The impact of the Protection of Personal Information Act on online consumers' privacy concerns

Panki Patrick Mosakoa

0406760R

WITS Business School

A research article submitted of the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration.

Johannesburg, 2023

Protocol number: WBS/BA0406760R/767

DECLARATION

I, Panki Patrick Mosakoa, declare that this research report entitled “The impact of the recent Protection of Personal Information Act on online consumers’ privacy concerns” is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Panki Patrick Mosakoa

Signed at Johannesburg on 28 February 2023

SUPPLEMENTARY INFORMATION

Nominated journal: International Journal of Business and Economics

Supervisor/Co-author: Dr Rukudzo Pamacheche

Word Count: 19740

Supplementary files:

Appendix 1 – Informed Consent

Appendix 2 – Sample of Questionnaire

ABSTRACT

Globally, consumer privacy remains a major concern when shopping online and merchants are collecting and using personal information. However, many nations have been responding with personal data protection laws to protect individuals' human rights to privacy. In South Africa, the government introduced the Protection of Personal Information Act (POPIA) in 2013 and fully enacted in July 2020. This study aimed to investigate the impact of POPIA on online shoppers' privacy concerns by examining consumer privacy concerns before and after POPIA was introduced and also determine the extent to which knowledge of POPIA has influenced online privacy concerns. A quantitative methodology using descriptive statistics and hypothesis testing was adopted to guide the analysis of data collected from a random sample drawn from students of one South African university using a pre-designed questionnaire. The results support the hypothesis that online shoppers' privacy concerns have not changed before and after the POPIA enactment. The descriptive statistics revealed that online shoppers lack knowledge of POPIA and still have concerns about the safety of their personal information, credit card and identity information theft, and impostor online organisations. With increased data breaches and deliberate information disclosure, these concerns prevent consumers from shopping online because of personal information safety fears. It is recommended that policymakers introduce more awareness campaigns and case laws of the legislation to the public. Organisations can invest more in employee training and development initiatives on POPIA regulations, POPIA compliance on internal systems, and online platforms to sensitise staff and minimise possible litigation.

Keywords: POPIA, online shoppers, privacy concerns, personal information protection

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

DEDICATIONS

I dedicate this research work to my family, my loving wife Boitumelo, and our son Bokang Mosakoa. To whom I love dearly and truly acknowledge, and appreciate their support during the difficult and demanding time spent in doing this MBA qualification.

ABBREVIATIONS AND ACRONYMS

ANOVA	Analysis of Variance
AU	African Union
BRC	British Retail Consortium
CCTV	Closed Circuit Television
CPA	Consumer Protection Act
CRSA	Constitution of the Republic of South Africa
DOJ&CD	Department of Justice and Constitutional Development
DPA	Data Protection Act
ECTA	Electronic Communications and Transactions Act
EU	European Union
FIP	Fair Information Practice
GDPR	General Data Protection Regulation
HELM	Home Energy & Lifestyle Management
ICO	Information Commissioner Officer
ID	Identity Document
IT	Information Technology
PAIA	Promotion of Access to Information Act
PI	Personal Information
PIFM	Personal Information Flow Model
POPIA	Protection of Personal Information Act

RSA	Republic of South Africa
SPSS	Statistical Package for the Social Sciences
TAM	Technology Acceptance Model
TRAM	Technology Readiness and Acceptance Model
TV	Television
UK	United Kingdom
URL	Uniform Resource locators
USA	United States of America
WBS	Witwatersrand Business School

1 INTRODUCTION TO THE RESEARCH

1.1 Background

Consumers globally using the internet perceive privacy as a general concern. Consumers are concerned about how corporates use and collect their data. However, in recent years, lawmakers globally have been enacting and enforcing privacy laws to mitigate privacy concerns by consumers using the internet. According to Botha et al. (2017), regulations on personal information protection are increasing globally. At least 120 new data laws have been introduced at a rate of 2 new nations per year between 1973 and 2017 (Greenleaf, 2017). Within the European Union (EU) countries, a privacy law called General Data Protection Regulation (GDPR) was approved and enacted into law in May 2018 (Hoofnagle, der Sloot & Borgesois, 2019). The GDPR is aimed at the personal data processing of individuals. Similarly, the United States of America (USA) introduced the Fair Information Practice (1973) and the United Kingdom (UK) brought the Data Protection Act (DPA) (1998) to regulate personal information processing and privacy rights. A similar trend has followed in Asia with countries such as India and Thailand, and in South America in countries like Brazil and Chile also recently approved privacy laws. Whilst, the exact information contained in each of these privacy laws differs, the common objective is increasing personal privacy and giving individuals control over their personal information (Onetrust DataGuidance, 2021).

