integrate with third-party services may inadvertently share PII with those parties without user consent or adequate safeguards.

Almost every service used on the internet has its own mobile application. To limit the risks associated with exposure, sensitive PII must be protected through strong data security procedures and compliance with applicable privacy regulations.

2.6. ONLINE PRIVACY POLICIES

Social networking platforms have transformed how people communicate and do business on a global scale. The social media networking sites have produced significant positive outcomes due to their widespread use, cost effectiveness and popularity which gain them large audiences. These in turn produce huge volumes of data which are essential for the companies to enhance their services. Considering the significance of this amount of data, it has become mandatory for the social networking sites or third-party app organisations to acquire consent from the users to use their data.

Online users have confidentiality concerns and want to manage their online presence to ensure that they have control over their private details shared online; in a study conducted by CISCO 32% of the participants expressed concern over their data security and online privacy (Mugadza & Mwalemba, 2023). Furthermore, the actions and attitudes of online users towards data security and their online presence displayed some proactiveness in trying to achieve data security (Mugadza & Mwalemba, 2023), although this needed some investigation and analysis of online privacy policy. Online privacy policy of third-party apps is guided by a combination of legal regulations, industry standards and best practices. Here are the primary factors:

- Transparency: Explain how the app collects, uses, shares and protects user data.
- Rights and choices: Inform users about their rights regarding their personal data, including how they can access, correct or delete their data.
- Regulatory requirements: Ensure compliance with relevant data protection laws and regulations.
- Avoid legal penalties: Reduce the risk of fines, sanctions and legal actions by adhering to legal standards.
- User confidence: Build user trust by demonstrating a commitment to protecting users' privacy.
- Reputation management: Enhance the app's reputation and user loyalty through responsible data practices.

Third-party apps fail to disclose their data gathering techniques for a variety of reasons, including financial interests, technological complexity and regulatory constraints. The following are some of the methods they employ to conceal their unethical practices.

- Incomplete disclosures: Some third parties may not fully disclose all data collection practices or third-party sharing arrangements.
- Complex language: Use of complex or vague language that makes it difficult for users to understand the full extent of data practices.
- Limited user control: Not providing sufficient mechanisms for users to manage their data preferences easily.
- Infrequent updates: Not updating the privacy policy regularly, leading to outdated information that does not reflect current practices.
- Insufficient security: Failing to implement or maintain adequate security measures to protect user data against breaches or unauthorised access.
- Reactive approach: Taking a reactive rather than proactive approach to security and privacy issues.
- Excessive data collection: Collecting more data than necessary for the app's functionality or stated purposes.
- Data retention: Retaining data longer than needed, increasing the risk of data breaches and non-compliance with data retention regulations.
- Opaque practices: Not being clear about what data are shared with third parties, including advertisers and analytics providers.
- User notification: Not adequately informing users when changes to data sharing practices occur.
- Difficult access: Making it difficult for users to exercise their rights to access, correct or delete their personal data.
- Delayed responses: Taking too long to respond to user requests regarding their personal data.

By addressing these areas and adopting a user-centric approach, third-party apps can improve their privacy policies and better protect user data, thereby enhancing trust and compliance.

2.7. CYBERSECURITY FRAMEWORKS

The Information and communication technology (ICT) security, i.e., computer security, refers to the security that provides confidentiality, integrity, availability, nonrepudiation, accountability, authenticity and reliability of information resources through computers (Von Solms & Van Niekerk, 2013). Information security (infosec) refers to preserving the confidentiality, integrity and availability of business information, safeguarding business continuity and reducing business impairment (Horne et al., 2016). Cyber security refers to information security that includes the defence of information, people and organisational assets (i.e., networks, infrastructure, etc.) through availability, integrity and confidentiality (Horne et al., 2016).

The terms computer security, information security and cyber security are used interchangeably in literature as well as by non-experts, although the common thread among the terms is confidentiality, integrity and availability. Literature has a plethora of information security and cybersecurity frameworks with the common thread of confidentiality, integrity and availability (CIA). Some of the indicators for measuring users' CIA are privacy, vulnerability, users' behaviour, users' awareness, risk and ethics (Brynielsson et al., 2016; Horne et al., 2016; Hoofnagle et al., 2019; Padilla & Freire, 2019; Wong et al., 2019; Enoch et al., 2020; Awojobi & Ding, 2020; Tode, 2023). Cybersecurity frameworks are vital for ensuring the security of third-party applications. These frameworks provide structured approaches to managing and mitigating cybersecurity risks. Below are some commonly adopted frameworks for third-party apps and reasons why they are favoured.

2.7.1. Cyber situation awareness (CSA)

The framework is essential in the identification, processing and comprehending of the details of the cyber-attack. It emphasises the real time awareness of the threats, vulnerabilities and current security incidents. It provides a comprehensive view of the threats and vulnerabilities which is essential in responding to the various security threats. The framework for the online privacy and data security of mobile users would be effective as it would focus on understanding the threats, vulnerabilities and contemporary breaches (Brynielsson et al., 2016). It would also enable online users to detect abnormal behaviours and thus identify mobile security breaches and respond effectively. One notable example of a CSA framework being used in third-party apps is the MITRE ATT&CK framework. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally recognized knowledge base of adversary tactics and techniques based on

real-world observations. It provides a detailed matrix of how adversaries operate, offering insights into their methods and the potential impacts of their actions.

Security Information and Event Management (SIEM) systems or Threat Intelligence Platforms (TIPs) use ATT&CK to correlate indicators of compromise (IOCs) with known attack techniques. This helps in detecting and responding to threats more effectively (Brynielsson et al., 2016). By integrating MITRE ATT&CK into their security frameworks, third-party apps can significantly enhance their ability to detect, analyze, and respond to cybersecurity threats in real-time, thereby improving overall security posture and resilience. While Cyber Situation Awareness (CSA) frameworks like MITRE ATT&CK provide valuable insights and improve security posture, their use in third-party apps comes with several limitations:

- Implementing and maintaining CSA frameworks requires skilled personnel and can be costly, which might be a challenge for smaller organizations or those with limited resources.
- The comprehensive nature of frameworks like MITRE ATT&CK can lead to information overload, making it challenging for security teams to prioritize and act on relevant threats.
- The broad range of techniques covered by CSA frameworks may lead to a high number of false positives, potentially diverting attention away from genuine threats.

In summary, while CSA frameworks are powerful tools for enhancing cybersecurity, their effectiveness in third-party apps can be constrained by complexity, limited contextual awareness, resource demands, and the need for continuous updates and accurate data. De need to carefully consider these limitations and integrate CSA frameworks as part of a broader, multi-layered security strategy.

2.7.2. General data protection regulation (GDPR)

The GDPR framework aims to reinforce privacy through the adoption of tough privacy and security policies worldwide. The GDPR originated in Europe but applies globally to the organisations that target the information of online users in Europe. The framework involves imposing huge fines for those who breach the security and privacy standards (Hoofnagle et al., 2019). This includes penalties of up to tens of millions of euros. According to the GDPR framework, personal data involve any information that can be used to identify a person, such as names, email addresses and location information, and infringement of such data attracts penalties.

The principles in this framework include transparency that requires the owners of the data to be aware of all the processing done on their data. It also dictates that processing data should be restricted to lawful purposes. Limits are placed on the amount of data collected; only the necessary amount of data may be collected. The principles also focus on the accuracy and storage limitations that direct that private data should be kept accurate and updated while storing should only last until the specified purpose has been achieved. Integrity principles require that the processing of personal data should be done in a manner that guarantees security, integrity and confidentiality, while accountability ensures that the personal data are used according to the GDPR principles.

Third-party applications often need to comply with GDPR requirements to ensure that personal data is processed lawfully, transparently, and securely. Here is a concrete example of how GDPR compliance frameworks are implemented in third-party apps. A CRM app, like Salesforce or HubSpot, which handles personal data of clients and prospects, must comply with GDPR to ensure the protection and proper management of personal data. These CRM systems integrate advanced encryption standards and security measures within the app to safeguard personal data. Furthermore, the CRM app includes automated alerts and reporting tools to track and notify data breaches within the required 72-hour timeframe. By incorporating these GDPR compliance features, third-party apps like CRM systems can help organizations meet regulatory requirements, protect personal data, and build trust with users' standards (Hoofnagle et al., 2019).

While the General Data Protection Regulation (GDPR) provides a robust framework for data protection and privacy, implementing it in third-party applications can present several limitations and challenges.

- Data Location Constraints: GDPR imposes restrictions on transferring personal data outside the EU. This can be challenging for third-party apps that rely on global data centers or cloud services.

- Financial Costs: Implementing and maintaining GDPR compliance features can be costly, especially for smaller organizations or startups.

- End-User Awareness: Ensuring that end-users understand their rights under GDPR and how to exercise them can be challenging. Effective communication and education are necessary but often overlooked.

In summary, while GDPR provides a strong framework for data protection, its implementation in third-party applications involves several limitations and challenges. Addressing these limitations requires a thorough understanding of the regulation, ongoing investment in resources, and a proactive approach to compliance management.

2.7.3. Contingency theory (CT)

The theory emphasises being prepared for sudden events that include major breaches or national disasters as a way of ensuring cybersecurity. Due to the constant occurrence of events that disrupt data security, contingency plans are essential in preventing data breaches. The theory focuses on the identification of new threats to cybersecurity to keep contingency plans updated to deal with the attacks (Padilla & Freire, 2019). Currently the theory seeks to eliminate data insecurity through threat intelligence that ensures that a company is well informed on the emerging threats. It also involves incidence response plans for prompt reaction to emerging security threats. Considering the data privacy of mobile users, the contingency theory focuses on robust threat analysis to identify the emerging trends to online privacy and implement effective strategies to counter the threats.

In the context of third-party applications, Contingency Theory can be applied to adapt security and risk management practices based on various factors such as the application's purpose, the type of data it handles, and the regulatory environment. Here's a practical illustration of how Contingency Theory can be applied. A cloud storage service provider, like Dropbox or Google Drive, needs to manage various aspects of security and compliance based on the unique needs of its clients (Padilla & Freire, 2019). Using Contingency Theory, the provider tailors its approach to different types of clients and data requirements, rather than applying a single, uniform strategy. This ensures that resources and efforts are focused where they are most needed, rather than applying uniform practices that may not be appropriate for all clients. Allows the provider to offer customized security, compliance, and support solutions that fit the unique needs of different clients, enhancing overall effectiveness and satisfaction. By applying Contingency Theory, the cloud storage service provider effectively adapts its practices to meet varying client needs and regulatory demands, leading to a more responsive and contextually appropriate approach to security and compliance. By applying Contingency Theory, the cloud storage service provider effectively adapts its practices to meet varying client needs and regulatory demands, leading to a more responsive and contextually appropriate approach to security and compliance.

While Contingency Theory provides a flexible approach to managing third-party applications by adapting practices to fit specific circumstances, there are several limitations and challenges associated with its implementation.

- Customization Challenges: Tailoring strategies and practices for different scenarios can be complex and resource intensive. It requires a deep understanding of various contexts and the ability to adapt solutions accordingly.

- Risk of Inconsistency: Tailoring practices to different contexts can lead to inconsistencies in how security, compliance, and operational standards are applied. This might create gaps in overall security or compliance.

- Adapting to evolving regulatory requirements can be challenging. Changes in laws or standards might require frequent updates to tailored solutions, adding to the complexity.

In summary, while Contingency Theory offers a flexible and context-sensitive approach to managing third-party applications, its implementation can be complex, resource-intensive, and prone to inconsistencies. Developers must carefully balance the benefits of tailored solutions with the potential challenges and limitations to effectively apply Contingency Theory in practice.

2.7.4. Cyber-attack theory (CAT)

The framework explains how the malicious attackers use the cyber domain to acquire and use personal data. The framework focuses on the strategies, procedures and techniques that the attackers use in the process. The components of the framework include the strategies that explain what the attackers aim to achieve, such as data theft. Technique is another component that entails the procedures that the attackers follow by exploring the weaknesses, social engineering and malware used by the attackers to acquire data (Enoch et al., 2020). In the context of this study the framework would be essential, as it involves the identification of the interests that make an attacker target online users and the strategies used by the attacker for data theft.

One prominent example of applying Cyber-Attack Theory in third-party applications is the use of the Kill Chain Model developed by Lockheed Martin (Naik et al., 2022). This model helps organizations understand and disrupt the stages of a cyber-attack. A third-party application, such as a financial management tool, integrates the Kill Chain Model to enhance its security posture by

detecting, preventing, and responding to cyber-attacks. The app has data loss prevention (DLP) measures in place to detect and prevent unauthorized data transfers. It also has incident response procedures to quickly address and mitigate any actions taken by attackers. Implementing measures at each stage of the Kill Chain allows the app to proactively prevent attacks rather than just reacting to them after they occur (Naik et al., 2022). Applying the Kill Chain Model in a third-party application like a financial management tool helps in systematically addressing and mitigating cyber-attacks by covering each phase of the attack lifecycle. Using Cyber-Attack Theory, such as the Kill Chain Model or other attack models, in third-party applications has several limitations. Here's a breakdown of these limitations.

- Attack techniques and tactics continually evolve, and Cyber-Attack Theory models may become outdated. Regular updates and adaptations are necessary to stay effective, which can be challenging.
- Focusing heavily on specific attack models might lead to a narrow view of cybersecurity, potentially overlooking other important aspects such as insider threats or data breaches.
- Extensive monitoring might lead to false positives, where legitimate activities are flagged as suspicious, which can impact performance and user experience.

In summary, while Cyber-Attack Theory provides a structured approach to understanding and mitigating cyber threats, its application in third-party apps is accompanied by challenges related to complexity, resource requirements, adaptability, and integration. Developers need to balance these limitations with the benefits of a comprehensive security framework to effectively protect against cyber threats.

2.7.5. Control objectives for information and related technologies (COBIT)

COBIT is a framework that sets out the practices for effective information and technology management. A major aspect of COBIT is information technology governance whose objective is to ensure proper use of information and avoid the risk of information infringement (Talab & Flayyih, 2023). Integration is another aspect of COBIT that ensures that the guidelines, regulations and best practices for information collection, sharing and use are maintained.

The framework has five principles that include stipulating the guidelines, good practices and objectives of good information technology governance; process description that ensures that the process model can be used by anyone; control objectives that involve a whole list of requirements to ensure effective control of information technology; management guidelines that are essential in

indicating responsibilities and giving suggestions on how information technology governance can be achieved; and the maturity models which explain how the information technology processes adjust to changes and how gaps can be filled.

An effective example of the COBIT being applied in third-party applications is the implementation of COBIT principles by a Software-as-a-Service (SaaS) provider that offers an enterprise resource planning (ERP) system. This type of application handles a wide range of business functions, including financial management, human resources, and supply chain operations, making effective IT governance and risk management crucial. The provider uses COBIT's performance metrics to track key performance indicators (KPIs) such as system uptime, transaction processing speed, and customer satisfaction. They regularly review these metrics to ensure the system meets performance standards. e ERP system integrates robust security measures including multi-factor authentication (MFA), encryption of data at rest and in transit, and regular security patching. The provider conducts security training for employees and implements monitoring systems to detect and respond to potential security incidents. Applying the COBIT framework to a SaaS ERP system helps ensure robust IT governance, effective risk management, compliance with regulations, and optimized performance.

While the COBIT offers a structured approach to IT governance and management, applying it to third-party applications presents several limitations and challenges:

- Strict adherence to COBIT's comprehensive control requirements might lead to over-compliance, where controls are put in place that are not necessary or do not add significant value.
- Implementing and maintaining COBIT practices can be resource intensive. It involves costs related to acquiring tools, training personnel, and possibly hiring specialized staff.
- Applying COBIT practices to scale with growing third-party applications or expanding business requirements may require additional modifications and resources.

In summary, while COBIT provides a comprehensive framework for IT governance and management, applying it to third-party applications involves complexities related to implementation, resource demands, adaptability, and potential overhead. Developers need to

carefully consider these limitations and balance the benefits of COBIT with the specific needs and constraints of their third-party applications.

2.7.6. Confidentiality, integrity and availability (CIA) triad

The CIA framework, also known as the CIA triad, is a model used to guide information security policies and practices. Each component of the CIA triad represents a crucial aspect of data security (Horne et al., 2016; Mathur et al., 2019; Maroufkhani et al., 2019; Wong et al., 2019; Awojobi & Ding, 2020; Tode, 2023). Furthermore, CIA could be described as follows:

- C – Confidentiality refers to information and communication technologies (ICT) privacy (Awojobi & Ding, 2020). In the government sector, confidentiality describes the limiting of access to classified material provided to authorised parties (Awojobi & Ding, 2020). In the business sector, it refers to protecting private data, like a customer's address, age and credit card number (Awojobi & Ding, 2020). In the human or user context, it refers to the protection of sensitive data about the user’s livelihood.

- I – Integrity describes the dependability of information and features offered by third-party apps (Awojobi & Ding, 2020). It is the knowledge that data or computing operations have not been corrupted or destroyed (Awojobi & Ding, 2020).

- A – Availability guarantees prompt and ongoing access to the system's data for authorised app users (Wong et al., 2019). Encryption is vital for information security but can also affect availability. If encryption is too strong or complex, it can slow down data access and processing, impacting system performance and availability.

Applying the CIA Triad in third-party applications involves implementing measures to safeguard these three core principles. For example, a third-party cloud storage application provides file storage and sharing services to various businesses and individual users. The application incorporates the CIA Triad principles to ensure the security and reliability of its services. The cloud storage application uses strong encryption methods to protect data at rest and in transit. Files are encrypted using Advanced Encryption Standard (AES) before being stored and decrypted only when accessed by authorized users. The application uses cryptographic hash functions (e.g., SHA-256) to generate hashes for files when they are uploaded. These hashes are checked during downloads and modifications to verify the file’s integrity. The application uses redundant servers and data centers across multiple geographic locations to provide high availability and disaster

recovery. Regular backups are performed to ensure data can be restored in case of hardware failure or other issues.

The CIA framework provides comprehensive security structure for recommendations that could be utilised for the protection of mobile users' PII data which could be accessed through mobile apps; therefore, the CIA triad was chosen as the theoretical baseline for examining the security and privacy vulnerabilities associated with third-party apps. In summary, applying the CIA Triad to a third-party cloud storage application involves implementing measures to protect data confidentiality, ensure its integrity, and guarantee its availability. While this approach provides a solid foundation for data security and service reliability, it also presents challenges related to complexity, cost, performance, and scalability that need to be carefully managed.

2.8. ADOPTED FRAMEWORK

Different frameworks are discussed from paragraphs 2.3.1 to 2.3.6. Table 2.1 summarises the benefits and challenges addressed in each framework and how they link to this study. Evidence from Table 2.1 shows that if a study investigates mobile users' privacy through confidentiality, integrity and availability, the CIA triad and the GDPR framework could be adopted as literature framework. Furthermore, if safeguarding mobile users against violation is also a key indicator, dependability together with CIA should be included as one of the key factors. For example, Li and Yang (2019) discuss the security and privacy challenges associated with mobile app development and how applying the CIA triad can help mitigate these challenges, giving insight into safeguarding mobile apps by ensuring that they adhere to confidentiality, integrity and availability principles.

While GDPR was used to highlight the best practices and challenges in mobile applications, Guamán et al. (2021) outlines the best practices for achieving GDPR compliance in mobile apps and emphasises the challenges of developers; these cover aspects like user consent, data minimisation and transparency requirements under GDPR and offer practical solutions for mobile app developers to address the requirements. Thus, the framework that embraces safeguarding mobile users' privacy through CIA and looks at dependability violation is the CIA triad, leading to its adoption for this study.

Table 2.1: Frameworks

Frameworks	Benefits	Challenges and limitations
Cyber situation awareness (CSA)	Improved threat detection Proactive security posture Informed decision making	Data overload Integration complexity Skill requirements Cost
General data protection regulation (GDPR)	Enhanced privacy and security Empowerment of individuals Encouragement of best practices	Compliance costs Complexity Continuous monitoring
Contingency theory (CT)	Realistic approach Enhanced flexibility Holistic perspective	Complexity Ambiguity Lack of prescriptive guidelines
Cyber-attack theory (CAT)	Proactive defence Enhanced preparedness Risk reduction	Complexity Evolving threat landscape Human factor Resource constraints
Control objectives for information and related technologies (COBIT)	Improved IT governance Enhanced risk management Better compliance	Complexity Resource intensity Measuring effectiveness
Confidentiality, integrity and availability (CIA) triad	Comprehensive security Risk mitigation Operational efficiency	Resource intensive Evolving threat Complexity

2.9. SIMILAR STUDIES AND LITERATURE GAPS

Safeguarding the privacy of mobile users is crucial, given the widespread use of mobile devices and the sensitive nature of the data they handle. Some literature works discussed below were done to try and safeguard the privacy of mobile users.

An observational study to show how the formulation of assistive structured privacy guidelines could be helpful in allowing software engineers to improve data subject privacy within their systems (Perera et al., 2020). They found that, irrespective of engineers' level of expertise, such guidelines led to similar levels of incorporation of privacy practices in the resulting designs. Based on this, Perera et al. (2020) published the following PbD guidelines:

- Minimise data acquisition
- Minimise number of data sources
- Minimise raw data intake

- Minimise knowledge discovery
- Minimise data storage
- Minimise data retention period
- Hidden data routing
- Data anonymisation
- Encrypted data communication
- Encrypted data processing.

These PbD measurements are the basic source of information used in this study which recommends measures for protecting mobile users against violations by third-party applications. Implementing the models and framework helps ensure that mobile user privacy is protected through a combination of technical measures, policy enforcement and compliance with regulatory standards. By prioritising user consent, transparency, data minimisation and robust security practices, organisations can build trust and safeguard the privacy of their mobile users.

Hayes et al. (2020) present a case study on how privacy issues arise when the data collected are more than was expected by the user, thereby increasing security risks for the individual (Ali et al., 2018; Burger, Oz, Kennedy & Crooks, 2019). It shows several concerns about how mobile apps collect and distribute personal information without the user's knowledge. Some of these concerns are about the disclosure of data being gathered by the apps and what PII is collected from individuals without their knowledge or consent (Tipton et al., 2016; Yin et al., 2020). The study provides an analytical framework highlighting the steps required to analyse apps and uncover privacy issues associated with mobile apps, as well as the possible use of the information collected. It shows that permissions and privacy policies alone are insufficient to determine how invasive an app could be. In this regard, the themes emerging from Hayes et al. (2020) that were relevant to this study were consequently focused on the “confidentiality” aspect of the C.I.A. triangle for determining concerns in the context of information security (Tipton et al., 2016; Yin et al., 2020). The study highlights how it is possible to establish how PII is being collected without user consent.

Shuba and Markopoulou (2020) shed light on the perceived risks to contemporary mobile users and the extent of personally identifiable information (PII) exposure, including destination server,

encryption level and app functionality. The study acknowledges the extent to which the mobile applications breach the data privacy policies by collecting data and using it in numerous ways. It also identifies the different attitudes that people have regarding their online privacy; however, the study does not offer solutions to prevent data breaches. The themes emerging from Shuba and Markopoulou (2020) relevant to this study were how mobile users could be alerted when malicious attackers were targeting private data. This focuses on the "integrity" aspect of the C.I.A. triangle.

There are several security and privacy concerns related to users' shared information, particularly when users upload personal content such as images, videos and audios. The attacker may misuse shared information. If children are targeted, the risks increase significantly. A study by Li and Yang (2020) provides a comprehensive analysis of various privacy and security risks. The study extensively analyses the threats to online privacy that only involve the social media, and it reiterates existing solutions, such as how each social media account should have its own unique and strong password, especially if using a strong password manager. The research left a gap needing to be filled, since the other internet platforms apart from social networks were omitted. Additionally, the research did not offer novel solutions or ways of improving the effectiveness of the existing ones which have failed to adequately protect users, thus social network users would still be exposed to attacks. According to the themes that emerged from Li and Yang (2020), users need to be properly educated about privacy. For this reason, the recommendations for protecting mobile users against violations by third-party applications constitute the main emphasis of this study.

A study by Yin et al. (2020) identifies the shortcomings of the CIA framework in dealing with online security, as the current widespread use of the internet has rendered the framework insufficient. The study however leaves a gap, as digital mass surveillance and how this is used to target end users are not specified under the new CACA theory provided by the author.

The need for information security is critical, as so many people rely on networks and communication. Kumar and Gupta (2022) explore information security's use of confidentiality, integrity and availability (CIA). The issues and needs related to information security are the main topics of their study, especially the security needs of the people that use the internet, because of the challenges of keeping information from being used by individuals. They show how the CIA framework could be used to address the security needs of people using mobile applications. However, there is no focus on the privacy and security of users when using third-party applications and they fail to give recommendations on safeguarding the users. This is why the primary focus of

this study was on recommendations for safeguarding mobile users against violations by third-party applications.

A study by Wong et al. (2019) examined how businesses might stop insider threats to the integrity of information sharing and the human factors that led to information leakage. The authors focused on how human factors contributed to the data breaches and gave practical solutions for doing away with such breaches, thus ensuring effective data privacy. This study left many gaps, as eliminating the human factor in data breaches would not solve the problem the main causes such as third-party applications would still cause data breaches.

A framework for classifying the many value orientations that adopting firms might get from the big data paradigm (Patel, 2021) was based on the discovery of eleven distinct value directions, which are divided into five dimensions: informational, transactional, strategic, transformational and infrastructure value. This research focused on the potential benefits of the big data technology and not on the ways in which big data could contribute to data security. With big data used in organisations, data security can be guaranteed through easy detection of anomalies, predictive analysis and other forms of analysis that would enable detection of threats and mitigate data breaches. The study left out the essential aspect of utilising the technology for data security.

Phishing is a highly effective cybercrime technique that enables perpetrators to deceive victims and steal vital data. A study by Alkhalil et al. (2021) looked at the state of phishing today and evaluated phishing techniques used to examine phishing attacks. Phishing attempts have been classified solely on basic phishing strategies and defences, with little consideration given to the importance of the entire phishing lifecycle. This study offers a new and comprehensive anatomy of phishing, including attack phases, attacker categories, vulnerabilities, threats, targets, attack media and attacking techniques. The authors' sole focus is on the different mechanisms that the attackers use in phishing and what the attackers target to acquire. They also offer numerous solutions to prevent phishing such as implement multi-factor authentication a crucial extra layer of security. However, it would have been better to explore effective ways in which phishing could be prevented. This would allow the early detection of threats and give solutions that the internet users could use after detection to prevent loss of data to malicious attackers.

Hatamian, Serna and Rannenberg (2019) emphasise that consumers find it challenging to evaluate the privacy features of applications and make educated privacy decisions while downloading apps,

since smartphone ecosystems lack privacy indications. The research highlights the importance of privacy information about apps in users' decisions to use apps. According to Ebrahimi and Mahmoud (2022), mobile app review summarisation (MARS) can determine the threats through reviews from the users and can categorise apps using their privacy scores. This is essential, as the online users prefer apps that they deem as secure and respecting their privacy. However, the research was incomplete, as it did not show how the users could measure an application's privacy situation using MARS.

Users affected by data breaches are highly vulnerable to identity theft. A study by Ablon et al. (2016) found that many customers chose not to take precautionary action following a corporation's notification of a data breach. However, Zou et al. (2019) demonstrate that information on how to use the available knowledge on the impending attack to alert the online user to apply the available means to protect the data is still unavailable, and thus the mobile user does not receive real-time warnings on the attacks that are about to occur despite accurate threat detection.

Shuba and Markopoulou (2020) show how threats to data breaches by third-party apps can be automatically detected. The detection is effective, as it classifies the request by these apps as either legal or malicious and therefore the user has adequate knowledge to make decisions on the sites to use. Alkhalil et al. (2021) analyse phishing from numerous perspectives. First it identifies the risks of phishing, the multiple mechanisms that the attackers use, the type of information that the attackers target and how such information would be used, thus proving the detrimental effects on the victims. Still, the gap related to how such information could be used to ensure that the mobile users or organisations are alerted prior to the attack so that it can be prevented, remains. As a result, the recommendations for protecting mobile users against violations by third-party applications were the primary focus of this study; this will help to raise awareness and promote safe online behaviour among users.

The globe is producing an unprecedented volume of digital data, which is more vulnerable than ever because it communicates nearly every element of existence (Baddar, 2017). Yahoo's catastrophic 3 billion account breaches were exposed to the massive security breaches (Bhadouria, 2022). In this regard, Baddar (2017) emphasized the necessity of backing up your data and how it can play a vital role in limiting the impact of third-party app violations, such as data breaches, loss, or corruption. Alkhalil et al. (2021) review phishing using different perspectives; among the strategies proposed

by the study to prevent phishing are increasing the knowledge of people on phishing and identifying and blacklisting the malicious sites.

Despite the numerous strategies that have been implemented, there is still a high rate of phishing. This proves how necessary it is for new research to focus on improving the efficiency of these methods or to develop new methods of dealing with phishing. Based on the findings of this study, a series of recommendations has been crafted to help protect mobile data users against third-party app violations in the first place, rather than merely reacting to them after the fact, when it is too late.

2.10. CONCLUSION

The goal of this literature review section was to offer some recommendations for improving the overall security of the users when interacting with third-party apps. Furthermore, this literature review was conducted to identify the privacy frameworks and models that could provide a structure for recommendations on safeguarding the mobile user against violations by third-party apps. Chapter 3 presents a systematic methodology based on the literature review in this chapter.

CHAPTER 3
METHODOLOGY

3.1. INTRODUCTION

This chapter presents the research methodology which is the entirety of the methods and procedures used in the study. The chapter starts off by grounding itself in what constitutes research and briefly describing the types of research and their functionality. Then it looks at the difference between research methodology and research methods, followed by a discussion of research methods in cybersecurity. While presenting all the above concepts, this dissertation explains how they have shaped the study.

3.2. RESEARCH

Research is defined as the creation of new knowledge and/or the use of existing knowledge in a new and creative way to generate new concepts, methodologies and understandings (Song, 2021). Research is the process undertaken within a framework of philosophies and/or research approaches, using procedures, methods and techniques that have been tested for their validity and reliability. It is designed to be unbiased and objective. However, the criteria and fulfilment of this process are discipline dependent.

In research, data are collected, analysed and transformed into information prior to providing answers to questions and suggesting decisions. Research needs to be controlled, logically and systematically valid and verifiable. Research draws conclusions based upon hard evidence gathered from data collected from real life experiences or observations (empirical).

The application of research is classified into two main categories (Fomunyam, 2020), namely:

(i). Pure research – it is research conducted to develop, test and validate theories and hypotheses that may or may not have practical application. It is more exploratory in nature.

(ii). Applied research – it is research conducted to solve a specific problem or answer practical questions that could lead to practical solutions for policy formulation or product development. It is mainly descriptive in nature.

The exploratory or descriptive nature of research referred to above describes the type of research, which comprises four categories: descriptive, exploratory, explanatory and correlational.

(i). Descriptive research explains a situation, problem, occurrence, service or programme in a methodical manner and provides information about the researched environment or population.

(ii). Correlational research seeks to uncover or develop a relationship or dependency between two or more features of a situation.

(iii). Explanatory research seeks to determine why and how two or more features of a situation or phenomenon are related.

(iv). Exploratory research is conducted to investigate an unknown domain or to determine the feasibility of researching a specific topic.

The mode of finding answers to research questions or fulfil the research objectives is either quantitative or qualitative (Fomunyam, 2020; Taherdoost, 2021; Thomas, 2021). Quantitative research uses a structured approach to inquiry, to determine the extent of a problem by quantifying it, while qualitative research uses an unstructured approach to explore the nature of a problem without quantifying it. However, some of the research challenges demand both a structured and unstructured approach, using a combination of quantitative and qualitative research. The latter is known as mixed method research.

3.3. RESEARCH METHODOLOGY AND RESEARCH METHODS

There is a distinct difference between research methodology and research methods. The Merriam-Webster dictionary defines methodology as a body of methods, rules and postulates employed by a discipline or a particular procedure or set of procedures, while a method is a procedure or process for attaining an object or a procedure followed in achieving the objective.

Research methodology is a systematic way to solve a problem and research methods are the various procedures, schemes, algorithms, etc., used in research to find solutions (Song, 2021; Thomas, 2021). All the methods used by a researcher during a research study are termed research methods. Research methods serve to collect samples, gather data and find a solution to a problem (Fomunyam, 2020; Taherdoost, 2021; Thomas, 2021).

3.3.1. Qualitative methods

Qualitative research focuses on obtaining data through open-ended and conversational communication such as interviews and focus groups. Qualitative research methods usually collect data at the site where the participants are experiencing issues or research problems, yielding real-

time data. In the main, qualitative methods are used by researchers that conduct exploratory research with the school of thought being interpretivism and/or constructivism.

Interpretivism assumes that reality is subjective, multiple and socially constructed, meaning questioning and observation are practical ways of obtaining findings. Interpretivist epistemology is the study of the interconnection between what is investigated and who or what is investigated. Due to the inclination towards relativist ontology and subjective epistemology, interpretivism views humans as inseparable from knowledge (Junjie & Yingxin, 2022). Interpretivism that emphasises the cognitive orientation is inclined towards constructivist ontology. It implies that humans drive processes and interaction within non-natural social structures (Alharahsheh & Pius, 2020). Interpretivism uses narrative data to extract the truth and gain knowledge depending on different reality lenses. It relies on the individual's communication-based experiences (i.e., voice, standpoint, experience, thoughts and feelings). The communication-based experiences could be gathered through research techniques illustrated in Figure 3.1.

Figure 3.1: Types of qualitative research
Source: https://www.questionpro.com/

Figure 3.1 illustrates the types of qualitative methods, namely:

- Interviews – are conversational methods that are carried out with one respondent at a time either face to face (which enables the researcher to also observe gestures) or via a phone call. It uses follow-up questions to help gather precise information.

- Focus groups – like interviews they include participants but in a group format (i.e., 5 to 10 people), not on a one-to-one basis. The group discussions produce the data to be collected. The data could be collected either physically or online.

- Ethnographic research – uses in-depth observational methods to study targeted audiences in their natural environments. It is a time-consuming method and solely depends on the researcher's expertise to analyse, observe and infer the data.

- Case study research – uses an entity as a research area and data collection methods that are bound within the research area. It then uses data inference to make conclusions related to other areas.

- Record keeping – makes use of the already existing reliable documents and similar sources of information. Systematic literature reviews are part of such methods.

- Process of observation – uses subjective methodologies to gather systematic data provided through five major sensory organs. It uses characteristics as data input instead of measurements made through numbers.

3.3.2. Quantitative methods

Quantitative research methods employ systematic gathering and analysis of numeric data to make decisions about the research problem. In the main, quantitative methods are used by researchers that conduct deductive logic and confirmatory research with the school of thought being positivism.

Positivism is aligned with the hypothetico-deductive model of science, meaning that it uses a circular process that begins with theory from the literature to (i) build testable hypotheses, (ii) design an experiment through operationalising variables (i.e., identifying variables to manipulate and measure through group assignments), and (iii) conduct an empirical study based on experimentation. The findings from the experimentation which is an empirical data collection and analysis stage can help strengthen or refine the theory.

According to Park, Konge and Artino (2020), the philosophical foundations of the positivist paradigm are anchored in:

- Understanding the nature of reality (ontology)

- Describing and understanding the nature of knowledge (epistemology)

- Understanding the values of the research process (axiology)
- Understanding the nature of reality known as ontology
- Understanding the process of conducting scientific investigation (methodology)
- Determining the criteria for evaluating quality of research (rigour).

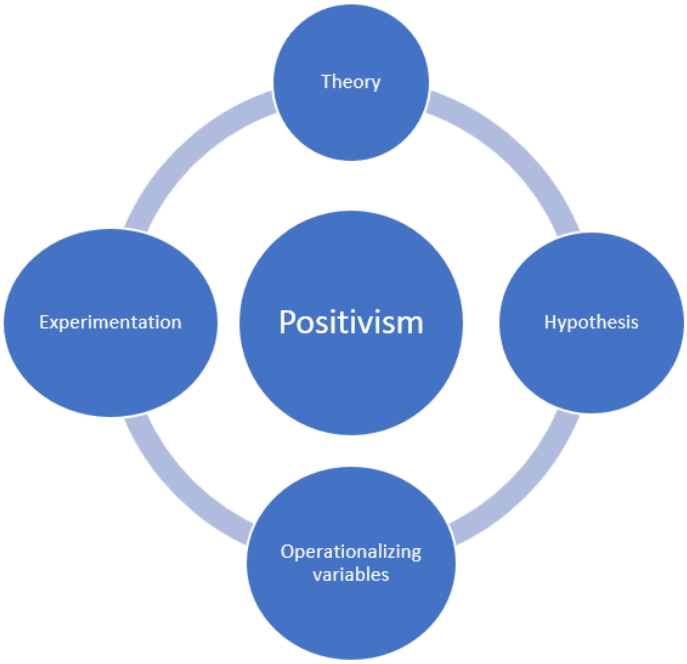

Figure 3.2: The positivism hypothetico-deductive model
Source: Alharahsheh, 2020

Figure 3.2 could be further expanded to illustrate the steps that a research study like the one documented through this dissertation could take. The positivism steps are known as scientific methods (see Figure 3.3). Positivism is a paradigm that relies on measurement and reasoning as well as knowledge that is quantifiable. Positivism attempts to derive and prove universal rules and the way they function (Junjie & Yingxin, 2022).

Positivist knowledge evolves from observations; the researcher asks questions and then thinks of a possible solution that is set as a hypothesis which is then investigated to obtain a conclusion which results in solving the observed problem.

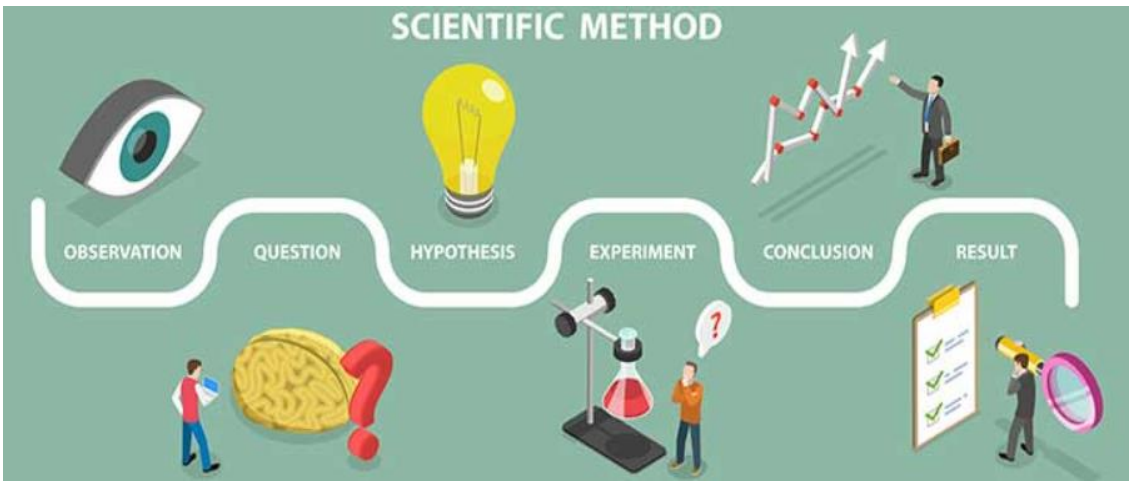

Figure 3.3: The scientific method through a positivism lens
Source: Nickerson, 2023

Quantitative methods are characterised by structured tools, sample size, closed-ended questions, prior studies, quantitative data, generalisation of results, etc. There are two categories of quantitative research methods:

(i). Those that focuses on collecting data directly (primary quantitative methods)

(ii). Those depending on data collected from previously done research or existing information (secondary quantitative methods).

A. Primary quantitative

According to Taherdoost (2021), a primary quantitative research design consists of:

(i). Techniques and types of studies

- Survey research – in quantitative methods data are collected through polls or surveys. The measurement scales could be nominal, ordinal, interval or ratio based.
    - Polls—either election polls or exit polls—are a method to collect feedback using close-ended questions (mainly multiple-choice) from a large sample size.
    - Surveys are used for collecting data from a pre-defined group of respondents.
- Correlational research – is conducted to establish a relationship between two closely-knit entities, how one impacts the other and what changes are eventually observed. Mathematical and statistical analyses are used in this type of quantitative research.
- Causal-comparative research – is also known as quasi-experimental research. It determines the cause-effect equation between one independent variable and other independent variable(s). Causal-comparative research is not restricted to the statistical analysis of two

variables but extends to analysing how various variables or groups respond to the influence of the same changes.

- Experimental research – uses one or more theories that determine the before and after thinking plan. It proves or disproves the research problem statement by using techniques to test the environment without altering it and then alter it to see if different findings could be obtained. Theory could be verified or refuted, in which case it could be enhanced, or a new theory could be constructed.

(ii). Data collection and analysis techniques

- The following techniques are used in disseminating the quantitative tools for collecting data: survey, email, buy respondents, embed survey in a website, social distribution, quick response (QR) code, short message service (SMS) survey and offline survey app.

- To analyse the collected data, quantitative methods use statistical analysis techniques, such as strengths, weaknesses, opportunities and threats analysis (SWOT), conjoint, cross-tabulation, totally unduplicated reach and frequency (TURF) and inferential statistics techniques (confidence interval, the margin of error, etc.). It should be noted that cross-tabulation establishes relationships, patterns and trends within the various parameters of the study.

- There are two main sampling methods for data collection in quantitative research:

    - Probability – participants of a sample are chosen by random selection processes, of which there are four main types:
        a) **Simple random sampling –** used where the population is large
        b) **Stratified random sampling** – used where the population is large and divided into groups known as strata which do not overlap
        c) **Cluster sampling –** used where the population is divided into clusters or segmentations
        d) **Systematic sampling –** used where the starting point of the sample is chosen randomly, and all the other elements are chosen using an interval calculated by dividing the population size by the target sample size.
    - Non-probability sampling – in this case the researcher's knowledge and experience are used to create samples but there may be difficulties in handling biasedness. There are at least five main types of such sampling:

a) **Convenience sampling –** participants are selected based on their proximity to the researcher
b) **Consecutive sampling –**involves collecting samples or data in a sequence over a period rather than all at once and may be particularly useful when dealing with dynamic systems or processes where conditions change over time
c) **Quota sampling –** sample selected using the researcher's knowledge of target traits and personalities to form strata
d) **Snowball sampling –** used when participants are difficult to contact and get information from
e) **Judgmental sampling –** samples are created based only on the researcher's experience and research skill.

B. Secondary quantitative

Secondary quantitative research uses existing data that are collected from at least five sources (Taherdoost, 2021): (i) data available on the internet, (ii) government and non-government sources, (iii) public libraries, (iv) educational institutions, and (v) commercial information sources. Secondary quantitative data help to validate, strengthen, prove or disprove the primary data and may be either published or unpublished. A good example of secondary quantitative research is a systematic review which uses data from research databases (Kowalczyk & Truluck, 2013; Malele, 2023).

3.3.3. Mixed methods

Mixed methods research is a "procedure that enables the collecting, analysing and integrating of data from both quantitative and qualitative methods in a single study or a series of studies to understand a research problem" (HELM Open, 2024). The combination of the qualitative and quantitative methods or the debate involving the two led to a new method better known as mixed methods (Malmqvist et al., 2019; Song, 2021; Thomas, 2021). Mixed method research is a procedure that enables the collecting, analysing and integrating of data from both quantitative and qualitative methods in a single study or a series of studies to understand a research problem (Fomunyam, 2020; Taherdoost, 2021; Thomas, 2021; HELM Open, 2024).

In mixed methods the terms measure and measurement are related to positivism, while communication-based questioning or data collection relates to interpretivism (Gobo, 2023). The adoption of both the positivism and interpretivism paradigms to guide the research study, as was the case in this dissertation, is known as pragmatism.

The mixed methods approach is based on the pragmatist research philosophy. Pragmatism emphasises a diversity of approaches based on the researcher's proposition and the use of research methodology that suits the research problem (Kaushik & Walsh, 2019). It improves the generalisability of qualitative findings and deepens the understanding of quantitative results.

3.4. RESEARCH DESIGN

The research design is the plan or structure for carrying out research. It also specifies the strategies and methods utilised to collect and analyse data (Malmqvist et al., 2019). The research design is determined by the researcher's present understanding of the subject and the objectives for reviewing and interpreting the data. This study was hybrid in nature with mixed methodology and thereby aligned to the pragmatism paradigm. As illustrated in Figure 3.4, this study obtained empirical results through the dissemination and analysis of questionnaires (i.e., positivism) and used a literature review to corroborate the empirical results (i.e., interpretivism), shaping the recommendations for safeguarding mobile users against the violations caused by third party-apps.

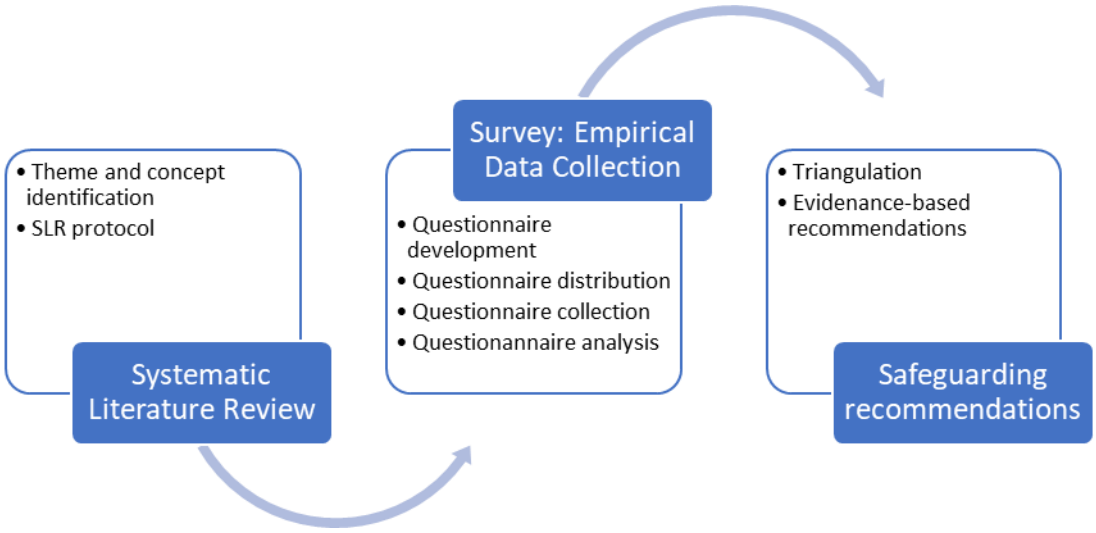

Figure 3.4: Research design adopted in this study
Source: Author

The research design used in this study is depicted in Figure 3.4; it comprised three phases:

- Phase 1: Systematic literature review phase – used for collecting secondary data to explore the concept of digital mass surveillance and how it impacts user privacy

- Phase 2: Survey – used for collecting empirical data through questionnaires and interviews to identify the level of consent provided by users and provide an online behavioural technique to promote awareness of third-party app violations

- Phase 3: Recommendation phase – used to make recommendations based on the data and analysis contributed by Phases 1 and 2.

3.4.1. Systematic literature review

Phase 1 of this study adopted a systematic literature review (SLR) approach for data collection purposes. The SLR considered the elements of document significance, timing, availability and quality of references (Dekkers et al., 2022). It was conducted to determine literature gaps and gain insight into the privacy and security violation issues involving mobile devices. The data-gathering process incorporated two distinct phases of literature investigation. Figure 3.5 illustrates the protocol that was applied to conduct the SLR.

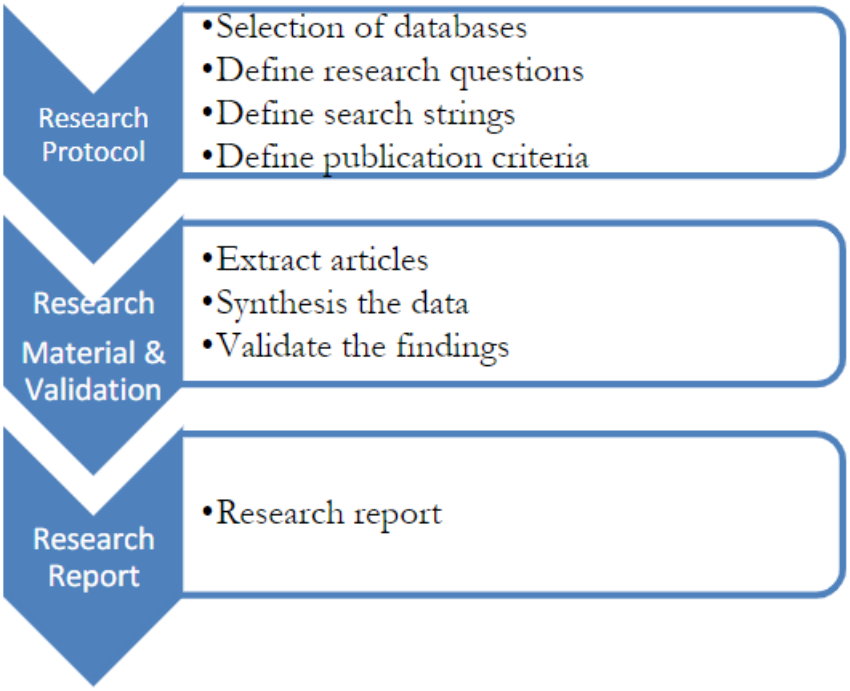

Figure 3.5: The SLR steps followed in this study
Source: Author

A. Selection of databases

To determine the literature gap, a search strategy was guided by research objectives and defined through research questions. Similar studies were identified by consulting different research databases. In this regard, most computing, information security and cyber-security researchers' work could be retrieved from the following digital libraries (Malele, 2023):

- Association for Computing Machinery (ACM)
- Google Scholar

- EBSCOhost
- Institute of Electrical and Electronics Engineers (IEEE) Xplore
- Semantic Scholar
- Scopus.

B. Search strategy/string and search criteria

In this study, the search criterion was set to only focus on English written articles published between 2015 and 2024. The following inclusion search criterion (IC) string was used:

- IC 1 – Cybersecurity AND Awareness AND Mobile device users
- IC 2 – Cybersecurity AND Privacy AND Models AND (violation OR safeguarding*)
- IC 3 – Cybersecurity AND Model AND Violation AND (Mobile users OR Mobile device users*)
- IC 4 – Cybersecurity AND Recommendation AND Violation AND (Mobile users OR Mobile device users*)

To exclude irrelevant articles, the following exclusion criterion (EC) was used to set the boundaries of this SLR method:

- EC 1 – Publication is not written in English
- EC 2 – Publication is not related to cybersecurity awareness and mobile user issues
- EC 3 – Publication that is a duplicate or already retrieved from another database
- EC 4 – Full text of the publication is not available
- EC 5 – Publication not a peer-reviewed paper
- EC 6 – Publication published before 2015.

3.4.2. Survey

A. Sampling method

Populations are typically big; hence, gathering data from each member of a population is difficult. There are different types of sampling methods that could help researchers to generalise their results to the broader population (Faria, 2022). When the complete population is difficult to estimate, a probability sample method known as cluster sampling is used (Faria, 2022).

- In cluster sampling greater risk is based on sample error and analysis complexity; however, the researcher needs to properly control the risk. Since South Africa has a large mobile device user population, a large population of at least 20 000 people was used to calculate the necessary sample size for this study. The population was randomly selected using a researcher's thinking frame that considers students in any South African university (as a cluster) to be at least 1000. If that number is multiplied by 20 universities, at least 20 000 can reflect 20 (out of 26) South African public universities. However, it should be noted that the sample size used in this study was not drawn only from university students but also from professionals and unemployed people, for example.

- Of note is the fact that it was difficult to draw a complete sample from the population of South African mobile users. In this regard, the RAOSOFT sample size calculator was used to determine the sample size of 377 participants of mobile device users, as illustrated in Figure 3.6. A critical part of drawing the sample of mobile device users for this study was to use different clusters that ensured they were chosen at random and appropriately represented the broader population.

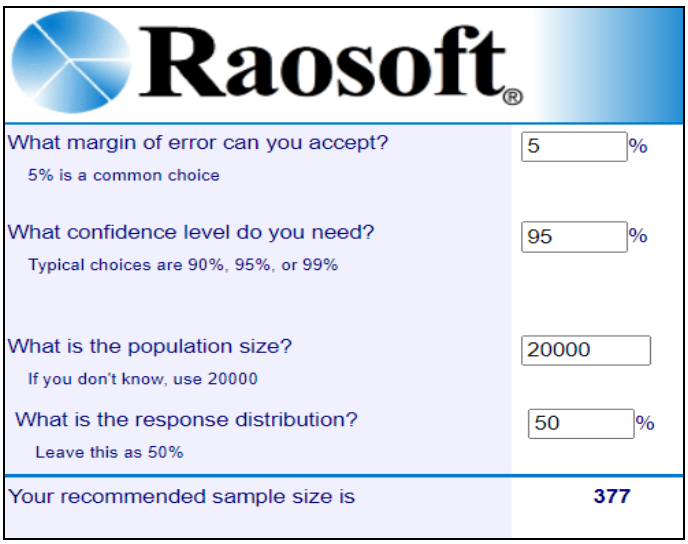

Figure 3.6: The Raosoft sample size
Source: http://www.raosoft.com/samplesize.html

B. Sampling tool

To guarantee scientific rigour and logical coherence, the questionnaire (as a data gathering tool) was developed guided by best practices in survey design and proven methodology. In this regard, different survey studies were consulted, adopted and adapted to suit the aim, objectives and research questions of this study (Fowler, 2019). Furthermore, the design of the questionnaire was influenced by the content of prior research questionnaires that focused on mobile app security and privacy issues (Balapour et al., 2020; Debatin et al., 2009). The questionnaire was designed to collect:

- Participants' age range (which was used to determine and understand the prevalence of cybersecurity and privacy issues among different age groups)
- Cybersecurity and privacy awareness (about digital mass surveillance and third-party app violations)
- Cybersecurity and privacy technical knowledge affecting users' app decision-making process
- Mobile users' concerns about information security and privacy
- Cybersecurity and privacy themes regarding:
    - Confidentiality (types and extent of data routinely collected by third-party apps, types of collected and distributed personal data)
    - Integrity (to identify the level of consent provided by users)
    - Availability (how much of the data are collected beyond the user's consent).

C. Questionnaire

A comprehensive analysis of the body of research on privacy and security issues pertaining to mobile apps was used to develop the questionnaire items. For example, data in Debatin et al. (2009) and Solove (2010) served as inspiration for inquiries about users' knowledge and behaviours. In this study, the questionnaire helped to:

- Establish a baseline understanding of the users' mobile app usage habits related to security and privacy issues
- Determine users' decision-making processes when choosing, downloading and installing mobile apps

- Explore how users navigate app stores, make choices and interact with third-party app installation procedures

- Understand the key aspects in identifying potential vulnerabilities or areas where users may be exposed to security or privacy risks during the app acquisition process (Balapour et al., 2020)

- Focus on gathering data related to users' concerns about information security and privacy when using mobile apps.

In this study the questionnaires were used to collect empirical data and were randomly distributed (both physically and electronically using Qualtrics software) to the total of 400 participants. Of note is that only 8% of the questionnaires (distributed through six clusters) were spoiled and 92 unspoiled, as illustrated in Figure 3.7. The only PII that could reflect on the questionnaire was the age range (20–69 years)—not the actual age—and the participants' gender.

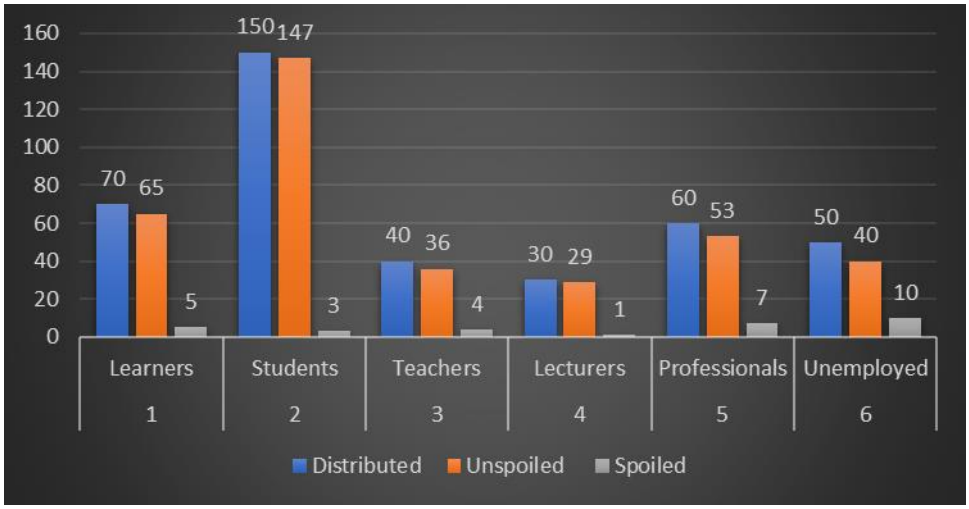

Figure 3.7: Distribution of questionnaire
Source: Author

3.4.3. Recommendations

Pragmatism promotes data triangulation, as it uses multiple data sources to solve a problem. In this regard, this study used the SRL, and survey results shaped the recommendations for safeguarding mobile users against third-party apps. The themes originating from literature (see the first section of Chapter 4) and the corroboration of the empirical data obtained from questionnaire analysis (see the second section of Chapter 4) were used to formulate the recommendations provided in Chapter 5.

3.5. LIMITATIONS

3.5.1. Sample size

The key constraints of this study were due to the quantity of sample members, as a large sample would require more time than the master's level timeframe. In this regard, guidance from other literature sources was adopted, leading to making inferences about the findings.

3.5.2. Questionnaires

Questionnaires are generally suited for collecting structured, quantitative data, as indicated in Appendix A. They may not capture the depth of insight that could be obtained through interviews or open-ended surveys. As a result, certain nuanced aspects of participants' concerns or experiences may have been overlooked. Furthermore, questionnaires are inherently prone to answer bias, which occurs when participants provide socially desired or erroneous information. This bias can influence the reliability of the data collected, as participants may not disclose their true opinions or experiences related to mobile app security and privacy. To counteract this, participants' responses were corroborated with the literature. The choice of a specific sampling method (cluster sampling) and the need to collect data from a diverse range of participants might have posed logistical challenges in terms of data collection and participant recruitment. These challenges could have affected the representativeness of the sample and, consequently, the generalisability of the findings.

3.5.3. Timeframe

The study used a cross-sectional timeframe which covered only 2023 and thus limited the collection and analysis of data to 2023. This potentially excluded later developments or changes in mobile app security and privacy practices; with different technological changes the period from 2024 onwards might have provided new challenges. In this regard, the inference was very important.

3.5.4. Resources

The limited resources, including time and budget, posed challenges to conducting comprehensive research. This restriction affected the extent to which data could be collected, analysed and validated, potentially limiting the study's overall robustness.

3.5.5. Ethical considerations

Considering ethics while performing research was critical for avoiding ethical concerns before and after the research (Faria, 2022). Before this study was conducted, the researcher was enrolled in the online ethics course offered by e-learning TRREE. Furthermore, the university’s ethical clearance and gatekeeping processes were followed. The process ensured that the proposal and questionnaires were scrutinised, and that participants’ consent was obtained before they responded to the

questionnaire. No participant was coerced. Furthermore, except for the average age group and gender, no personal data were collected.

3.5.6. Validity and reliability

In this study the validation method was essential for verifying the research findings' quality, credibility and dependability. The critical aspect of the validation process was to examine whether the measurement tools, such as questionnaires, accurately and consistently measured the theoretical constructs or concepts of interest. Furthermore, the study relied on secondary data provided by literature, meaning that the study inherited the basic research qualities of validity and reliability demonstrated by prior research. This approach ensured the content reliability of the data collection tools by using only double peer-reviewed articles from accredited journals (Barth et al., 2019; Maroufkhani et al., 2019; Hayes et al., 2020).

To promote reliability and validation, the data scrubbing technique was used for data preparation (collection, cleaning and organisation) to verify that the data collected were high quality and error-free. Data scrubbing is the process of identifying data defects and then updating, changing or removing the data to correct them. To achieve the latter, the following actions were taken:

- Remove superfluous information
- Remove duplicates in the data
- Correct structural issues in step three
- Address any missing information
- Remove anomalies from the data
- Verify the information.

3.6. CONCLUSION

The research methodology and tools detailed in this chapter followed a mixed method approach enabling a pragmatic research orientation. Pragmatism strengthened this study by allowing the researcher to use any suitable methods to solve the research problem. The next chapter analyses both the literature review and the empirical data collected in the form of findings. The actual recommendations are presented in Chapter 5.

CHAPTER 4

RESULTS AND FINDINGS

4.1. INTRODUCTION

This chapter presents the findings of the SLR and the survey that was conducted using the data collected through an empirical process. The results indicate that the SLR differed significantly from a mere Google or internet search study as it showed the areas in which third-party apps might violate privacy. It also highlighted areas that could be used to safeguard mobile users. Furthermore, it showed the indicators in some areas that could be used to develop the necessary recommendations for safeguarding mobile device users against violations by the third-party apps sector. The survey concurred with the literature. It revealed how users consented to or did not understand their consent to third-party app violations. It showed their level of cybersecurity awareness of potential violations by third-party apps. Furthermore, it revealed how users felt about security and privacy, especially when affected by the third-party apps sector. The SLR and survey results are presented based on the study's objectives; the summary of indicators used for recommendations is provided towards the end of this chapter.

4.2. TO 1: TO EXPLORE THE CONCEPT OF DIGITAL MASS SURVEILLANCE AND HOW IT IMPACTS USER PRIVACY

Chapter 1 introduced the above theoretical objective. To achieve this objective the SLR was conducted, and the empirical data were collected using the methods highlighted in Chapter 3.

- What is digital mass?
- How does digital mass surveillance impact user privacy?
- How is digital mass surveillance used to target users?
- How does digital mass align to the CIA framework?
- What are the levels of transparency, oversight and accountability in surveillance practices, as well as efforts?
- What indicators could be noted from digital mass surveillance that could assist in developing privacy-enhanced frameworks for safeguarding individual rights in the digital age?

4.2.1. Findings from the SLR

A. Digital mass surveillance

Digital mass surveillance refers to the digital tracing aspect used in the ICT sector. A good example of digital tracing was when different digital tracing strategies were adopted during the COVID-19 period, as illustrated in Figure 4.1.

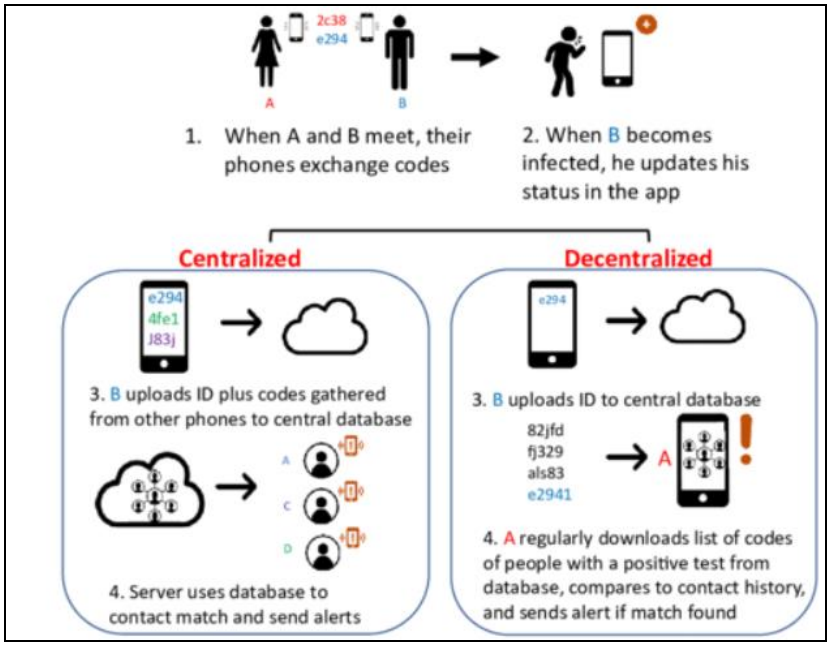

Figure 4.1: Digital contact tracing strategies during COVID-19
Source: Skoll et al., 2020

Figure 4.1 illustrates the digital tracing strategy known as voluntary contact-tracing applications. In this space, apps are subdivided into two categories:

(i) Data are collected in a centralised manner

(ii) Data are collected in a decentralised manner.

For example, when two individuals come into contact their phones exchange anonymised key codes. In this strategy, the comparison of the downloaded codes is used to alert the user about the exposure. Skoll et al. (2020) explain it as follows:

> *"When B becomes infected, he updates his status in the app. In a centralized approach, B uploads both his ID code and all the codes of people he has been in contact with to a central server. The central server, usually run by a public health authority, uses the codes to do contact matching and sends alerts to those exposed to B. In a decentralized approach, B only uploads his ID to the central server and keeps his contact history on his phone. All other phones regularly download codes from the cloud that are uploaded from positive cases."*

The second digital tracing strategy that was introduced during COVID-19 was mandatory centralised mass surveillance. In this strategy, location data to map individuals' movements are used to evaluate any contact with others. Mandatory centralised mass surveillance uses technologies such as QR codes, CCTV footage, facial recognition cameras, location-tracking bracelets and cell phone tower signals (Skoll et al., 2020). During COVID-19 both these strategies of digital tracing were used by many countries.

Digital mass surveillance could be defined as the gathering of diverse data about users based on their digital behaviour (Knoxster, 2017). It can be used to target users online in various ways, leveraging the vast amount of data collected to identify, monitor and potentially influence individuals' online activities. In this regard, in the ICT sector third-party app providers commonly gather a variety of data, including personal details, location data, device details, usage statistics, social media data, in-app purchase records, payment information and even fitness and health data. For example, during account registration or user interactions with the app's features the third-party app commonly gathers individuals' names, phone numbers, email addresses, dates of birth, etc. (Gamage, 2020). Furthermore, there are other ICT sector stakeholders which apply digital mass surveillance through their different online platforms. For example:

- Digital advertisers observe consumer behaviour by monitoring the websites they visit to determine the kinds of goods and services they would find appealing (Mehta et al., 2019). Companies frequently utilise (tracking) cookies to monitor consumers' browsing behaviour, but alternative technologies include flash cookies and device fingerprinting (Schechner, 2019). Researchers have discovered that the 100 most popular sites collect over 6,000 cookies, with 83% being third-party cookies, and that some individual websites gather more than 350 cookies (Seng et al., 2021). These cookies enable businesses to collect extensive information about millions of customers, some of which is used for online behaviour advertising (OBA). To demonstrate the scale of this business, Facebook has 1.65 billion individual profiles (Seng et al., 2021). The advertisements users view on other websites they visit are influenced by the data that are kept. These kinds of digital trackers enable advertisers to target audiences with their advertisements. The data are used by websites such as Amazon for real-time pricing targeting (Mehta et al., 2019). For example, Amazon uses this data to ascertain the price a user is willing to pay, after which it may increase the offer (Mehta et al., 2019).

- Google Analytics is a widely used application for tracking website traffic and identifying top websites. Schechner (2019) criticises Google Analytics for potential privacy and security

concerns due to several reasons, such as tracking user behaviour. Google Analytics tracks user interactions with websites, including page views, clicks, time spent on pages, and more. Furthermore, Google Analytics collects IP addresses, which can be used to identify a user's approximate location. Data can potentially be shared with third parties, depending on how the website owner has configured the service. Google Analytics is part of the broader Google ecosystem and data collected can be combined with other Google services like Google Ads. This integration can lead to more comprehensive user profiles and targeted advertising (Schechner, 2019).

B. Transparency, oversight and accountability in surveillance practices

In surveillance practices how much of the data are collected beyond the user's consent is a question that deals with the transparency, oversight and accountability of surveillance practices, especially of third-party apps. The third-party app providers gather users' data from their interactions with the social media (Reardon et al., 2019). For example, some apps are presently integrated with the platforms of social media, automatically using the apps' undetectable capability to collect data from social media profiles without explicitly asking the user (Reardon et al., 2019). The data could include social connections, content or even the interests of the users that have been shared or liked.

As of the beginning of 2021, global users have had access to nearly six million mobile apps available on the market through the leading app stores, the majority of which not only require additional permissions to function but may also track and collect various types of data for third-party advertisers across multiple websites and other apps (Richter, 2021). While one of the primary goals of tracking is to recommend relevant advertising, the danger of external actors gaining access to sensitive information and distorting the intent of data collecting cannot be ignored. Concerns about consumer privacy emerge because customers are not always aware of the degree of data collecting or how their data are used across many apps. Figure 4.2 below depicts the quantity of personal data acquired across some apps.

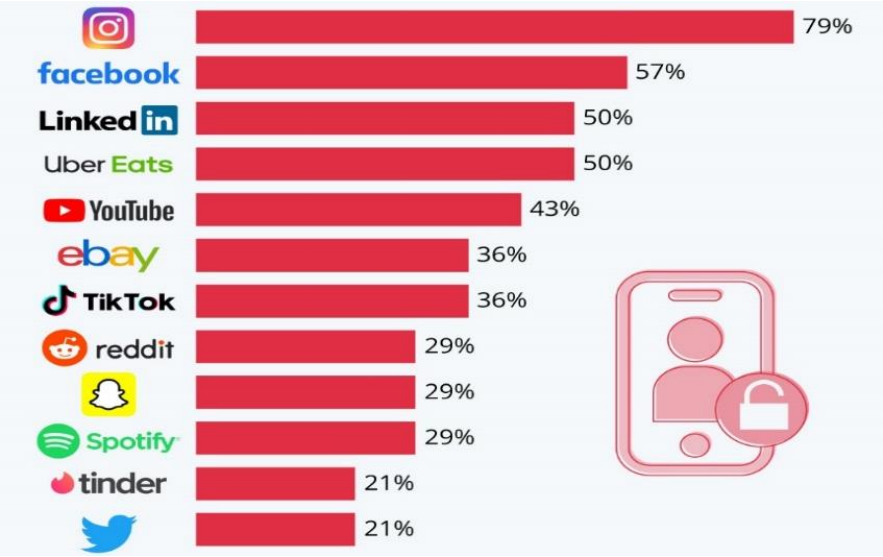

Figure 4.2: Personal data collecting
Source: Richter, 2021

Figure 4.2 illustrates the amount of data collected by third-party selected iOS apps. Facebook was the major culprit, as it scored 79% in collecting private data from users, while Twitter (now X) and Tinder scored the least (21%) without transparency to the user. In fact, Facebook's data collection practices have faced scrutiny and criticism over privacy concerns. Regulations like GDPR in Europe and CCPA in California have prompted Facebook to provide users with more transparency and control over their data, including options to view and download their data or request its deletion (Schechner, 2019). In this regard, as part of governance no organisation provides oversight or accountability. Literature shows that the apps which presently offer in-app purchases or even some type of subscription services might collect the payment information, including the details of credit cards as well as the billing addresses (Sharma & Sahay, 2019). The collected information is commonly handled securely by the payment processors of third-party app providers.

Compared to standard payment methods (e.g., credit cards), transactions with third-party in-app payment are conveniently completed within the mobile app. Users can pay their bills directly without moving to another app or browser. For example, Discovery Bank's Shared-value Banking concept considers individual financial behaviours to determine how financially healthy clients are. Client transactional data are an essential source of information for Discovery Bank's behavioural profiles. Delta Lake enables Discovery Bank to combine diverse data types from several sources, allowing for enhanced behavioural segmentation. This cutting-edge hyper-personalisation method delivers a holistic perspective of clients, going beyond basic demographics to incorporate transactional conduct and purchasing preferences and allowing for a better understanding of their banking habits. Using Databricks, Discovery Bank identifies hundreds of characteristics connected with how customers spend at various frequencies and intervals. To develop detailed indices and

measures, the data are enhanced with a wide range of classifications, including digital; geographic; affluent; environmental, social and governance (ESG); and other aspects. Unfortunately, the information is not made transparent to the user and there is no oversight of or accountability for what could be done with that data. The third-party apps also collect fitness and health data such as sensitive information on the physical activity extent of the users, vital signs and medical conditions (Wells & Spry, 2022). This type of data should be handled extensively and carefully to comply with the regulations of data protection and user privacy (Khatoon et al., 2019). For example, commercial health-related apps are frequently viewed as potentially invasive, with period trackers being popular (Richter, 2021). As of June 2022, mobile female health app Flo had the fewest number of data trackers, with five trackers active on its iOS version and only two trackers for Android users. In comparison, Pregnancy App & Baby Tracker reported 35 mobile trackers for iOS and Android. In the second half of 2022, public concern centred on the likelihood that commercial female health apps and menstrual cycle self-tracking apps might be used to monitor women's reproductive cycles and enforce an abortion ban in the United States.

4.2.2. Findings from the empirical data collection

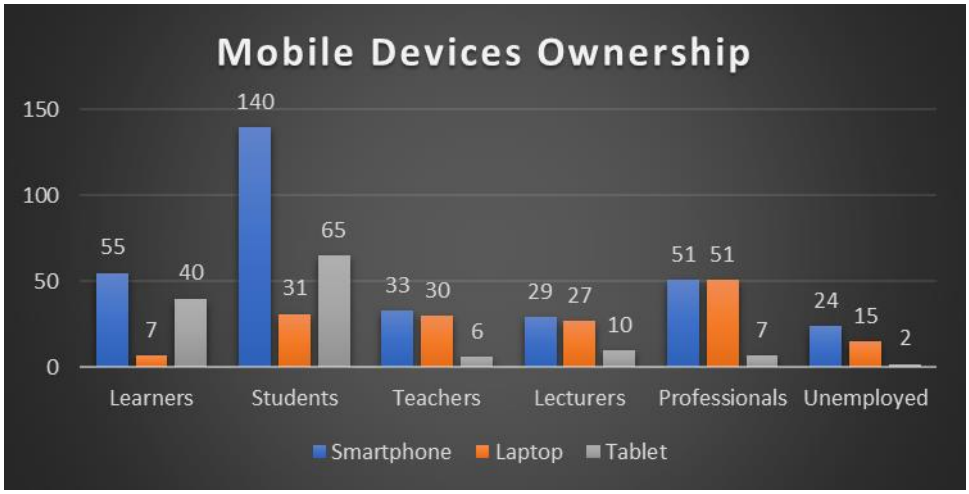

Figure 4.3: Users mobile device ownership.
Source: Author

Figure 4.3 shows that most participants owned or had a smartphone capable of accessing the internet. In fact, of the 370 participants, 332 owned smartphones, 161 owned laptops and 130 owned tablets. Figure 4.3 was not constructed from the sample size subtraction (i.e., boolean “OR”) but from the addition point of view (i.e., boolean “AND”) point of view. It is of note that despite the huge ownership of smartphones, laptops and tablets had their own share based on their affordability and quick access – most people owned all three mobile devices. However, unlike other participants, most learners owned tablets, maybe due to the COVID-19 period that fostered online learning and online platforms.

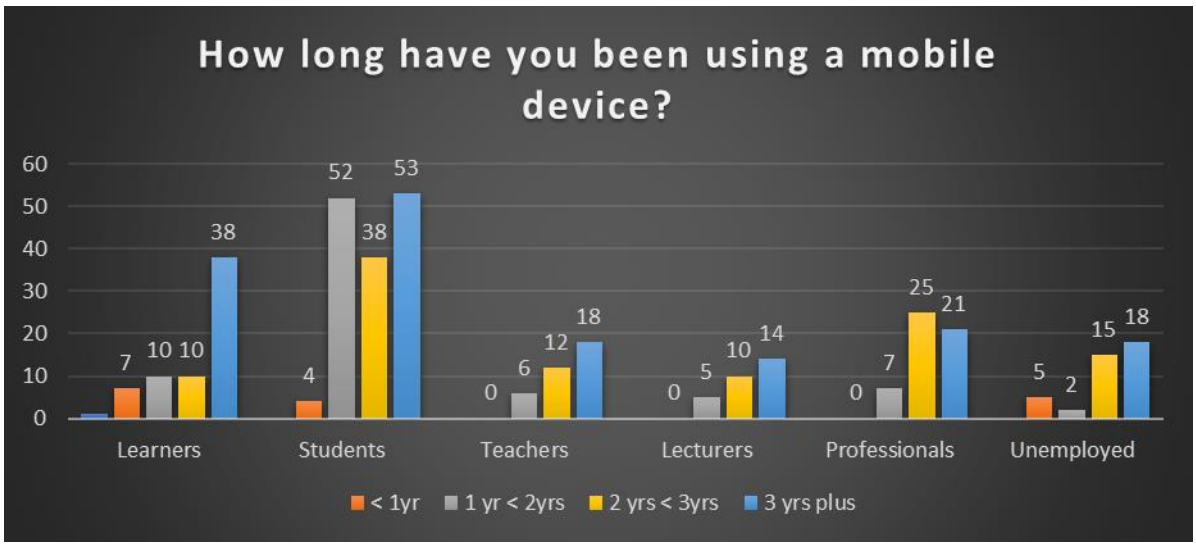

Figure 4.4: Number of years of using a mobile device
Source: Author

Figure 4.4 illustrates that most mobile device users had used their devices for more than two years. In fact, most professionals had been users of such devices for more than three years; this also applies to unemployed individuals. Thus, no matter what the socio-economic status of the participants, almost all of them owned mobile devices and had used them over the years. This means that all the participants in one way or the other had interacted with third-party apps for their education, social interaction and general life needs.

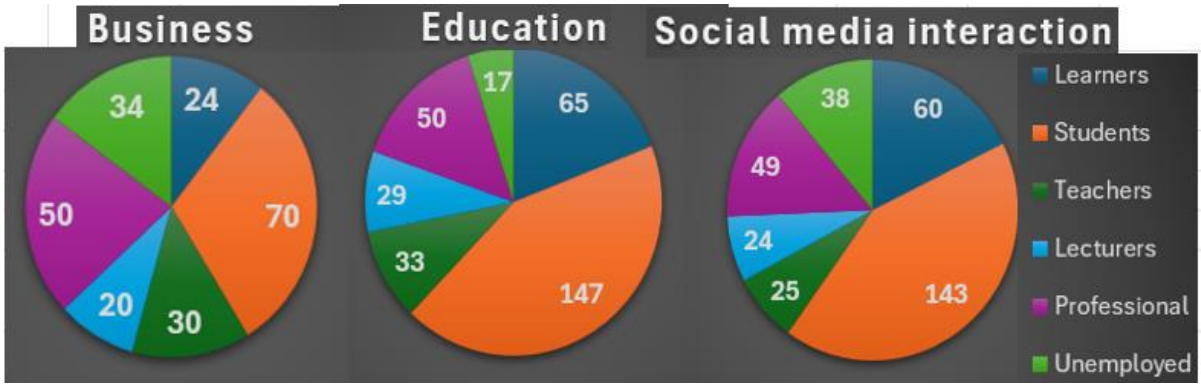

Figure 4.5a: Number of participants accessing third-party apps
Source: Author

Figure 4.5a illustrates that most participants used their mobile devices to access the internet and interact with social media, online businesses and educational platforms or apps. It is of note that all learners and all students used their devices for educational purposes, while few unemployed people used the educational apps, but did use their mobile devices for social media. Considering this, it was deemed proper to assess the participants' knowledge of digital mass surveillance; it was found that very few knew about digital mass surveillance (see Figure 4.5b). Thereafter, their understanding of

digital mass surveillance was also assessed by checking their interaction with digital mass surveillance technologies (Figure 4.5c).

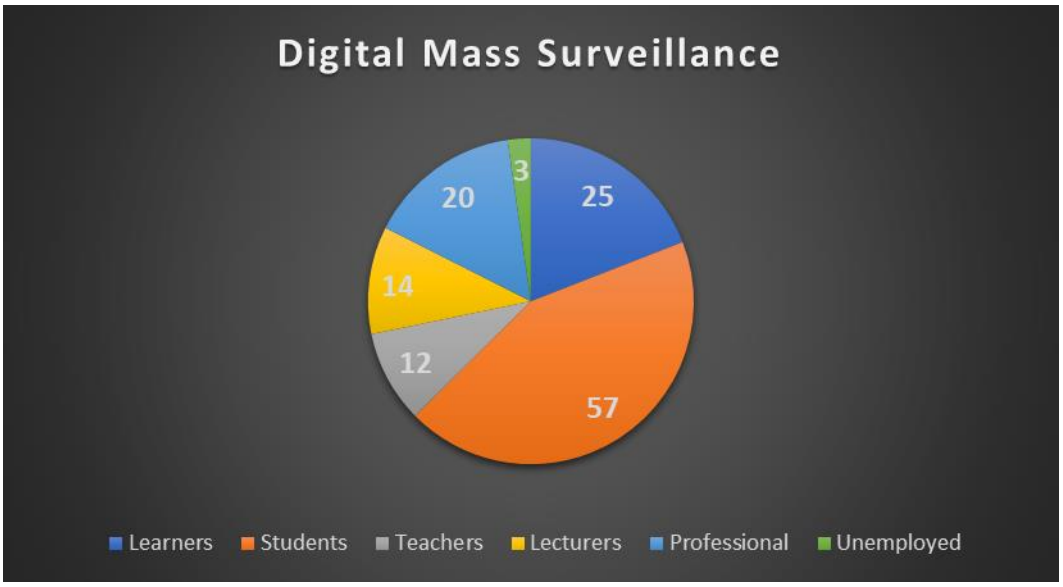

Figure 4.5b: Participants knowing about digital mass surveillance.
Source: Author

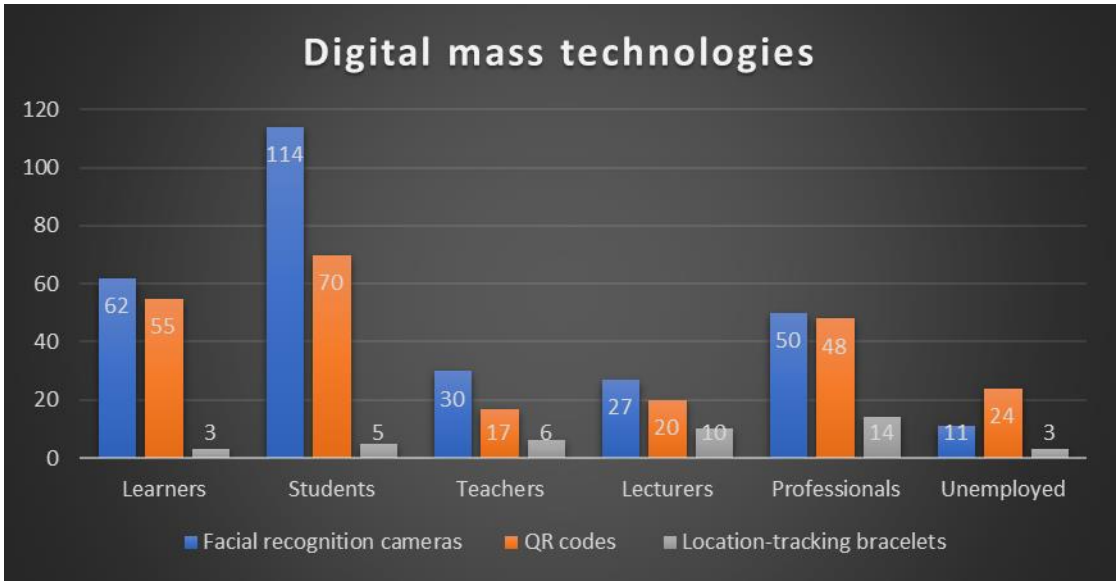

Figure 4.5c: Digital mass technologies
Source: Author

Figure 4.5c illustrates the digital mass technologies that participants were exposed to during their years of owning and using mobile devices. Facial recognition seemed to be the most common technology: almost all participants had interacted with it. Thus, the users' understanding of digital mass surveillance cybersecurity concepts was tested using four indicators (privacy, transparency, oversight and accountability).

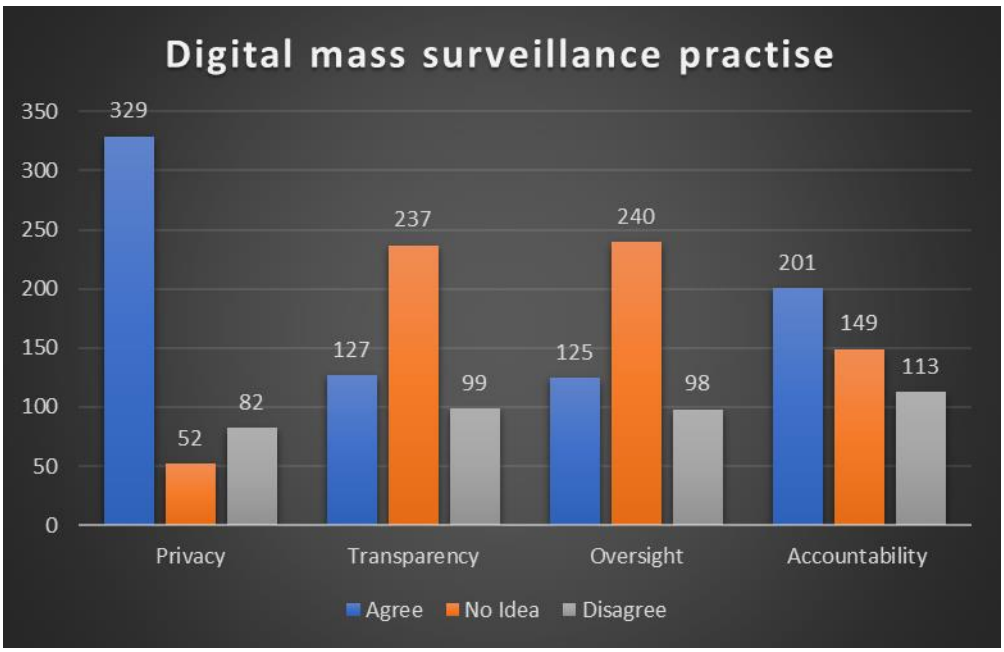

Figure 4.6: Understanding of four digital mass surveillance indicators
Source: Author

Figure 4.6 illustrates the participants' responses to whether they felt that during the digital mass surveillance practice (when their profiles were collected) the third-party organisation provided privacy, transparency, oversight and/or accountability. Most participants thought that during digital mass surveillance privacy was highly protected and further questions (which are shared in the next sections of this chapter) revealed that literature was correct in stating that most individuals did not know what happened to the profiles' data (Huckvale et al., 2019; Gamage, 2020). Furthermore, most participants were unaware of transparency and oversight during digital mass surveillance, while they felt that during the digital mass surveillance the third-party apps had some form of accountability.

4.2.3. Themes relating to TO1

Digital mass surveillance involving third-party apps raises several key themes, reflecting the various implications and concerns associated with the pervasive collection and monitoring of data. Understanding these themes is crucial for developing strategies to protect privacy, ensure security, and address ethical considerations. Here's an overview of the prominent themes that emerge from the concept of digital mass surveillance in the context of third-party apps:

- Privacy Invasion: Third-party apps may engage in extensive monitoring of user activities, communications, and personal data without explicit consent.

- Lack of Informed Consent: Users may not be fully aware of or understand the extent of data collection and monitoring by third-party apps.

- Data Profiling: Aggregated data can be used to create detailed user profiles, potentially leading to targeted advertising or behavioural manipulation.

4.3. TO 2: TO IDENTIFY THE TYPES AND EXTENT OF DATA ROUTINELY COLLECTED BY THIRD-PARTY APPS AS WELL AS THE LEVEL OF CONSENT PROVIDED BY USERS FOR SUCH DATA

The previous section (4.2) pointed out that some of the data collected by third-party apps were the profiles of those users that registered to use the third-party apps. Furthermore, empirical evidence collected from different clusters showed that most people did not know of their profiles being collected by third-party apps, especially during digital mass surveillance.

Theoretical objective 2 was presented in Chapter 1. It aimed to identify the types of data collected by third-party apps and the frequency with which it was collected. In this regard, the following questions assisted in achieving the objective:

- What kind of data is collected by third-party apps? And why is it frequently collected?
- What is the quantity and extent of data typically gathered by third-party apps?
- How much does the user understand about the information that has been gathered?
- Do users understand why third-party app organisations collect their data? Do users consent to such data collection?

To achieve this objective the SLR was conducted, and the empirical data were collected using the methods highlighted in Chapter 3. The results are presented in the section below.

4.3.1. Findings from the SLR

In this era, mobile devices are widely used around the world. Mobile devices' popularity is rapidly expanding, opening more business possibilities for more mobile platforms and apps. Mobile app development has become a thriving industry and the use of artificial intelligence (AI) in mobile apps has expanded their popularity (Turner, 2021).

In 2021, there were approximately 7.34 billion mobile device users which significantly increased the need for mobile services (Wamba et al., 2015; Turner, 2021). This increase has accelerated mobile device users' app download and app utilisation for purchasing services and products for

their daily living (Furletti et al., 2017). The interaction of mobile device users with the apps has resulted in personal identifiable information (PII) and profiling of users.

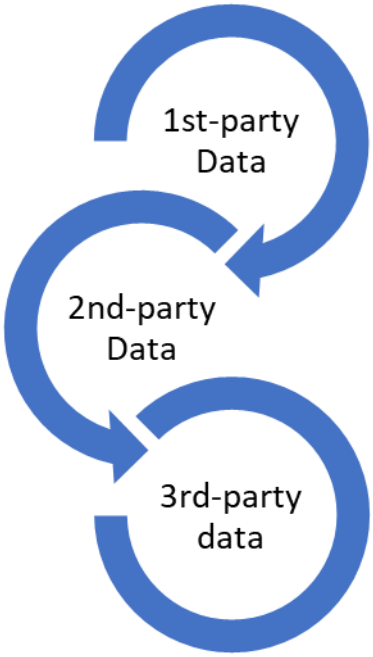

Figure 4.7: Sources of obtainable PII
Source: Garg et al., 2021

Figure 4.7 illustrates that in the field of data engineering and business management, the PII comprises at least three categories, namely:

- First-party data – refers to the users' transactional and interactional consented information from different systems, such as customer relationship management (CRM) systems, point of sale systems, websites, online shopping, apps, internet of things, etc.

- Second-party data – refers to the first party data from another organisation or business entity easily deployed to augment the internal dataset of the organisation seeking the data; for example, second-party data that come from the other stakeholders and partners that share a similar supply chain or consumer line database.

- Third-party data – refers to the datasets that the current organisation collects from first and/or second party datasets and manages for itself without ownership. It is the dataset that is drawn from a range of sources about the user of interest. Third-party data can include datasets that are "stitched" together from a wide variety of sources or even come from governmental, non-profit or academic sources. Weather data and public demographic data can be examples of third-party data. Third-party data are often shared, bought and sold on data marketplaces/exchanges.

Clearly almost all datasets are important in data engineering. Literature points to the fact that the issues regarding PII as acquired by third-party agencies go beyond what is specified in the privacy and security policy and this phenomenon has gradually become more pronounced (Moreno et al., 2016). This means the growing user numbers lead to the growth, collection and capturing of PII data, stored in large amounts through mobile apps (Moreno et al., 2016; Trabucchi et al., 2017). For example, users habitually complain about getting calls from organisations trying to sell them what they previously searched for, as this is the result of stolen or misused PII collected by mobile apps (Wijesekera et al., 2015).

Currently various types of apps are being released by third-party developers for those who use the apps to improve their daily tasks. Mobile apps are becoming an integral part of people's daily lives (Gordon et al., 2020). With increasing dependence on apps, the stakeholders for whom the data are of greatest value are the app providers, advertisers and researchers. Through the analysis of user data, the app providers could easily gain insight into the users' preferences and behaviour (Talal et al., 2019).

Unfortunately, the SLR of the user level of understanding and consent about the type and extent of data routinely collected by third-party apps did not result in many articles, pointing to a gap in the literature that this study seeks to help fill. Some researchers (Taherdoost, 2012; Wijesekera et al., 2015; Moreno et al., 2016; Tipton et al., 2016; Trabucchi et al., 2017; Yin et al., 2020) state that mobile device users feel that:

- Although they use the apps, their confidentiality levels are very low when coming to the misuse of their data (confidentiality)
- Their PII is not protected by third-party apps; hence, there is no integrity in how apps deal with their PII (integrity)
- Their PII could be sold to the highest bidder, so their PII is available to anyone who wants to use it (availability).

4.3.2. Findings from the empirical data collection

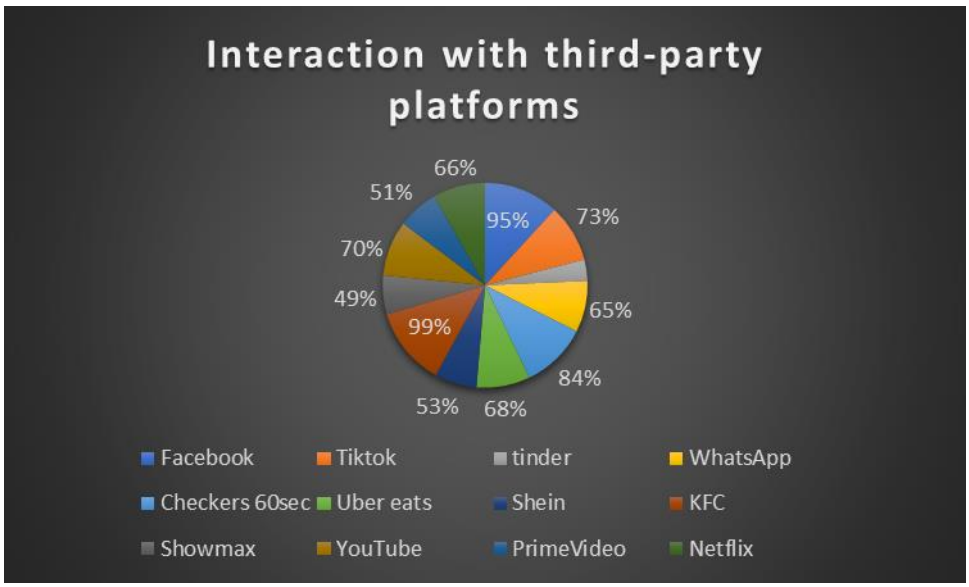

Figure 4.8a: Users' response to third-party app profiling
Source: Author

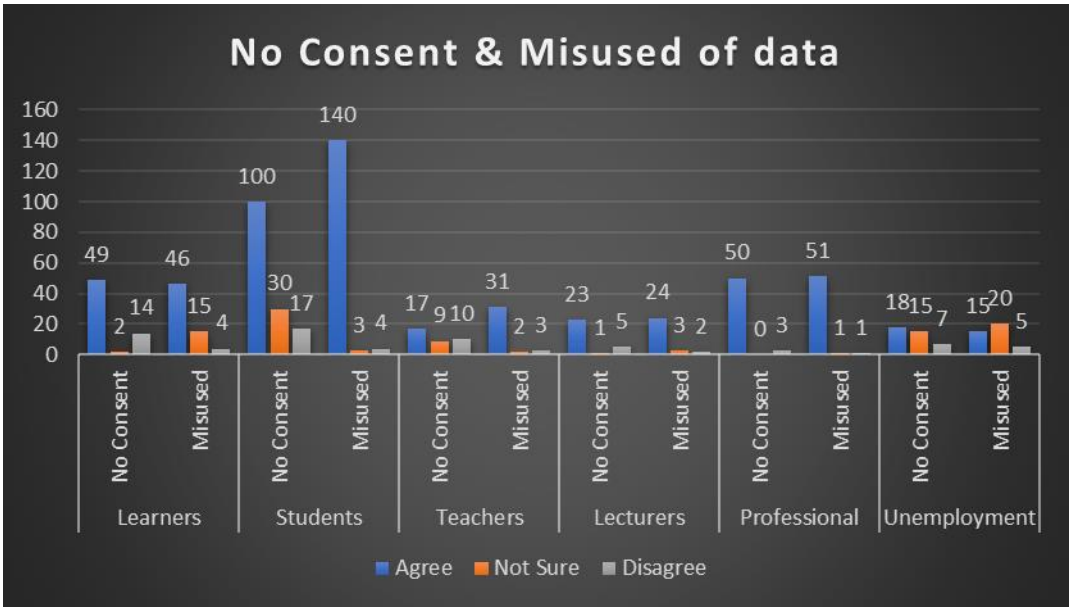

Figure 4.8b: Consent and misuse of PII data
Source: Author

Figure 4.8a shows that most participants felt that their third-party apps profiled them when they interacted with their platforms. These platforms were social media, supermarkets, food and clothing platforms. Figure 4.8b shows that most participants felt that their third-party apps used their data without consent and that they misused such data. Unfortunately, most of the unemployed participants did not seem to bother or did not really know about their PII in the third-party apps.

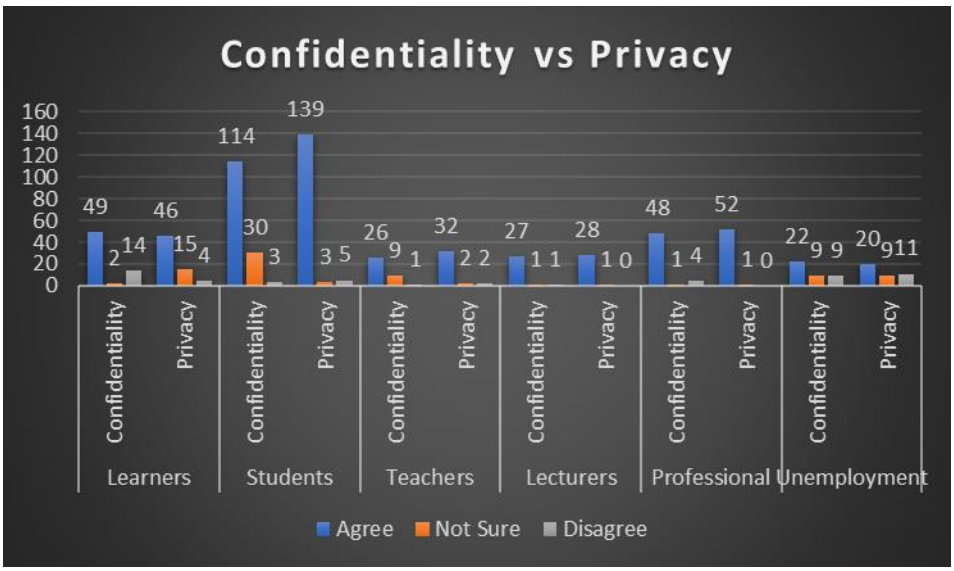

Figure 4.9a: Confidentiality vs privacy
Source: Author

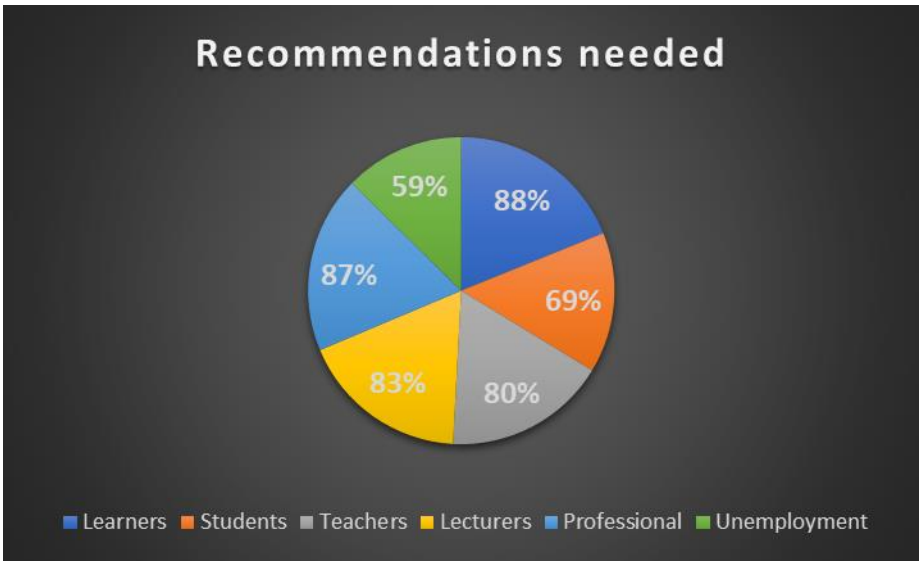

Figure 4.9b: The need to safeguard users against violations by third-party apps
Source: Author

Figure 4.9a shows that most participants felt that the third-party apps violated their confidentiality (i.e., concern) and privacy (concerns people). The latter called for checking the level of security and privacy awareness of participants, as presented in Section 4.4. In this regard, most participate felt that they needed to be safeguarded against the third-party apps, as illustrated by Figure 4.9b.

4.3.3. Themes relating to TO2

When third-party apps are involved in violations, several recurring themes and issues emerge. These themes highlight various aspects of security, privacy, and operational concerns that can arise from such violations. Understanding these themes can help in developing better safeguards and

frameworks to protect users and their data. Here's an overview of common themes from theoretical objective:

- Data Privacy Breaches: Unauthorized access to sensitive personal information, such as contact details, financial information, and usage patterns.
- User Consent and Control: Insufficient information provided to users about how their data is collected, used, and shared.
- User Education and Awareness: Insufficient user knowledge about security best practices and potential risks associated with third-party apps.

4.4. EO: THE BEHAVIOURAL CHANGE TECHNIQUE TO PROMOTE AWARENESS OF THIRD-PARTY APP VIOLATIONS

4.4.1. Findings from the SLR

A. Users' behaviour towards third-party apps

No-one can deny the importance of mobile devices (i.e., smartphones, wearable smart devices, etc.) and third-party apps in today's world. Lives have been made much easier by mobile devices and apps in the prevailing digital environment. Smartphone users can install third-party apps through the mobile app marketplace ecosystem, most of which require permission from the user to obtain access on the user device to networks, contacts, device state, call logs, location, phone gallery and camera (Felt et al., 2011). To safeguard sensitive user data and stop privacy breaches, most contemporary smartphones adopt the permission-based paradigm (Reardon et al., 2019). Permissions may be necessary when connecting with the system application programming interface (API), databases or message-passing system (Reardon et al., 2019).

The public API describes 8648 methods, some of which are protected by permissions (Seng et al., 2021). If a third-party app wants to access resources or user information, it will request permission from the user. The developer must define the application's permissions by specifying them in the patent file and demanding that the user approves them at runtime. When an app requests significant data from a user or device, developers must design a valid privacy policy. The inclusion of a privacy policy in the app comprehensively outlines how the app can gather, use and share data, including the types of third-party apps and who will receive it. But in the end, it is the user's sole

responsibility to decide whether to allow an app that requests specific permissions on his or her device.

Most apps on the market request data that are irrelevant to the app's main feature, which could result in the leakage of private information or inefficient use of mobile resources. This situation is particularly concerning regarding those with low literacy who cannot make their own decisions about the legality of apps. Even among literate smartphone users, the majority ignore privacy permissions when installing programmes on their devices. In this way users become victims of data theft, which can lead to more significant concerns for them (Kovacs, 2021).

The fundamental issue is that most users do not read or comprehend the purpose of the permissions asked by the apps they install, allowing programmes to gain illegal access to and misuse their devices. One of the major challenges is privacy concerns, such as data leakage (Kovacs, 2021) and superfluous permissions (Kovacs, 2021), which could result in the release of personal information. While some of the flaws may be related to the system's liberty, portability and ease of use, others are caused by a lack of awareness and technical talent among mobile application developers (Alshomraniet al.,2023; Rashidi & Fung, 2015). Many mobile app developers do not prioritise privacy and are unaware of the potential harm caused by third-party advertisements and analytics technologies (Alshomraniet al.,2023). A detailed survey of mobile app security concerns showed that up to 70% of Android applications gained permissions that were not required for the programme to function (Rashidi & Fung, 2015).

These superfluous permissions are bad in terms of increased resource consumption and private data leaking. The threats fall into five general categories: information leakage, privilege escalation, repackaging, denial of service (DoS) attacks and collusion (Rashidi & Fung, 2015). In recent years, mobile apps have had a major impact on business, society and lifestyles. Various app markets provide a diverse choice of apps for entertainment, business, health care and social life.

B. Users’ privacy awareness of third-party apps

During the early stages of mobile apps, it was found that about 30% of Android users, 40% of iPhone users, 25% of Mac users and less than 20% of Windows users said that they did not want to use any unidentified applications. However, participants had more free apps on their mobile devices.

Figure 4.10: Users' perspectives on security and privacy during app installation
Source: Thinkwithgoogle.com, 2022

Figure 4.10 depicts the results of a recent study conducted by Thinkwithgoogle.com (2022), which showed that 84% of mobile users were concerned about their privacy as a way of cybersecurity mitigation, 51% opted to use the company or brand mobile app and 58% preferred mobile apps that used cookies. Users of third-party apps frequently agree to the collection of minimal personal data like name and email. Perrotta et al. (2021) emphasise that some third-party apps violate people's privacy because they gather their financial information without providing any real-time information regarding the kind of data they are collecting.

In a study that tested users' awareness of and behaviour towards third-party apps, most users were optimistic in their responses on their ability (self-efficacy) to protect their information. However, most of them also mentioned that they had experienced cybersecurity incidents, like PII leakage, and compromised accounts. Furthermore, they agreed that they did not set up their privacy portfolios during interaction with third-party apps. Therefore, it can be concluded that there is a significant mismatch between users' privacy perceptions and reality (Seng et al., 2021). Mobile privacy concerns have been assuming great importance, due to inadequate disclosure to customers of the collection process by third-party apps of mobile data relating to privacy issues (Tode, 2023). The app service providers collect data and use it to understand and know their users' interests. For example, many users are exposed to pop-up messages or requests to agree to the terms and conditions provided by third-party apps. Most users click "I agree" to the terms and conditions, thus allowing apps to use their data. For example, based on algorithm adjustment and the users' behaviour, location is used to forecast and draw users' attention. The user's location provides significant data about the user, so marketers should ensure that the location data collection is

permission-based to avoid legal issues linked to user privacy invasion. This is because the data about the whereabouts of the user could reveal private information about the user such as the user's income, purchasing patterns and many more. This highlights the need for the regulation of all marketing apps related to digital marketing issues. Therefore, self-regulatory solutions could be the way to go.

When users allow apps to collect their data, they give permission for the apps to do whatever they want with it. Unfortunately, if a user denies providers access to his or her information, they do not allow the user to use their app, or the user receives limited services. This calls for the government or mobile technology bodies to regulate the third-party app ecosystem. While the data may be used to improve an app's functioning, it is more frequently shared and sold to third parties; as they saying goes: "If the service is free, you are the product". The simplest apps that users download exploit whatever information they have about the users' activities to generate revenue.

These apps share users' personal information with third-party companies, which may use it to advertise products or services. It is crucial to always be wary of an app's intentions when it asks for access to personal data and to remember that not being careful may lead to danger. Due to ineffective encryption techniques, some apps make users susceptible to phishing or hacking. An investigation of how mobile users decide on their PII privacy and disclosure behaviour during their interaction with third-party apps showed mixed results (Nikkhah & Sabherwal, 2022). Furthermore, the interplay between security and privacy within information disclosure happens to decrease based on the user's awareness. It should be noted that the method used by the mobile app to collect data could be paraphrased as follows: "If the mobile app service is free, the user is the product and profit provider".

4.4.2. Findings from the empirical data collection

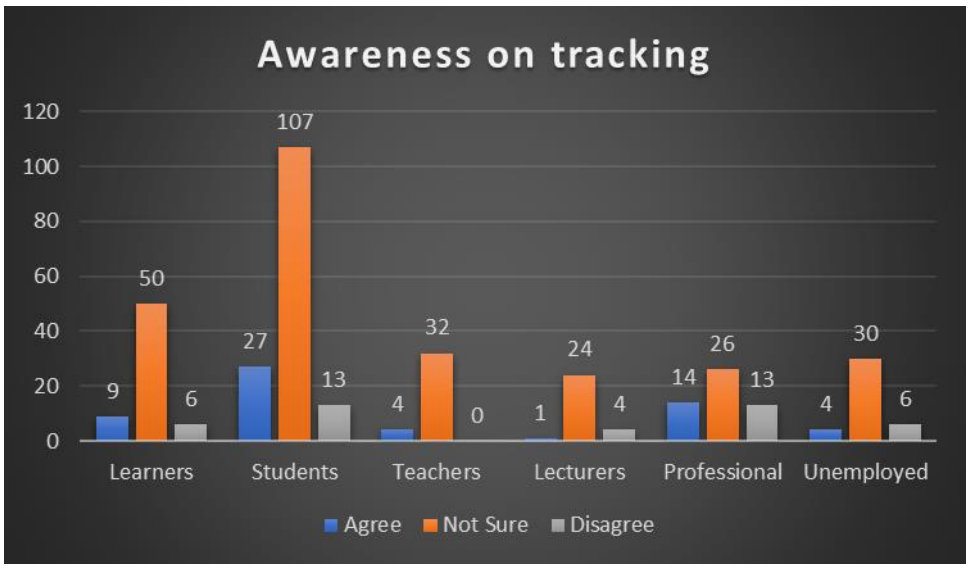

Figure 4.11a: Participants' awareness of third-party app user tracking
Source: Author

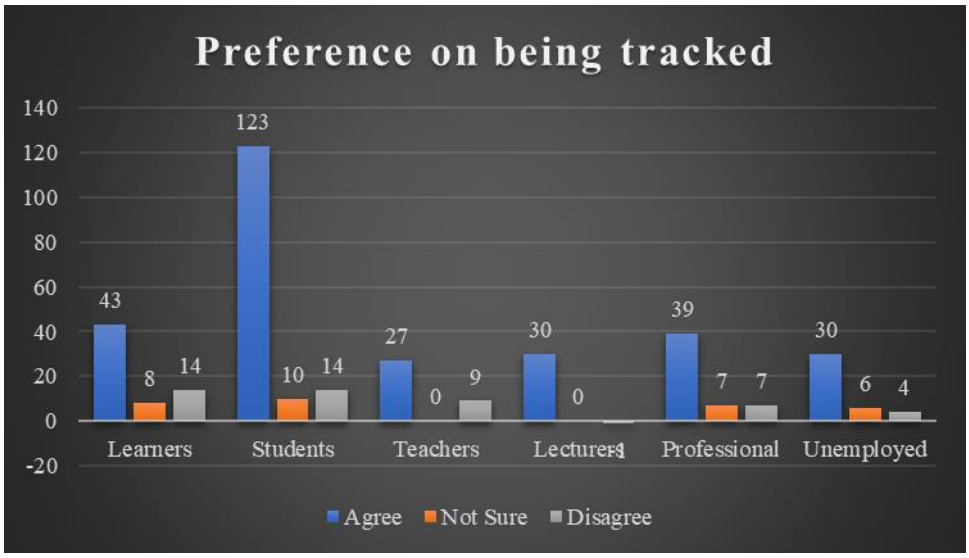

Figure 4.11b: Participants' preference in terms of being tracked by third-party apps
Source: Author

Figure 4.11a illustrates that most participants were not aware that third-party apps were tracking their engagement with their apps. Figure 4.11b depicts that most participants were concerned about the tracking and did not want to be tracked. This shows that mobile devices users care about their data and the fact that their privacy could be violated.

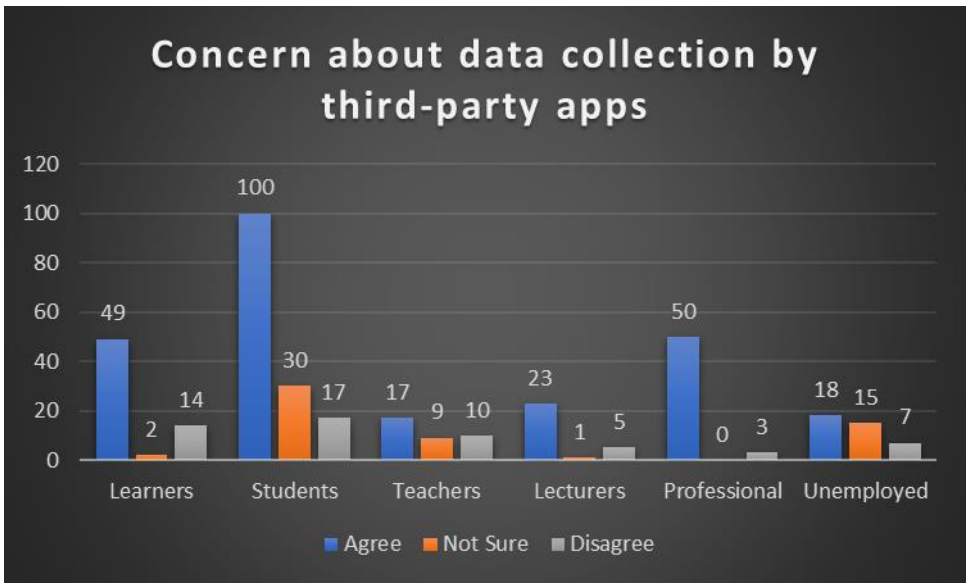

Figure 4.12: Participants' concerns about data collected by third-party apps
Source: Authors

Figure 4.12 illustrates that most participants agreed with the concerns regarding excessive data collection by third-party apps. For example, 94% (50) of 53 professional participants, followed by 79% (23) of 29 sampled lecturers, were against the idea of third-party apps collecting their data. Except for lecturers and learners, all the other clusters were unsure whether to express concern about their data being acquired by third-party apps. Overall, most users were concerned about data collection by third-party apps.

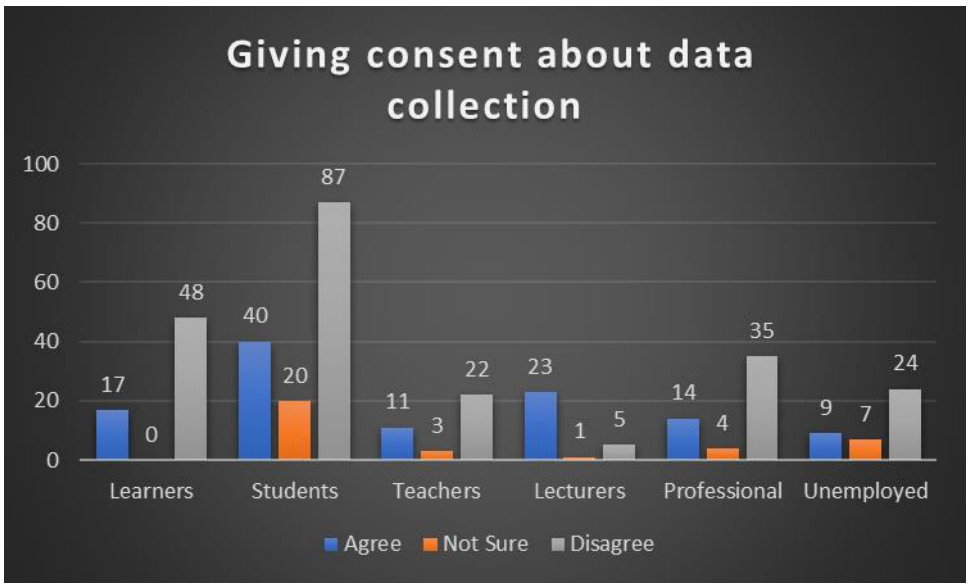

Figure 4.13a: Giving Consent About Data Collection
Source: Authors

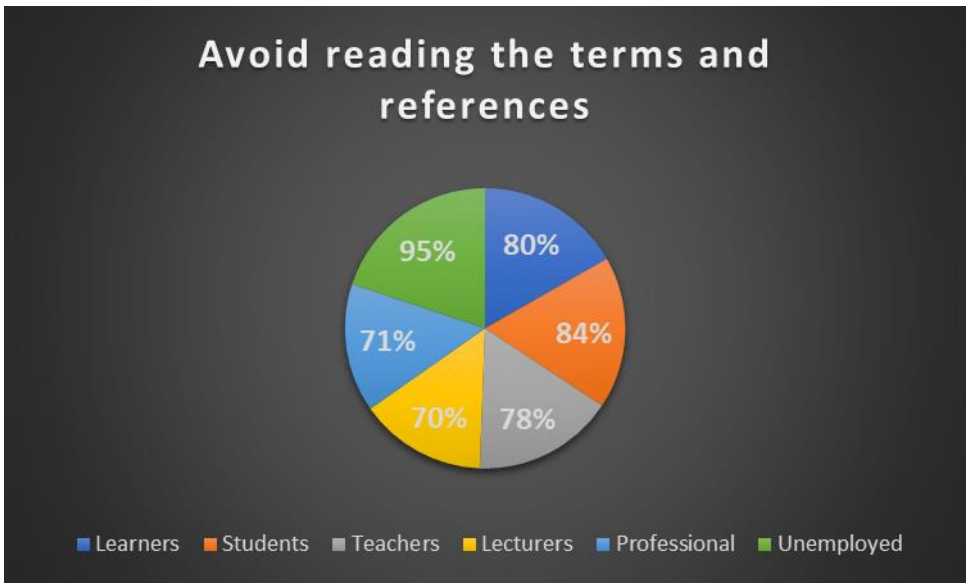

Figure 4.13b: Consent given to app unaware.
Source: Authors

Figure 4.13a illustrates that most participants disagreed that they gave mobile apps consent to collect their data. For example, 74% (48) of 65 learners, 59% (87) of 147 students, 61% (22) of 36 teachers, etc., gave the third-party apps rights to collect their data. However, most of these participants were unaware that they had given consent to their data being collected, since they avoided reading the terms and references of the third-party apps, as illustrated in Figure 4.13b. This led to extensive probing of the mobile device users' awareness of or attitude to general mobile device security.

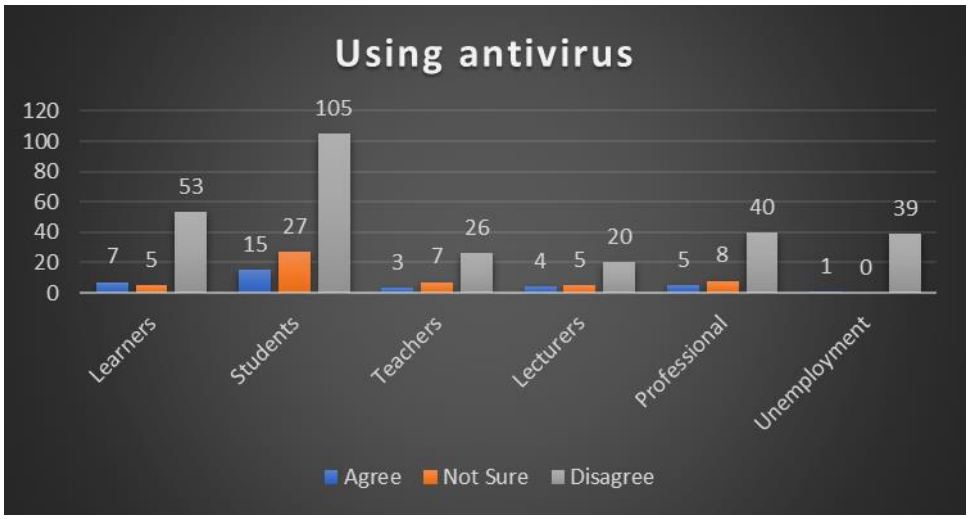

Figure 4.14a: Using Antivirus
Source: Authors

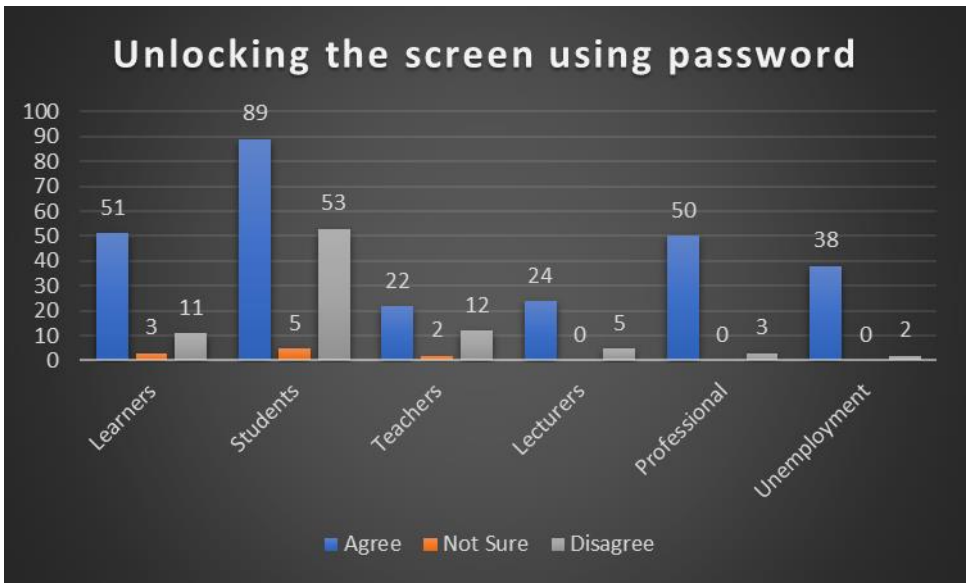

Figure 4.14b: Unlocking the screen using password
Source: Authors

Figure 4.14a illustrates that most users did not use antivirus protection for their mobile devices, while Figure 4.14b shows that most users did use a password for unlocking their mobile device screens.

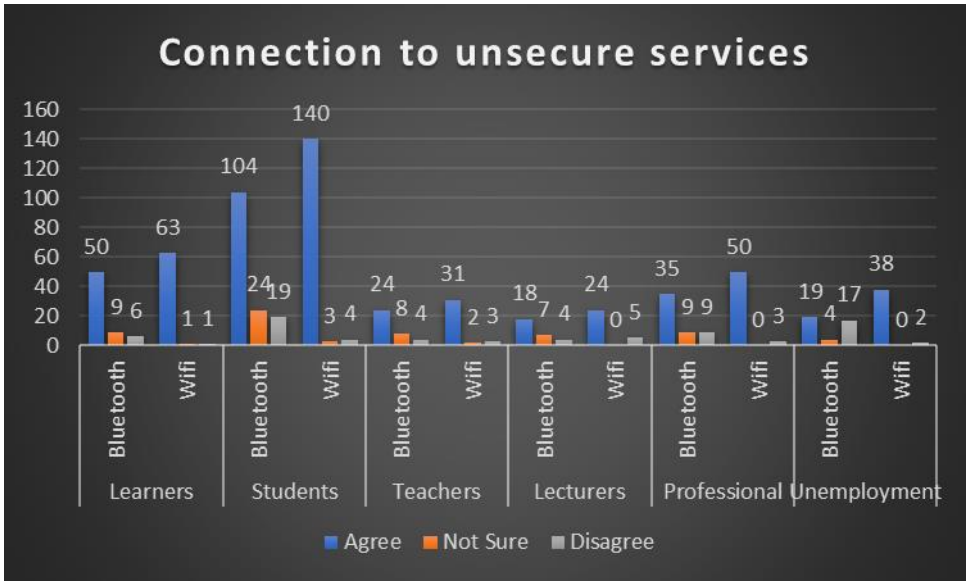

Figure 4.15a: Participants' connection status to unsecured services
Source: Authors

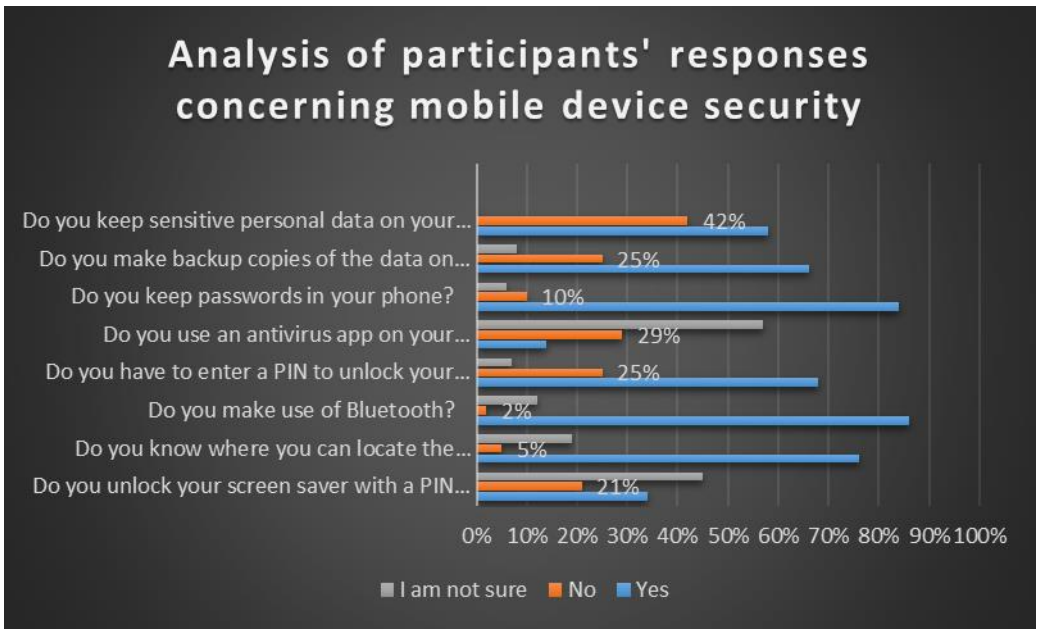

Figure 4.15b: Participants' attitude to and opinion of mobile device security.
Source: Authors

Smart mobile devices could be used as a tool by cybercriminals. Unsurprisingly, mobile device users in the survey underestimated the importance of their collective identities to scammers and how they might be sold. Figure 4.15a shows that most users just opened, accessed and used Bluetooth and public WiFi services anywhere when they had the need to do so, without checking the security of the connection, which in this case would normally be to unsecured services. Figure 4.15b gives a general overview of participants' attitude to and opinion of mobile device security.

Figure 4.13 shows that 34% of users used a PIN code or password to unlock their screen savers, indicating a basic understanding of security procedures. Nonetheless, 21% of users didn't use any kind of screen lock, pointing to a serious lack of prioritising or awareness of security. What's more troubling is that 45% of participants didn't know how to use a password or PIN code, which highlights the urgent need for user education regarding the significance of this basic security feature.

As far as knowledge of IMEI location is concerned, most participants (76%) had a decent level of technical knowledge since they were able to locate their International Mobile Equipment Identity (IMEI) (see Figure 4.15b). This capability is essential for security management and device identification. However, 19% of participants were confused about where to obtain their IMEI and 5% of participants did not know, indicating a potential area for improved user knowledge through focused information dissemination. There was a general lack of knowledge about antivirus software. It could be because most mobile users believed that it was not necessary for mobile

devices. On the other hand, a notable majority of participants were unclear about the use of antivirus programmes and 29% of participants did not use them.

4.5. DISCUSSION

The SLR clearly identified the need for recommendations on safeguarding mobile device users in their interaction with third-party apps; this was confirmed by some empirical studies. Both SLR and empirical data showed that most mobile device users did not give consent to third-party apps using their data.

Mobile users in this study had a reasonable awareness of security procedures and adopted such procedures. To improve overall mobile security, however, there are large knowledge and behaviour gaps that need to be filled. There is an immediate need for extensive user education and awareness initiatives, as indicated by the large number of participants who were ignorant of fundamental security procedures. By promoting improved security practices and knowledge of mobile device protection, such programmes should help to reduce the hazards related to using mobile devices. For example, keeping Bluetooth turned on but setting the device to “invisible” or “non-discoverable” can be a relatively safe approach for reducing the risk of unauthorised connections. Because this area of device management is commonly recognised, few participants had any reservations about how they used Bluetooth.

Furthermore, 68% of the participants used a pin to unlock their sim cards. This shows significant awareness of this crucial security feature. But 25% of participants didn't use a SIM PIN, which could endanger their data if their smartphones were stolen or lost. Furthermore, 7% of participants were unaware of how to use a SIM PIN, indicating a need for user education to improve security measures.

The high level of not using antivirus apps suggests a significant gap in knowledge regarding mobile security and the benefits of antivirus protection, emphasising the importance of enhanced user education in this area. Related to this is that although it was not made clear in the survey whether passwords were securely stored, 84% of participants said they kept passwords on their phones. Ten percent of participants did not keep their passwords on their phones, which lowered the possibility of security issues. There is a need for greater knowledge and application of secure password management strategies, as seen by the 6% of participants who were unclear regarding password storage methods.

Sixty-six percent of participants said that they regularly made backup copies of their phone data, demonstrating a good understanding of the value of data backup for recovery in the event of device malfunction or loss. But 25% of people didn't back up their data, putting them at serious risk of losing everything. Additionally, 8% of participants expressed uncertainty about creating backups, indicating a need for more instruction on the value and techniques of data backup. When it comes to storing sensitive personal data on their phones, 58% of participants reported doing so, underlining the importance of strong security measures to protect this information. Conversely, 42% of users didn't keep sensitive data on their devices – possibly as a safety precaution against future hacks.

The insecure third-party mobile applications can have a detrimental impact on mobile users in terms of information security and data privacy. Insufficient protection for third-party mobile app platforms may result in harmful installations. The goal of this study was to make recommendations for safeguarding mobile device users against third-party app violations of privacy. To achieve this, a literature review and empirical data collection were conducted.

This study found that some of the themes or indicators for measuring mobile users' CIA against the third-party apps are privacy, transparency, oversight and accountability (Brynielsson et al., 2016; Horne et al., 2016; Hoofnagle et al., 2019; Padilla & Freire, 2019; Wong et al., 2019; Enoch et al., 2020; Awojobi & Ding, 2020; Tode, 2023). There is an apparent lack of disclosure regarding regulations or governance during digital mass surveillance.

The protection of data based on users' profiles as they register on the third-party apps seems to be compromised. In this regard, the following proposals are made for drafting recommendations that could safeguard mobile device users against violations by third-party apps:

- The CIA concept with digital mass surveillance governance indicators – using the concept of the CIA framework, the indicators of digital mass surveillance are closely aligned and could be used for drafting recommendations:
    - Privacy – is within the confidentiality container of the CIA
    - Transparency – is within the integrity container of the CIA
    - Oversight and accountability – are both within the availability container of the CIA.
- Inadequate CIA disclosures during digital mass surveillance – most mobile device users are not aware that their interaction with third-party apps discloses some data about their devices

or them as individuals (Huckvale et al., 2019; Reardon et al., 2019). This was supported by empirical evidence, as illustrated in Figure 4.6.

- Non-disclosure and identification of digital trackers during digital mass surveillance – inadequate disclosure of server-client (communication or interaction) data is a challenge within mass surveillance. As a mobile device user, it is easy to be deceived and believe that the information received is only transmitted one way. For example, when a user uses Google search or Facebook for checking other people's profiles, it appears that the data only flow one way (Schechner, 2019). However, information flows just as much from the user into the device and to the services used as it does from the mobile device to the user. A server-client model is used to disclose users' data (client) to the cloud or service provider organisation (server). Regardless of how users use the internet, it is practically guaranteed that a user's online behaviour will be tracked in some way (Schechner, 2019). This was supported by empirical evidence, as illustrated in Figure 4.5.

- Privacy awareness – regarding third-party apps it is essential to maintain digital privacy and security in an increasingly interconnected world where personal data are an asset. By being aware, informed and proactive, users can better protect their privacy and make conscious choices about the apps they use and trust with their data. The confidentiality component of the CIA triad primarily deals with preventing unauthorised access, disclosure or use of sensitive information. While confidentiality measures can indirectly support privacy by protecting personal data against unauthorised access, the same can be said about the integrity component which involves measures to prevent unauthorised modification or destruction of data. Like confidentiality, maintaining data integrity indirectly supports privacy by ensuring that personal information is accurate and reliable. The following privacy themes were instrumental in drafting recommendations that could safeguard mobile device users against violations by third-party apps:

    - Users' behaviour – refers to altering users' behaviour so that they better protect themselves against third-party app violations, which involves a combination of awareness, education and proactive steps.

    - Users' awareness – refers to educating oneself and others about common privacy risks associated with third-party apps, such as data breaches, unauthorised data sharing and potential misuse of personal information.

- Risk and ethics – refer to privacy awareness and encourages developers and app users to consider the ethical implications of data collection and usage. It promotes responsible practices that prioritise user privacy and consent.

Some app providers depend on third-party services plus tools for functions like advertisement targeting, analytics and payment processing (Talal et al., 2019). Due to variations in app providers' adherence to similar security standards, some third-party integrations could introduce vast additional security risks in the apps that mobile device users download.

4.6. CONCLUSION

Data breaches occur due to regular permission requests from third-party applications which acquire access to the user's data, such as personal identifiers, contacts and location information. The user consent strategy of protecting data is supposed to prevent data breaches and ensure security. However, it is ineffective since many users either do not have adequate knowledge of the impact of granting permissions to third-party applications to access their data or become exhausted reading the requests and just grant permissions or feel obligated to agree to the terms to use the app.

This chapter provided useful insights into participants' background information, technological competence and privacy awareness. The findings highlighted the magnitude of privacy problems in mobile apps. Most participants were concerned about data collecting and tracking. According to the findings, it is critical to install strong security measures and perform regular data backups. Many participants were uninformed of the risks and did not see cybercrime as a serious issue. This was demonstrated by the findings in Figure 4.13b, which showed that most users just opened, accessed and used Bluetooth and public Wi-Fi services whenever they needed to, without considering the security of the connection, which would typically be unsecured. While Figure 4.13a provided a general idea of how participants approached mobile device security, Figure 4.13 showed that 34% of users used a PIN code or password to unlock their screen savers, indicating a basic understanding of security procedures.

Nonetheless, 21% of users didn't use any kind of screen lock, pointing to a serious lack of prioritising or awareness of security. What's more troubling is that 45% of participants didn't know how to use a password or PIN code, highlighting the urgent need for user education regarding the significance of this basic security feature. Figure 4.13 demonstrated that 34% of users employed a PIN number or password to open their screensavers, suggesting a rudimentary grasp of security measures. However, 21% of users did not employ a screen lock, indicating a major lack of

prioritisation or security awareness. What's more disturbing is that 45% of participants had no idea how to use a password or PIN code, highlighting the critical need for user education on the importance of this basic security measure.

The chapter’s findings, as well as the increasing complexity of the end-user mobile and online environment, emphasise the importance of ongoing training programmes for basic online security and the establishment of a security culture among smart mobile device users. It is also beneficial to educate users on the best security practices, which are described in greater detail in the following chapter.

CHAPTER 5

MAIN CONTRIBUTION: RECOMMENDATIONS

5.1. INTRODUCTION

The CIA framework refers to user risks and inherent complications that might cause data leakage and compromise information confidentiality, integrity and availability, addressing the crucial need to protect users' sensitive data and personally identifiable information (PII) that may be accessed through mobile apps. The CIA triangle serves as a theoretical standard in this study to investigate the privacy and security problems raised by third-party apps.

The researcher used a systematic literature review (SLR) as well as empirical research to obtain data regarding mobile device users' privacy awareness and consent for personal information identification and digital mass surveillance during their interaction with third-party mobile apps. The results were presented in Chapter 4 and themes contributing to the recommendations made in this chapter were sourced and validated in the SLR and empirical data.

The discussion in this chapter constitutes this dissertation's main contribution, which is a total list of 10 recommendations that were produced by collecting data through the SLR and empirical questionnaires. The CIA framework was used as the aligning conceptual framework for the recommendations to be safeguarding mobile users against violations by third-party applications. In this regard, the recommendations presented in this dissertation follow the CIA framework. They are designed to assist the users with CIA cybersecurity threats, privacy issues and vulnerability that could be brought about by violation of users' data by third-party apps.

- Confidentiality refers to the safeguarding of information against unauthorised access. Making use of secure search engines is a form of protection for users. These search engines work differently from the most popular search engines like Google or Yahoo. Private search engines have a different business model than big search engines, which rely on advertisements for revenue. One such example is DuckDuckGo, a private search engine that refrains from user tracking to provide a more secure user-focused search engine. Qwant is another private search engine that respects user privacy and does not track user searches (Zhang et al., 2019). Yet another good option for user browsing is a private search engine called Search Encrypt. This search engine uses a client-side encryption to keep users' search history private from other users sharing the same device.

- Integrity is the state in which data are complete, reliable and free from unintentional modifications or changes by unauthorised users. Mobile apps are particularly vulnerable to "man in the middle" attacks. Data that are sent to and from the server are intercepted by the attacker. As a result, login passwords, sensitive data and even files can be intercepted and used to the attacker's advantage (Michael, 2019). It happens mostly because with so many agreements, permissions and "confirm" buttons, people do not pay enough attention to what they agree to, creating an ideal environment for malicious interception attempts. Therefore, taking extra precautions is always advised, such as encrypting passwords that may be stored locally on the user’s mobile device; 43% of participants polled in this study indicated that they kept their passwords encrypted on their phones.

- Availability means that it is available when needed. Permissions should be limited to those required for the app's functionality. It is crucial to regularly back up vital personal information on external hard drives. Ransomware, a sort of virus, involves fraudsters locking computers and preventing access to valuable files. According to the results of this study, 66% of individuals polled claimed they routinely backed up their data (Zhang, 2024). Backing up files can help mitigate the effects of a ransomware attack. Additional protection is afforded by installing appropriate security software. Other types of malwares can prevent access to data by overloading the system or just deleting files, so caution is advised.

5.2. RECOMMENDATIONS TO SAFEGUARD MOBILE USERS AGAINST VIOLATIONS BY THIRD-PARTY APPS

Third-party apps collect a wide range of data from users, often with the goal of providing personalised services, improving user experience and monetising user information (Huckvale et al., 2019). While some mobile device users are aware of the level of consent they grant to third-party agencies, others may be unaware or may not completely comprehend the ramifications of their consent.

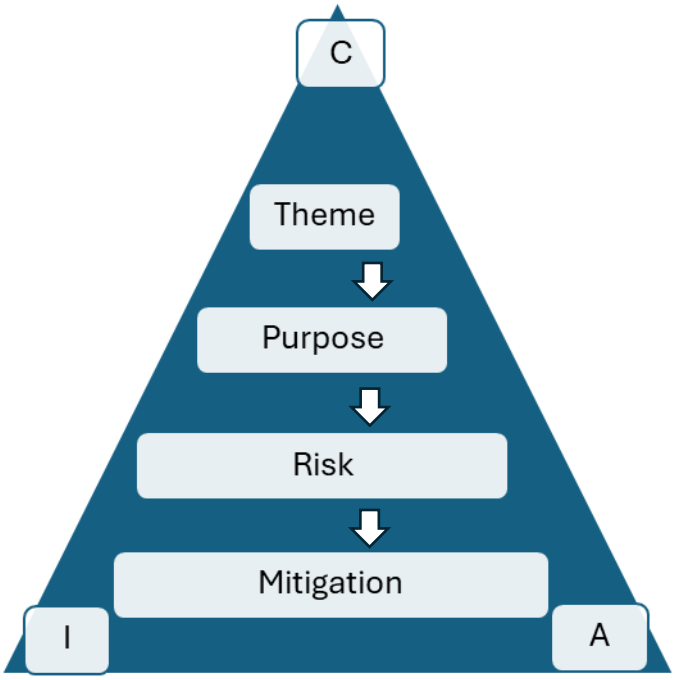

Figure 5.1: The conceptualisation of the study recommendations.
Source: Authors

This section presents the recommendations for safeguarding mobile users against violations by third-party applications and uses the format in Figure 5.1 to briefly show how the recommendation was conceptualised and in which CIA Triad framework the recommendations cover. In this regard, the format allowed the researcher to briefly explain the risk and mitigation of not adhering to the recommendations.

5.2.1. Recommendation 1: Users should prioritise their privacy awareness

Theme: Permissions may be necessary when connecting with the system application programming interface (API), databases, message-passing system or third-party apps (Reardon et al., 2019). However, Figure 4.11a shows that most participants were unaware that third-party apps tracked their app engagement. This demonstrates that mobile device users were concerned about their data and how their privacy might be abused.

Purpose: This recommendation will ensure that no user data are accessed by the wrong people.

Possible risk: People are often exposed to all risks associated with social engineering and online crimes since the data acquired may not be adequately protected (Alkhalil et al., 2021). Smartphones save information about users, from their name and address to their driver's licence number, passport number and credit card number (Hatamian et al., 2019). Mobile devices retain far more personally identifiable information (PII) than fixed platforms. These aspects of mobile platforms (active

collection of personal data and absence of antiviral programmes) might make users feel more at risk than they would on fixed platforms, which would call for more investigation.

Mitigation: Users should be secured against the various third-party applications and assured that no user data could be accessed by third-party hackers and spies. This assurance should reflect on the third-party apps' cookies or policies.

5.2.2. Recommendation 2: Read the privacy policies of third-party apps

Theme: The empirical data in Figure 4.11a show that most participants denied that they provided mobile apps permission to collect their data. However, because they avoided reading the terms and references of third-party apps, most of these participants were unaware that they had given consent for their data to be gathered, as shown in Figure 4.11b. This was supported by a study conducted by Zou et al. (2019), who discovered that most smartphone users ignore privacy permissions while installing third-party apps, becoming victims of data theft, which can lead to more serious concerns for them.

Purpose: This recommendation ensures that no user data are accessed without the user's consent.

Possible risk: Online users should be encouraged to read and understand the privacy policies of applications and websites before they consent to requests to access their private data. Research by Tode (2023) indicated that many users consented to third-party applications without understanding their privacy policies and without knowing how their data would be used. Therefore, data breaches are mostly contributed to by online users' behaviour as they agree to the cookies' request to access their data without adequate knowledge of the site. Hence, they consent to malicious websites collecting their private data without knowing how their data are to be used.

Mitigation: Privacy policies outline what data the app collects from users, including personal information and browsing behaviour. By reading the policy, users can understand the extent of data collection through cookies and other tracking technologies.

- Purpose of data usage: Privacy policies specify how the collected data will be used. This includes purposes such as improving services, advertising or sharing with third parties. Understanding these purposes helps users make informed decisions about whether to accept cookies.

- Consent requirements: Many jurisdictions require informed consent for data collection through cookies. By reading the privacy policy, users ensure that they are giving informed consent based on their understanding of how the data will be used.

- Opt-out options: Privacy policies often explain how users can opt out of certain types of data collection or cookies. This can include instructions on managing cookie settings in the browser or within the app itself.

- Legal protection: In some cases, privacy policies can provide legal protection. They may outline users' rights regarding data access, correction or deletion, depending on applicable laws and regulations.

5.2.3. Recommendation 3: Enable multi-factor authentication

Theme: Alkhalil et al. (2021) conducted research on the various phishing tactics employed by attackers and the information they want to obtain. The report also provides several strategies to prevent phishing, such as implementing multi-factor authentication, which is an important additional layer of security. When it comes to storing sensitive personal data on their phones, 58% of participants reported doing so, highlighting the significance of effective security methods to protect this information, one that offers an extra layer of protection beyond the password.

Purpose: Robust authentication is an essential security component of digital tools and technologies. Multi-factor authentication is the initial line of defence that attackers must overcome before causing damage, because user authentication provides an access point for cybercriminals or harmful actors.

Possible risk: According to research by Ogbanufe (2023), more than 99.9% of compromised systems did not employ multi-factor authentication (MFA) to secure their accounts.

Mitigation: Multi-factor authentication (MFA) can assist in protecting users against third-party apps in several ways:

- Mitigation of credential theft: Third-party apps might be compromised or designed maliciously to steal login credentials. If such an app captures a user's password, MFA can prevent unauthorised access because the attacker would not have the second factor required to complete the login process.

- Control and visibility: Many MFA systems alert users and administrators when and where authentication attempts occur. This allows users to detect unauthorised access attempts originating from third-party apps and acts (such as revoking access tokens or changing passwords).

- Integration with OAuth and SSO: For applications that use OAuth (Open Authorisation) or Single Sign-On (SSO), MFA can be integrated to provide an additional layer of security during the authentication process. This ensures that even if a third-party app gains access through legitimate authentication, it still cannot proceed without the second factor of authentication.

5.2.4. Recommendation 4: Ensure regular updates and app source verification

Theme: The literature indicates that mobile devices are used extensively worldwide. The growing use of mobile devices is creating new commercial opportunities for mobile platforms and apps. The sector involved in developing mobile apps is flourishing, especially with the integration of artificial intelligence (AI) into these applications, which has increased their appeal (Turner, 2021). This necessitates considering the source in addition to frequent updates.

Purpose: When downloading third-party software on their mobile devices, users should prioritise regular updates as well as scrutiny of the source. Failure to do this could create significant security breach issues and allow the hackers to exploit underlying vulnerabilities to access the data (Hildmann & Kovacs, 2019).

Possible risk: Users who download applications from untrusted sites risk unwittingly downloading compromised or dangerous software on their devices. These applications might have security flaws that hackers could use to obtain private information without authorisation, or they may jeopardise the device's overall security. Users can reduce such risks by being cautious and making sure that app sources are reliable. There are numerous examples of apps that were downloaded from unreliable sources and resulted in user data compromise or security breaches. For example, counterfeit or modified versions of popular apps such as WhatsApp on unofficial app stores have caused users to unwittingly download malware-infected software, leading to data theft, financial fraud and other security incidents. In summary, avoid sideloading apps whenever possible; download apps only from official app stores (such as Google Play Store or Apple App Store) or reputable sources recommended by the platform.

Mitigation: Updating mobile apps on a regular basis is crucial to maintaining security. Updates frequently contain bug fixes, security feature improvements and patches for known vulnerabilities. Through timely installation of updates, users can reduce the possibility of known vulnerabilities being exploited, protecting their devices and data against possible threats. Ensuring regular updates on third-party apps plays a crucial role in mitigating privacy and security risks in several ways:

- **Data breach prevention**: Updated apps often have strengthened security measures that help prevent unauthorised access to sensitive data. This reduces the likelihood of data breaches that could lead to the exposure of personal information.

- **Privacy enhancements**: Updates may include privacy-focused improvements, such as enhanced data handling practices or clearer user consent mechanisms. This helps ensure that data are handled in accordance with privacy preferences and regulatory requirements.

- **Bug fixes**: Updates typically address bugs and software glitches that could inadvertently expose data or weaken the app's security posture. Regular updates minimise these risks by improving the overall stability and reliability of the app.

- **Enhanced encryption and authentication**: Updated apps often implement stronger encryption standards and authentication mechanisms, making it harder for unauthorised entities to intercept or access data transmitted through the app.

5.2.5. Recommendation 5: Back up data

Theme: This study shows that 25% of people polled did not back up their data, putting them at risk of losing everything. Furthermore, 8% of participants were unsure about creating backups, highlighting the need for more training on the importance and practices of data backup. This was supported by a Baddar (2017) study that underlined the need of backing up your data and how it can play a critical role in mitigating the impact of third-party app violations such as data breaches, loss, or corruption.

Purpose: Backing up data is crucial for limiting exposure to third-party apps and mitigating privacy and security risks.

Possible risk: Third-party apps can sometimes experience bugs, glitches or crashes that lead to data loss. Without backups important information stored in these apps may be lost.

Mitigation: Backing up data is crucial for limiting exposure to third-party apps and mitigating privacy and security risks in several important ways:

- **Protection against data loss:** Regular backups ensure that copies of important data are stored securely. In case of data loss due to app malfunctions, device failure or security incidents, data can be restored without relying on potentially compromised third-party apps.

- **Recovery from ransomware and malware attacks:** Ransomware and malware attacks can encrypt or delete data, making it inaccessible. Having backups allows restoring data to a pre-attack state, reducing the impact of such incidents on privacy and security.

- **Protecting against device theft or loss:** If a mobile device is lost or stolen, backups ensure that data remain accessible from other devices or can be restored once access is gained to a new device. This prevents sensitive information from falling into the wrong hands.

5.2.6. Recommendation 6: Use security software

Theme: Checkpoint (2017) found that a robust antivirus solution may greatly minimize the danger and effect of copycat malware on Android devices by providing detection, real-time protection, and safe surfing capabilities. The empirical data in Figure 4.14a showed that most users did not use antivirus software to protect their mobile devices. The large percentage of people who did not use antivirus apps indicates a sizeable knowledge gap about mobile security risks and the benefits of antivirus protection, underlining the significance of further user education in this area.

Purpose: Using antivirus software helps mitigate security risks associated with third-party apps by providing malware detection, behaviour monitoring, real-time protection and privacy safeguards. It complements the security practices of app stores and helps users maintain a secure and protected digital environment.

Possible risk: Not using antivirus software in relation to third-party apps increases the likelihood of malware infections, data breaches, phishing attacks, performance issues and other security threats. Antivirus protection is essential for safeguarding devices, data and personal information against the evolving landscape of cyber threats associated with third-party app usage.

Mitigation: Antivirus software plays a crucial role in mitigating violations and security risks associated with third-party apps by employing several key mechanisms and capabilities:

- **Malware detection and prevention:** Anti-virus software scans apps and files for malware, including viruses, trojans, ransomware and other malicious software. This helps detect and prevent malicious apps from compromising the device and accessing sensitive information.

- **Behaviour monitoring:** Some anti-virus programmes monitor the behaviour of apps in real time. This helps identify suspicious activities or unauthorised access attempts by apps, which could indicate potential privacy or security breaches.

- **Phishing protection:** Anti-virus software often includes features to protect against phishing attacks, where malicious apps or websites attempt to trick users into revealing sensitive information, such as passwords or credit card details.

5.2.7. Recommendation 7: Limit the information that is exposed

Theme: A digital tracing approach called voluntary contact-tracing applications was employed during the COVID-19 outbreak, as demonstrated by the SLR finding in Figure 4.1. To assess all interactions with others, this approach uses location data to map the places people visit. The empirical data in Figure 4.5b measure the participants' understanding of digital mass surveillance; it was discovered that relatively few knew about it. This recommendation addresses the question raised in the literature findings on "digital mass surveillance and how it affects user privacy".

Purpose: Users can adhere to the principles of minimising data collection, limiting data to what is necessary and de-identifying collected data; these platforms can mitigate privacy risks and enhance user trust (Zhou et al., 2012). Limiting the information exposed to third-party apps is critical for mitigating privacy and security risks.

Possible risk: Third-party apps may not have robust security measures, leading to potential data breaches where sensitive information is accessed by unauthorised parties.

Mitigation: To effectively limit the information exposed to third-party apps requires:

- **Minimising data exposure:** By providing only necessary information to third-party apps, users reduce the amount of personal data that could potentially be accessed or compromised in case of a data breach or misuse.

- **Reducing attack surface:** Limiting the information exposed helps reduce the digital footprint and minimises the attack surface for malicious actors looking to exploit vulnerabilities in apps or services.

- **Preventing unauthorised access:** By withholding sensitive information, such as personal identifiers or financial details, users lessen the risk of unauthorised access to accounts or personal data by third parties or cybercriminals.

5.2.8. Recommendation 8: Strengthen password management practices

Theme: A study by Li and Yang (2020) emphasized how strong passwords are part of a broader security practice that includes user awareness and cautious behaviour. The empirical results depicted in Figure 4.14b demonstrate a concerning statistic: 45% of participants did not know how to use a password or PIN code, emphasising the critical need for user education on the importance of this basic security feature.

Purpose: Mobile device users should prioritise password management techniques such as using strong, unique passwords, storing passwords securely and updating passwords on a regular basis. Mobile device users can greatly improve their security posture by implementing password management techniques, shielding confidential and private data from hackers and unwanted access.

Possible risk: Weak passwords are easier for attackers to guess or crack using automated tools, potentially allowing unauthorised access to accounts.

Mitigation: A more secure mobile environment overall will result from educating users about these procedures and the significance of handling data securely (Balash et al., 2022). Using a strong password on third-party mobile apps offers several key benefits:

- **Enhanced security:** A strong password significantly increases the difficulty for unauthorised users to guess or brute-force their way into accounts. This helps protect personal and sensitive information from being accessed by malicious actors (Balash et al., 2022).

- **Prevention of unauthorised access:** Strong passwords act as a barrier to unauthorised access attempts, reducing the risk of identity theft, financial fraud or privacy breaches. This

is especially important for mobile apps that may store personal data or have access to sensitive features like payment information.

- **Mitigation of credential stuffing attacks:** Weak passwords are often targeted in credential stuffing attacks, where hackers use lists of known usernames and passwords to gain unauthorised access to multiple accounts. Strong passwords make it more difficult for attackers to exploit these vulnerabilities.

- **Protection against account takeover:** A strong password reduces the likelihood of someone gaining control of accounts through techniques like phishing or social engineering. This helps maintain users' control over their personal data and prevents misuse of their accounts.

5.2.9. Recommendation 9: Monitor account activity

Theme: This recommendation addresses the question raised in the above literature findings on how much of the data are collected beyond the user's consent and aligns with the principles of the CIA triad. Regardless of how users feel about their personal information being shared with third-party apps, it is critical to at the very least comprehend the information they are presenting (Sarkar et al., 2019). According to the empirical results shown in Figure 4.12, most participants believed that third-party apps collect too much data.

Purpose: Users should frequently review the data collected by third-party apps. This means that if the user is storing personal information, he or she must always be aware of where it is and be able to update or delete it at the request of the data subject.

Possible risk: Some apps may collect more data than necessary or share data with other parties without users' knowledge. Without monitoring, users may not realise the extent of data being collected or how it's being used.

Mitigation: Monitoring account activity is essential for limiting exposure to third-party apps and mitigating privacy and security risks in several significant ways:

- **Early detection of unauthorised access:** Regularly monitoring account activity allows users to quickly identify and respond to any unauthorised access attempts or suspicious

activities. This early detection helps prevent further compromise of accounts or personal information.

- **Alerts for anomalies:** Many online services and apps have alert mechanisms for unusual account activities, such as login attempts from unfamiliar locations or devices. Monitoring these alerts enables prompt action to secure accounts and investigate potential security breaches.

- **Identification of data breaches:** Monitoring account activity helps users recognise signs of a data breach, such as unauthorised changes to account settings, unexpected purchases or abnormal login patterns. This allows users to take immediate steps to mitigate the impact and secure information.

5.2.10. Recommendation 10: App reviews and ratings

Theme: Creating sufficient awareness of the basics of reading and understanding the privacy policies of applications and websites would effectively eliminate data breaches (Reidenberg and Schaub, 2018). Figure 4.8a demonstrated that most participants believed their third-party apps profiled them when they engaged with their platforms. Reading app reviews and ratings will give insight into the app's reliability, functionality, and general quality.

Purpose: Reading third-party app reviews and ratings helps users make informed decisions, mitigate risks and choose apps that best meet their needs while prioritising security and reliability.

Possible risk: Not reading third-party app reviews and ratings can lead to installing unreliable, insecure or unsuitable apps that compromise the device's performance, data privacy and overall user experience. Taking the time to review feedback from other users helps users make more informed decisions and avoid potential pitfalls.

Mitigation: Reading third-party app reviews and ratings serves several important purposes:

- **Assessing reliability and quality:** Reviews and ratings provide insight into the app's reliability, functionality and overall quality. They can help users gauge whether the app performs as advertised and meets user expectations.

- **Identifying security concerns:** Reviews often highlight security issues or vulnerabilities that users have encountered. This information can alert users to potential risks associated with the app, such as data breaches or privacy violations.

- **Understanding user experiences:** Reviews offer firsthand accounts of other users' experiences with the app. This includes usability, performance issues, bugs and customer support responsiveness, giving a clearer picture of what to expect.

- **Evaluating customer support:** Reviews can indicate how well the app developer responds to user feedback and addresses issues. Good customer support can make a significant difference when encountering problems with the app.

5.3. RECOMMENDATIONS VALIDATION: CONTRIBUTION TO THE BODY OF KNOWLEDGE

Recommendations 5.3.1 to 5.3.10 were validated through different formats that contributed to the body of knowledge, namely:

- This study produced this Master of Science in Computer Science dissertation which offers 10 recommendations for safeguarding mobile users against violations by third-party applications. The researcher believes that the examination process constitutes a validation procedure for the presented recommendations.

- A conference paper highlighted some of these recommendations and the systematic literature review carried out in this study was submitted, blind reviewed, accepted, and presented at the conference. It was published as a Springer Link book chapter. Please see:

    - Mphasane, K; Malele, V. & Mapayi, T. Social media applications' privacy policies for facilitating digital living. *Proceedings of the 7th Computational Methods in Systems and Software 2023*. To appear in the Springer Series: Lecture Notes in Networks and Systems. https://link.springer.com/book/9783031535482

- At the time of submitting this dissertation two other outputs were drafted and submitted:

    - A conference paper that is under review waiting for acceptance. This conference paper further validates the recommendations made by this dissertation:

        - Mphasane, K., Malele, V. & Keifer, T. Safeguarding mobile users from violation by third-party apps. Paper 15 submitted for review to the 2nd

International Conference on Technological Advancement of Embedded and Mobile and Systems (ICTA-eMOS) to be held in Sainte Famille Hotel in Kigali, Rwanda on 19-20 September, 2024.

- A journal article was submitted as a contribution to the body of knowledge. The article is also under review:
  - Mphasane, K. & Malele, V. Recommendations for safeguarding mobile users' privacy. Submitted to the Journal of Information Systems and Informatics, X(X), 2024.

5.4. CONCLUSION

These recommendations are useful for scholars, companies, practitioners and legislators. Following these recommendations can significantly reduce the risks associated with third-party apps and better protect personal information and digital identity. They also lay the groundwork for additional research on the subject, which will be conducted towards obtaining a doctoral degree in Computer Science. The acceptance of conference papers proves that such recommendations for safeguarding mobile users need to be systematically and logically presented through an SRL as well as empirical research, as in the case of this dissertation. These recommendations were not based on a mere Google search.

CHAPTER 6

CONCLUSION AND FUTURE STUDIES

6.1. CONCLUSION

The proliferation of third-party apps has precipitated concerns over privacy and security. Mobile device users should be aware of how third-party apps collect their information. The primary objective of this study was to provide recommendations for protecting mobile users against third-party application violations. The CIA triad theoretical framework was used in this study to understand and assess privacy issues relating to third-party mobile applications collecting and sharing personal data from mobile users with or without their consent or awareness. These recommendations were listed in Chapter 5 of this dissertation.

The study's secondary goals were classified into theoretical and empirical goals in Chapter 1. The theoretical objectives were accomplished as follows. An overview of the literature review was included in Chapter 2, using a systematic literature review approach. Chapter 3 outlined research paradigms. It influenced the decision to perform the research pragmatically, which assisted in constructing the questionnaire used in the study. Chapter 4 highlighted the study findings as well as the growing complexities of mobile users and the online environment. It emphasised the importance of ongoing training programmes on basic internet security and the development of a security culture among smart mobile device users. The contribution of the dissertation to the body of knowledge was discussed in Chapter 5. The recommendations dealt with the research findings and proposed strategies to address the problems and limitations thereof.

A literature review focusing on third-party apps' privacy and security violations was conducted. The main findings showed that various third-party programmes violated users' privacy and security; users were not given the opportunity to exercise proper security measures. Furthermore, mobile users were prepared to share all their personal information with third-party apps, which might be misused by any untrustworthy or unknown organisation. The literature analysis effectively indicated that consumers had little understanding of the origin of privacy breaches and inadequate approaches to handling those breaches. The concepts of breaches, commencement and other associated features showed that individuals were typically unaware of privacy-related measures that could help prevent critical breaches.

According to the study's empirical analysis, most users of mobile devices learnt about privacy and security concerns from social media and search engines. However, the appropriate procedures for protecting privacy were not well understood. Most users were aware of the need for security measures, such as enhanced security like MFA, but did not (i) read the security protocols that come from third-party apps, and (ii) practice security protocols when using third-party apps.

Due to the bottleneck of technological aspects in legislating the third-party apps space, there is a need for unambiguous privacy and security policy to regulate third-party apps. Secondly, platforms should make it easy to implement proper security policies. Lack of awareness regarding the privacy and security of mobile devices is increasing together with the susceptibility to breaches. In this regard, mobile device manufacturers should improve security awareness by embedding a video that creates cybersecurity once the user turns on the new device.

In summary, this study met its primary and secondary research objectives, which were as follows:

- **Objective 1: Exploring digital mass surveillance and its impact on user privacy**

  A thorough literature review was carried out to fully comprehend the ramifications of digital mass monitoring. This included researching scholarly articles, studies and expert analyses to better understand the diverse nature of monitoring activities. The study's thorough investigation yielded rich insights into monitoring methods and highlighted their significant influence on user privacy in the digital sphere.

- **Objective 2: Identifying types and extent of data routinely collected by third-party apps**

  To accomplish this objective, empirical analysis was essential. Users of mobile devices were given carefully crafted questionnaires that probed the depths of third-party apps' data gathering techniques. Through direct user engagement, the research revealed the volume and variety of data that were routinely collected, providing insight into the degree of user data exposure within the digital ecosystem.

- **Objective 3: Identifying the level of consent provided by users regarding data collection by third-party apps**

  Gaining insight into the dynamics of user consent required a thorough examination of user attitudes and actions. The study investigated consumers' knowledge of consent processes and

willingness to share data with third-party apps, using empirical approaches that included questionnaires. This extensive investigation exposed user views regarding consent, critical gaps and misconceptions that underpin data privacy standards.

- **Objective 4: Providing a behavioural change technique to promote awareness of third-party app violations**

To achieve this objective, theoretical frameworks and actual findings had to be combined. Using empirical data and behavioural change theories, the study put forth practical methods to raise user awareness and strengthen preventative privacy protection mechanisms. A comprehensive strategy for reducing third-party app infractions was provided by the recommendations, which ranged from user-centric privacy-enhancing technologies to educational efforts.

To conclude, the study also distinguished itself by adopting a pragmatic research approach, conducting a systematic literature review and addressing both theoretical and empirical goals. Furthermore, it provided ten recommendations that could assist users to safeguard themselves online. These characteristics differentiate it from other studies and contribute to the study's comprehensiveness and applicability in the domain of safeguarding mobile users against third-party application violations.

6.2. STUDY LIMITATION

Whilst the study findings provide strong evidence regarding violations by the third-party apps and the need to safeguard mobile users against such. The study was limited to participants in South Africa, where cultural differences and access to resources may differ from other countries. When it comes to selecting an acceptable sample size for case studies, there are always legitimate concerns. Whilst the author acknowledges that a large sample is more likely to represent the diversity of the population, reducing biases and allowing for findings that are applicable to a broader audience. The author believes that the sample size of 377 participants is more than suffice in the context of the research question the study was looking to address. While the CIA triad addresses security objectives, it may not fully consider compliance obligations, legal requirements, industry standards and regulatory frameworks governing information security and privacy.

A study relying solely on the CIA triad may fail to account for the legal and regulatory landscape within which organisations operate and the implications for security practices and compliance efforts. In summary, while the CIA triad is a valuable conceptual framework for understanding and

addressing information security concerns, it should be used judiciously and supplemented with other frameworks, models and methodologies to ensure a holistic and contextually relevant approach to security and risk management.

Despite efforts to develop comprehensive search strategies, systematic literature reviews may still miss relevant studies due to limitations in database coverage, indexing inconsistencies or variations in terminology used across different disciplines. This can introduce the risk of incomplete retrieval of relevant literature. However, research adds useful, theoretically supported answers to the subject by methodically analysing the literature and identifying gaps.

6.3. FUTURE STUDIES

Future research in the domain of safeguarding mobile users against third-party application violations should consider several promising avenues. Longitudinal studies are essential for tracking the dynamic nature of security and privacy issues in the mobile app ecosystem over time. Such studies can offer significant insights into evolving threats, user behaviours and the effectiveness of recommendations over extended periods. Furthermore, studies should focus on user education initiatives to create innovative approaches for informing and educating consumers about the dangers of using third-party apps.

An interesting research strategy is to identify DNS (server) connections to determine whether an application connects to servers that have low security standards, such as inadequate encryption or an expired certificate. Evaluating the impact of different educational interventions on user behaviour and awareness is crucial for designing effective educational campaigns. There is also a need for app development that will assist the users in testing and not just downloading unnecessary apps. This will be addressed in a system development PhD project once this MSc dissertation has been passed.

The exploration of privacy-enhancing technologies is another critical research area. Researchers should investigate emerging technologies aimed at enhancing user privacy within mobile applications, such as privacy-preserving frameworks, encryption methods and secure authentication mechanisms. Assessing their effectiveness and usability can aid in the development of more secure and privacy-friendly mobile applications. Moreover, regulatory frameworks and their enforcement mechanisms should be scrutinised to identify potential gaps and areas for improvement. Research in

this domain can help ensure that the privacy regulations provide robust protection for mobile user data and are effectively enforced.

Ethical considerations relating to mobile app data collection and sharing deserve closer attention. Investigating the ethical practices of app developers and assessing their alignment with user expectations and societal values are vital. This research can shed light on ethical dilemmas in the mobile app ecosystem and guide the development of ethical guidelines and best practices. User-centric design principles for mobile applications emphasising transparency and user control over data sharing should be a focal point of future research. Assessing the impact of user-friendly interfaces and privacy settings on user decision making can inform the development of apps better aligned to user preferences and concerns.

Cross-platform analysis is essential for understanding how security and privacy practices differ across various mobile platforms, such as iOS and Android. Exploring the unique challenges and vulnerabilities associated with each platform can inform platform-specific recommendations and strategies. Researchers should also remain vigilant against emerging threats in the mobile app ecosystem, including new forms of data collection, invasive permissions or novel attack vectors. Investigating countermeasures and mitigation strategies is crucial to stay ahead of evolving threats.

To foster continuous improvement in mobile app security and privacy, the development of user feedback mechanisms within mobile apps must be considered. These mechanisms can enable users to report privacy and security concerns directly, facilitating user-driven improvements. Behavioural analysis is another essential research avenue, aiming to understand how users interact with mobile apps concerning privacy and security. Exploring the factors influencing user decision making regarding app installation, data sharing and permissions can offer valuable insight into user behaviours and motivations.

Collaborative research efforts involving academia, industry and regulatory bodies should be encouraged to create a holistic approach to mobile app security and privacy. Such collaborations can lead to the sharing of data, insights and best practices, ultimately benefiting all stakeholders. Impact assessment research can evaluate the real-world effectiveness of security and privacy interventions, such as app store policies, privacy tools or user education campaigns, providing evidence-based insight into their impact on mitigating violations.

Recognising that privacy perceptions and behaviours may differ significantly across cultures and regions, research should explore cultural and regional variances in mobile app privacy expectations and behaviours to develop context-sensitive recommendations and strategies. These recommendations collectively represent a comprehensive roadmap for future research endeavours to enhance the protection of mobile users against third-party application violations.

Finally, it is critical to recognise this study's limitations and suggest directions for additional study. More research is necessary in a few areas to improve comprehension of mobile app security and privacy. Longitudinal studies should feature in future research to monitor how security and privacy concerns in the mobile app ecosystem change over time. This method can offer pertinent information on new dangers and the long-term efficacy of recommendations. To find gaps and areas for improvement, more research on regulatory frameworks and enforcement methods is necessary. Robust protection of mobile user data and efficient enforcement of privacy standards can be guaranteed by research in this field.

REFERENCES

Ablon, L., Heaton, P., Lavery, D.C. & Romanosky, S. 2016. Consumer attitudes toward data breach notifications and loss of personal information. Rand Corporation.

Alharahsheh, H.H. & Pius, A. 2020. A review of key paradigms: positivism VS interpretivism. Global Academic Journal of Humanities and Social Sciences, 2(3):39-43.

Ali, S., Islam, N., Rauf, A., Din, I.U., Guizani, M. & Rodrigues, J.J. 2018. Privacy and security issues in online social networks. Future Internet, 10(12):114.

Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I. 2021. Phishing attacks: a recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3:563060.

Alkhariji, L., Rana, O. & Perera, C. 2020. Examining the interplay between privacy by design (PbD) schemes and privacy patterns.

Alshomrani, N., Furnell, S. and He, Y., 2023, July. Assessing User Understanding, Perception and Behaviour with Privacy and Permission Settings. In International Conference on Human-Computer Interaction (pp. 557-575). Cham: Springer Nature Switzerland.

Alturki, R. 2021. Research onion for smart IoT-enabled mobile applications. Scientific Programming, 2021:1-9.

Appel, G., Libai, B., Muller, E. and Shachar, R., 2020. On the monetization of mobile apps. International Journal of Research in Marketing, 37(1), pp.93-107.

Awojobi, B. & Ding, J. 2020. Data security and privacy. In: Cybersecurity for information professionals: concepts and applications. p. 291.

Balapour, A., Nikkhah, H.R. & Sabherwal, R. 2020. Mobile application security: role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52:102063.

Baddar, S.A.H. 2017. How on earth could that happen? An analytical study on selected mobile data breaches. In: Adaptive mobile computing. Academic Press. pp. 153-183.

Balash, D.G., Wu, X., Grant, M., Reyes, I. & Aviv, A.J. 2022. Security and privacy perceptions of (third-party) application access for Google accounts. In: 31st USENIX Security Symposium (USENIX Security 22). pp. 3397-3414.

Barth, S., de Jong, M.D., Junger, M., Hartel, P.H. & Roppelt, J.C. 2019. Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics and Informatics, 41:55-69.

Belanche, D., Flavian, M. & Perez-Rueda, A. 2020. Mobile apps use and WOM in the food delivery sector: the role of planned behavior, perceived security and customer lifestyle compatibility. Sustainability, 12(10):4275.

bferrite. 2023, March 6. How the copycat malware infected Android devices around the world. CheckPoint. https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/

Bhadouria, A.S. 2022. Study of impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications.

Brynielsson, J., Franke, U. & Varga, S. 2016. Cyber situational awareness testing. In: Combatting cybercrime and cyberterrorism: challenges, trends and priorities. pp. 209-233.

Burger, A., Oz, T., Kennedy, W.G. & Crooks, A.T. 2019. Computational social science of disasters: opportunities and challenges. Future Internet, 11(5):103.

Thomas, C.G. 2021. Research methodology and scientific writing. Springer.

Nickerson, C. 2023. Positivism in sociology: definition, theory & examples. Simple Psychology. https://www.simplypsychology.org/positivism-in-sociology-definition-theory-examples.html

Christian, M. 2022. Information security and privacy in a digital world: a human challenge. TU Darmstadt Publication Service. https://tuprints.ulb.tu-darmstadt.de/21138/

Craig, A., Horne, A.A. & Maynard, S.B. 2016. A theory on information security. Australasian Conference on Information Systems. Wollongong, Australia.

Debatin, B., Lovejoy, J.P., Horn, A.K. & Hughes, B.N. 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1):83-108.

Dekkers, R., Carey, L. & Langhorne, P. 2022. Search strategies for [systematic] literature reviews. In: Making literature reviews work: a multidisciplinary guide to systematic approaches. Cham: Springer International Publishing. pp. 145-200.

Ebrahimi, F. & Mahmoud, A. 2022. Unsupervised summarization of privacy concerns in mobile application reviews. In: Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering. pp. 1-12.

Enoch, S.Y., Huang, Z., Moon, C.Y., Lee, D., Ahn, M.K. & Kim, D.S. 2020. HARMer: cyber-attacks automation and evaluation. IEEE Access, 8:129397-129414.

Faria, R. 2022. “Being” ethical in research. In: Qualitative research in criminology: cutting-edge methods. Cham: Springer International Publishing. pp. 229-240.

FortKnoxster. 2017. What is privacy and why does it matter? https://medium.com/fortknoxster/what-is-privacy-and-why-does-itmatter8648b2b8a297/ Date of access: 15 March 2021.

Fowler, G.A. 2019. It’s the middle of the night. Do you know who your iPhone is talking to? Washington Post, p. 28.

Franceschi-Bicchierai, L. & Coluccini, R. 2019. Researchers find Google Play Store apps were actually government malware.

Furletti, B., Trasarti, R., Cintia, P. & Gabrielli, L. 2017. Discovering and understanding city events with big data: the case of Rome. Information, 8(3):74.

Gamage, H.T.M., Weerasinghe, H.D. & Dias, N.G.J. 2020. A survey on blockchain technology concepts, applications, and issues. SN Computer Science, 1:1-15.

Garg, S., Kaur, K., Kaddoum, G., Garigipati, P. & Aujla, G.S. 2021. Security in IoT-driven mobile edge computing: new paradigms, challenges, and opportunities. IEEE Network, 35(5):298-305.

Gobo, G. 2023. Mixed methods and their pragmatic approach: is there a risk of being entangled in a positivist epistemology and methodology? Limits, pitfalls and consequences of a bricolage methodology. Forum: Qualitative Sozialforschung/Forum: Qualitative Social Research, 24(1). https://doi.org/10.17169/fqs-24.1.4005

Gordon, W.J., Landman, A., Zhang, H. & Bates, D.W. 2020. Beyond validation: getting health apps into clinical practice. NPJ Digital Medicine, 3(1):14.

Guamán, D.S., Del Alamo, J.M. & Caiza, J.C. 2021. GDPR compliance assessment for cross-border personal data transfers in Android apps. IEEE Access, 9:15961-15982.

Taherdoost, H. 2021. Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. International Journal of Academic Research in Management (IJARM), 10(1):10-38. hal-03741847

Hatamian, M., Serna, J. & Rannenberg, K. 2019. Revealing the unrevealed: mining smartphone users privacy perception on app markets. Computers & Security, 83:332-353.

Hayes, D., Cappa, F. & Le-Khac, N.A. 2020. An effective approach to mobile device management: security and privacy issues associated with mobile applications. Digital Business, 1(1):100001.

HELM Open. 2024. What is Pragmatism? University of Nottingham.

https://www.nottingham.ac.uk/helmopen/rlos/research-evidence-based-practice/d

Hildmann, H. & Kovacs, E. 2019. Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety. Drones, 3(3):59.

Hiza, D. 2022. Assessing the significance of CIA triad security model in establishing ICT security controls in the public sector. Institute of Accountancy Arusha (IAA). (Dissertation – PhD).

Hoofnagle, C.J., Van Der Sloot, B. & Borgesius, F.Z. 2019. The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1):65-98.

Huckvale, K., Torous, J. & Larsen, M.E. 2019. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. JAMA Network Open, 2(4):e192542-e192542.

Isa, M. 2019. SA suffers as cyber-crime rises globally. Sabinet African Journals, 22. https://hdl.handle.net/10520/EJC-19e6843605

Kapoor, M.C. & Goyal, R. 2023. Objectives and outcomes of a clinical trial. Indian Journal of Anaesthesia, 67(4):328-330. doi: 10.4103/ija.ija_215_23

Kaushik, V. & Walsh, C.A. 2019. Pragmatism as a research paradigm and its implications for social work research. Social Sciences, 8(9):255.

Kehdinga, G.F. 2020. Pure and applied research as the epicenter of research in engineering education. International Journal of Engineering Research and Technology, 13(9):2402-2408. doi:10.37624/IJERT/13.9.2020.2402-2408

Khatoon, A., Verma, P., Southernwood, J., Massey, B. & Corcoran, P. 2019. Blockchain in energy efficiency: potential applications and benefits. Energies, 12(17):3317.

Kim, J.H., 2017. Smartphone-mediated communication vs. face-to-face interaction: Two routes to social support and problematic use of smartphone. Computers in Human Behavior, 67, pp.282-291.

Kollnig, K., Shuba, A., Binns, R., Van Kleek, M. & Shadbolt, N. 2022. Are iPhones really better for privacy? A comparative study of iOS and Android apps. Proceedings on Privacy Enhancing Technologies, 2:6-24.

Kumar, P.R. & Gupta, R.S. 2022. Enhancing information security through the CIA triad: a systematic review. Computers & Security, 110:102453. Date of access: 28 July 2024.

Lakens, D. 2022. Sample size justification. Collabra: Psychology, 8(1):33267.

Lenarduzzi, V., Pecorelli, F., Saarimaki, N., Lujan, S. & Palomba, F. 2023. A critical comparison on six static analysis tools: detection, agreement, and precision. Journal of Systems and Software, 198:111575.

Li, H. & Yang, S. 2020. The impact of privacy threats on social media users: a review and solutions. Journal of Cybersecurity, 13(2):55-77.

Li, X. & Yang, Z. 2019. Security and privacy challenges in mobile application development. Journal of Mobile Computing and Security, 12(3):45-67.

Liginlal, D., Sim, I. & Khansa, L. 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers & Security, 28(3-4):215-228.

Naik, N., Jenkins, P., Grace, P. and Song, J., 2022, October. Comparing attack models for it systems: Lockheed martin’s cyber kill chain, mitre att&ck framework and diamond model. In 2022 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1-7). IEEE.

Junjie, M. & Yingxin, M. 2022. The discussions of positivism and interpretivism. Global Academic Journal of Humanities and Social Sciences, 4(1):10-14. https://www.gajrc.com doi:10.36348/gajhss.2022.v04i01.002

Malele, V. 2023. Cybersecurity cloud-based online learning: a literature review approach. Journal of Information Systems and Informatics, 5(4):1623-1632.

Malmqvist, J., Hellberg, K., Möllås, G., Rose, R. & Shevlin, M. 2019. Conducting the pilot study: a neglected part of the research process? Methodological findings supporting the importance of piloting in qualitative research studies. International Journal of Qualitative Methods, 18:1609406919878341. https://doi.org/10.1177/1609406919878341

Maroufkhani, P., Wagner, R., Wan Ismail, W.K., Baroto, M.B. & Nourani, M. 2019. Big data analytics and firm performance: a systematic review. Information, 10(7):226.

Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M. & Narayanan, A. 2019. Dark patterns at scale: findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW):1-32.

Mehta, N., Agashe, A. & Detroja, P. 2019. Swipe to unlock: the primer on technology and business strategy. Belle Applications.

Michael, T. 2019. Data privacy and security: why mobile apps are the new weak link. Infosecurity Magazine, 17 June. https://www.infosecurity-magazine.com/next-gen-infosec/privacy-mobile-apps-weak-link-1-1/

Miller, C.A., Guidry, J.P., Dahman, B. & Thomson, M.D. 2020. A tale of two diverse qualtrics samples: information for online survey researchers. Cancer Epidemiology, Biomarkers & Prevention, 29(4):731-735.

Moreno, J., Serrano, M. & Fernández-Medina, E. 2016. Main issues in big data security. Future Internet, 8(3):44. https://doi.org/10.3390/fi8030044

Moura, P., Fazendeiro, P., Inácio, P.R., Vieira-Marques, P. & Ferreira, A. 2020. Assessing access control risk for mhealth: a delphi study to categorize security of health data and provide risk assessment for mobile apps. Journal of Healthcare Engineering.

Mugadza, K. & Mwalemba, G. 2023. Online platform privacy policies: an exploration of users' perceptions, attitudes and behaviours online. South African Computer Journal, 35(2):78-96.

Nikkhah, H.R. & Sabherwal, R. 2022. Information disclosure willingness and mobile cloud computing collaboration apps: the impact of security and assurance mechanisms. Information Technology & People, 35(7):1855-1883.

Kowalczyk, N. & Truluck, C. 2013. Literature reviews and systematic reviews: what is the difference? Radiologic Technology, 85(2).

Ogbanufe, O. 2023. Securing online accounts and assets: an examination of personal investments and protection motivation. International Journal of Information Management, 68:102590.

Oliveira, A.C., da Silva, L.F., Eler, M.M. & Freire, A.P. 2020. Do Brazilian federal agencies specify accessibility requirements for the development of their mobile apps? In: XVI Brazilian Symposium on Information Systems. pp. 1-8.

O'Loughlin, K., Neary, M., Adkins, E.C. & Schueller, S.M. 2019. Reviewing the data security and privacy policies of mobile apps for depression. Internet Interventions, 15:110-115.

Padilla, V.S. & Freire, F.F. 2019. A contingency plan framework for cyber-attacks. Journal of Information Systems Engineering & Management, 4(2):2-7.

Park, Y.S., Konge, L. & Artino, A.R. 2020. The positivism paradigm of research. Academic Medicine, 95(5):690-694.

Patel, R.V. & Ng, L.Y. 2021. Developing a value-oriented framework for big data analytics in enterprises. Enterprise Information Systems, 15(4):305-322.

Perrotta, C., Gulson, K.N., Williamson, B. & Witzenberger, K. 2021. Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. Critical Studies in Education, 62(1):97-113.

Rains, T., 2020. Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks. Packt Publishing Ltd.

Rashidi, B. & Fung, C.J. 2015. A survey of Android security threats and defenses. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6(3):3-35.

Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., ... & Werner, J. 2020. Apps gone rogue: maintaining personal privacy in an epidemic (preprint).

Rawat, B.D., Chaudhary, V. & Doku, R. 2020. Blockchain technology: emerging applications and use cases for secure and trustworthy smart systems. Journal of Cybersecurity and Privacy, 1(1):4-18. https://doi.org/10.3390/jcp1010002

Reardon, J., Feal, Á., Wijesekera, P., On, A.E.B., Vallina-Rodriguez, N. & Egelman, S. 2019. 50 ways to leak your data: an exploration of apps' circumvention of the Android permissions system. In: 28th USENIX security symposium (USENIX security 19). pp. 603-620.

Reidenberg, J.R. & Schaub, F. 2018. Achieving big data privacy in education. Theory and Research in Education, 16(3):263-279.

Richter, F. 2021. Infographic: personal data: Instagram is a real tattletale. Statista Daily Data. https://www.statista.com/chart/24495/apps-sharing-personal-information-with-third-parties/ Date of access: 17 August 2023.

Seng, S., Al-Ameen, M.N. & Wright, M. 2021. A look into user privacy and third-party applications in Facebook. Information and Computer Security, 29(2).

Sarkar, S., Banatre, J.P., Rilling, L. & Morin, C. 2018. Towards enforcement of the EU GDPR: enabling data erasure. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE. pp. 222-229.

Schechner, S. & Secada, M. 2019. You give apps sensitive personal information then they tell Facebook. Wall Street Journal:82.

Serkan, A. 2009. Theories used in information security research: survey and agenda. In: The handbook of research on social and organisational liabilities in information security. IGI Global. doi:10.4018/978-1-60566-132-2.ch017

Sharma, A. & Sahay, S.K. 2019. Group-wise classification approach to improve Android malicious apps detection accuracy. arXiv preprint arXiv:1904.02122.

Shuba, A., Bakopoulou, E. & Markopoulou, A. 2018. Privacy leak classification on mobile devices. 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). https://doi.org/10.1109/spawc.2018.8445948

Skoll, D., Jennifer C., Miller, J.C. & Saxon, L.A. 2020. COVID-19 testing and infection surveillance: is a combined digital contact-tracing and mass-testing solution feasible in the United States? Cardiovascular Digital Health Journal:1-11.

Solove, D.J. 2010. Fourth amendment pragmatism. Boston College Law Review, 51:1511.

Song, D.W. 2021. What is research? WMU Journal of Maritime Affairs, 20:407-411. https://doi.org/10.1007/s13437-021-00256-w

Stardust, Z., Gillett, R. & Albury, K. 2023. Surveillance does not equal safety: police, data and consent on dating apps. Crime, Media, Culture, 19(2):274-295.

Taherdoost, H., Sahibuddin, S., Ibrahim, S., Kalantari, A., Jalaliyoon, N. & Ameri, S. 2012. Examination of electronic service definitions. 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT). https://doi.org/10.1109/acsat.2012.51

Talab, H.R. & Flayyih, H.H. 2023. An empirical study to measure the impact of information technology governance under the control objectives for information and related technologies on financial performance. International Journal of Professional Business Review, 8(4):25.

Talal, M., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Alsalem, M.A., Albahri, A.S., Alamoodi, A.H., Kiah, M.L.M., Jumaah, F.M. & Alaa, M. 2019. Comprehensive review and analysis of anti-malware apps for smartphones. Telecommunication Systems, 72:285-337.

Tan, B., Anderson Jr, E.G. & Parker, G.G. 2020. Platform pricing and investment to drive third-party value creation in two-sided networks. Information Systems Research, 31(1):217-239.

Telecominfo. 2012. The mobile app ecosystem – members & their functionality [Weblog]. https://telecominfo.wordpress.com/2012/03/02/the-mobile-app-ecosystem/ Date of access: 31 October 2023.

Thinkwithgoogle.com. 2022. https://www.thinkwithgoogle.com/marketing-strategies/app-and-mobile/smartphone-privacy-security-statistics/ Date of access: 31 October 2023.

Tipton, S.J., Forkey, S. & Choi, Y.B. 2016. Toward proper authentication methods in electronic medical record access compliant to HIPAA and C.I.A. triangle. Journal of Medical Systems, 40(4). https://doi.org/10.1007/s10916-016-0465-x

Tode, C. 2023. 5 legal issues that could impede mobile marketing's progress. Marketing Dive. https://www.marketingdive.com/ex/mobilemarketer/cms/news/legal-privacy/10035.html Date of access: 12 February 2023.

Trabucchi, D., Buganza, T. & Pellizzoni, E. 2017. Give away your digital services: leveraging big data to capture value. Research-Technology Management, 60(2):43-52. https://doi.org/10.1080/08956308.2017.1276390

Turner, A. 2021. Cell phone statistics, surveys & trade-in data [Blog post]. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world%20%20%E2%80%8C. Date of access: 31 October 2023.

Von Solms, R. & Van Niekerk, J. 2013. From information security to cyber security. Computers & Security, 38:97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wamba, S.F., Akter, S., Edwards, A., Chopin, G. & Gnanzou, D. 2015. How “big data” can make big impact: findings from a systematic review and a longitudinal case study. International Journal of Production Economics, 165:234-246. https://doi.org/10.1016/j.ijpe.2014.12.031

Wells, C. & Spry, C. 2022. An overview of smartphone apps. CADTH Horizon Scan. https://www.ncbi.nlm.nih.gov/books/NBK595384/

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D. & Beznosov, K. 2015. Android permissions remystified: a field study on contextual integrity. In: 24th USENIX Security Symposium (USENIX Security 15). pp. 499-514.

Wong, W.P., Tan, H.C., Tan, K.H. & Tseng, M.L. 2019. Human factors in information leakage: mitigation strategies for information sharing integrity. Industrial Management & Data Systems, 119(6):1242-1267.

Yang, W., Li, J., Zhang, Y. & Gu, D. 2019. Security analysis of third-party in-app payment in mobile applications. Journal of Information Security and Applications, 48:102358.

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. 2020. Hierarchically defining internet of things security: from CIA to CACA. International Journal of Distributed Sensor Networks, 16(1):1550147719899374. https://doi.org/10.1177/1550147719899374

Zhang, B., Chen, G., Ooi, B.C., Shou, M.Z., Tan, K.L., Tung, A.K., ... & Zhang, M. 2024. Managing Metaverse data tsunami: actionable insights. IEEE Transactions on Knowledge and Data Engineering.

Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y. & Qian, F. 2019. Dangerous skills: understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In: 2019 IEEE Symposium on Security and Privacy (SP). IEEE. pp. 1381-1396.

Zhou, L., Bao, J., Watzlaf, V. & Parmanto, B. 2019. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR mHealth and uHealth, 7(4):e11223.

Zhou, W., Zhou, Y., Jiang, X. & Ning, P. 2012. Detecting repackaged smartphone applications in third-party Android marketplaces. In: Proceedings of the second ACM conference on Data and Application Security and Privacy. pp. 317-326.

APPENDIX A

QUESTIONNAIRES

Questionnaire for a Master's Degree Study

School for Computer Science and Information System

Dear Participant

This questionnaire is part of the research study conducted by Mr LK Mphasane (orcid.org 0009-0002-3538-0608) for a MSc in Computer Science and Information Systems degree under supervision of Dr V Malele at the Unit of Data Science and Computing, School of Computer Science and Information Systems, Faculty of Natural and Agricultural Sciences Vanderbijlpark Campus of the North-West University.

The title of the study is Recommendations for safeguarding mobile users from violation by third-party applications. It aims to offer recommendations for protecting mobile users against being violated by third-party applications. In this regard, you are request to participant in this study by responding to this questionnaire with non-biasness and favour. The questionnaire establishes a baseline understanding of the users' mobile app usage habits related to security and privacy issues.

Gender						
Female						
Male						
Age Range						
20-30yrs						
31-40yrs						
41-50yrs						
51-60yrs						
>61yrs						
Please indicate which mobile device do you own?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Smartphone						
Tablet						
Laptop						
Please indicate the number of years you owned a mobile device.						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
<1yr						
1yr < 2yrs						
2yrs < 3 yrs						
>3yrs						

1. Do you know what a digital mass technology is?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						

2. Which of digital mass technologies have you been exposed to?														
	Facial Recognition Cameras				QR Codes				Location-tracking					
	A	N	D		A	N	D		A	N	D			
Learners														
Students														
Teachers														
Lecturers														
Professionals														
Unemployed														

3. Do you know and understand the following four digital mass surveillance indicators?															
	Privacy				Transparency				Oversight				Accountability		
	A	N	D		A	N	D		A	N	D		A	N	D
Learners															
Students															
Teachers															
Lecturers															

Professionals																	
Unemployed																	

4. Do third-party apps profile you when you interact with:																		
	Facebook			TikTok			Tinder			WhatsApp			Checkers60sec			Uber Eats		
	A	N	D	A	N	D	A	N	D	A	N	D	A	N	D	A	N	D
Learners																		
Students																		
Teachers																		
Lecturers																		
Professionals																		
Unemployed																		
	Shein			KFC			Showmax			YouTube			Prime Video			Netflix		
	A	N	D	A	N	D	A	N	D	A	N	D	A	N	D	A	N	D
Learners																		
Students																		
Teachers																		
Lecturers																		
Professionals																		
Unemployed																		

5. Do you think the third-party apps:-																		
	use your data without consent									**misuse your data**								
	A			N			D			A			N			D		
Learners																		

Students																		
Teachers																		
Lecturers																		
Professionals																		
Unemployed																		

6. Do you think third party-apps violates your						
	Confidentiality			**Privacy**		
	A	N	D	A	N	D
Learners						
Students						
Teachers						
Lecturers						
Professionals						
Unemployed						

7. Do you think there is a need to safeguard users against violations of third party-apps?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						

8. Are you aware that the third-party apps are tracking your presence?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						

Not Sure						
Disagree						
9. Do prefer that third-party apps should track your presence?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						
10. Are you concerned about data collection by third-party apps						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						
11. Do you use anti-virus on your mobile device?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						
12. Do you use password to lock your screen?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						

13. Do you access internet using unsecured connections?						
	Learners	**Students**	**Teachers**	**Lecturers**	**Professionals**	**Unemployed**
Agree						
Not Sure						
Disagree						

APPENDIX B

Private Bag X6001, Potchefstroom
South Africa 2520
Tel: +2718 299-1111/2222
Web: http://www.nwu.ac.za
Research Data Gatekeeper Committee

NWU RDGC PERMISSION GRANTED LETTER

Based on the documentation provided by the researcher specified below, on 13-October-2023 the North-West University (NWU) Research Data Gatekeeper Committee (NWU-RDGC) hereby grants conditional permission for the specific project (as indicated below) to be conducted at the NWU:

Project title: Recommendations for safeguarding mobile users from violation by third-party applications.

Project leader: Vusumuzi Malele

Researcher/Project Team: Mr. Letsholo Kagiso Mphasane

Ethics reference no: NWU-01304-23-A9

NWU RDGC reference no: NWU-GK-23-186

Specific Conditions:

1. The researcher on the questionnaire requests the age of the participants. Please provide justification for this and clarify how will confidentiality be ensured when reporting.
2. Please provide more clarity on how the recruitment process and consenting process will be done.

Approval date: 13-October-2023 Expiry date: 13-October2024

General Conditions of Approval:

- The NWU-RDGC will not take the responsibility to recruit research participants or to gather data on behalf of the researcher. This committee can therefore not guarantee the participation of our relevant stakeholders.
- Any changes to the research protocol within the permission period (for a maximum of 1 year) must be communicated to the NWU-RDGC. Failure to do so will lead to withdrawal of the permission.
- The NWU-RDGC should be provided with a report or document in which the results of said project are disseminated.

APPENDIX C

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	LK MPHASANE
Assignment title:	Turnitin-External
Submission title:	Dissertation_Final_Pliagrism_Version.docx
File name:	Dissertation_Final_Pliagrism_Version.docx
File size:	1.54M
Page count:	96
Word count:	26,858
Character count:	153,753
Submission date:	27-Jul-2024 10:06PM (UTC+0200)
Submission ID:	2423134002

Dissertation_Final_Pliagrism_Version.docx

ORIGINALITY REPORT

13%	11%	5%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

APPENDIX D

MAGRIET ENGEL COACHING

6 August 2024

L.K. MPHASANE
North-West University

Dear Sir/Madam

Declaration of language editing

I, Magrietha Maria Engelbrecht, hereby declare that I personally read through the dissertation:

Recommendations for safeguarding mobile users from violation by third-party applications

by **L.K. MPHASANE** in July/August 2024 and highlighted language errors.

Yours sincerely

6 August 2024