According to Abdulrauf and Fombad (2016), Africa is lagging when compared to other continents in respect of individual privacy law adoption. As such, researchers (Mutimukwe, Kolkowaska & Gronland, 2019; Zenda, Vorster & da Viega, 2020) argue that in African nations, more work should be done to regulate personal information privacy violations since only 37% of African nations' have information privacy regulations. However, the African Union continues to increase the initiatives to compel its member countries to introduce data privacy regulatory frameworks (Ball, 2017).

In South Africa, the trend of privacy laws was operationalised in 2013 with the approval of the Protection of Personal Information Act (POPIA). The POPIA seeks to

protect individuals' constitutional rights to privacy. This is under The Constitution of the Republic of South Africa (RSA) which gives all citizens the right to privacy. Thus, de Bruyne (2014) argues that the POPIA was enacted to protect individual privacy rights under the country's constitution which states that "everyone has the right to privacy". However, technology is vigorously evolving, especially the devices and applications that are being introduced by various organisations such as smartphones, mobile computers, social media (Instagram, WhatsApp, Facebook, and Twitter), and the internet. The digital world is under attack as individuals' personal information is easily accessible while being stored digitally (Sekgweleo & Mariri, 2019). As a result, it has become easier to access people's personal information without their permission. Once this information is stolen or hacked it can cause harm to both individuals and organisations.

This research is about internet users that do online purchasing of any goods or services in South Africa (SA). These consumers must share some level of personal information (PI) for these online purchases. SA is regarded as a country in which regulation and enforcement are moderately applied (DLA Piper, 2018). As a consequence, massive data breaches of PI of South Africans were reported during the last five years. The data breach has grown to an average cost of R46 million per annum in SA (isite Computers, 2021). Several cases of data breaches include the 60 million SA citizens' identity number breach (Fihlani, 2017), Liberty insurance email ransom request, 943,000 SA drivers PI breach (Malinga, 2018), Experia credit bureau data leak of 800,000 local businesses and 24 million SA citizens (Isite Computers, 2021). Therefore, in these instances, data compromises the security of individuals leading to accidental or illicit, destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed (Sekgweleo & Mariri, 2016). In addition, privacy concerns for personal information protection during online shopping have been found to harm online shoppers' intentions to make purchases online (Jordan et al., 2018).

1.2 Context

The study is conducted against worsening consumer concerns about their privacy by corporates that continue to collect personal data and fail to protect that information from unauthorised environments. Consequently, consumers' security is compromised when sensitive and confidential personal data collected by companies are exposed to criminals. The study is therefore evaluating the extent to which POPIA is effective in protecting South African consumer privacy concerns using the internet and how consumers perceive the Act.

1.3 Research conceptualisation

1.3.1 Problem statement

The vigorous and continuous evolution of technology has increased the pressure on personal information's easy accessibility whilst being stored digitally. According to Schatz and Bashroush (2016), Isite Computers (2021), and Zenda et al. (2020), cases of data breaches increase when, through accident or deliberate means, confidential and secured data is released into untrusted environments. Post-POPIA introduction, online shoppers' rights to privacy continue to be compromised when their confidential and private information ends up in an untrusted environment. Issues of fear of identity theft, impersonation, and overall mishandling of personal information remain persistent.

1.3.2 Purpose statement

The purpose of this quantitative cross-sectional study is to measure the impact of POPIA on online shopping consumers' privacy concerns. The study uses descriptive statistics and hypothesis testing to ascertain whether consumer perceptions about their privacy changed before POPIA was enacted and after POPIA became law. In this way, the privacy concerns of consumers and the extent to which POPIA has been effective to protect consumer information are understood.

1.3.4 The aim of the research

The main aim of the study is to find out if the introduction of the South African Protection of Personal Information Act has had an impact on privacy concerns for personal information online shoppers share when making online purchases.

1.3.4 Research objectives and questions

Objectives for this research:

- To explore general privacy concerns online shoppers had before the POPIA became effective.
- To analyse the effects of the POPIA on online shoppers' concerns about personal information gathered during online purchases.
- To determine the extent to which knowledge of the POPIA has reduced online privacy concerns.

The research questions for the study:

- What privacy concerns for personal information data do online shoppers have when making online purchases?
- Has the introduction of the POPIA changed privacy concerns regarding personal information disclosed while shopping online?
- Has consumer knowledge of the POPIA reduced online privacy concerns among online shoppers?

1.4 Delimitations and assumptions of the research study

Theofanidis and Fountouki (2019) define delimitations as limitations intentionally set by the author/s himself/herself to limit the scope of their research. Thus, given this definition, the delimiting factors for this study were a sample limited to the University of Witwatersrand students and the use of an online survey. It was assumed respondents answered the questions with honesty and truthfulness, were aware of online shopping and POPIA existence, and the research findings are an accurate correlation and inference position of the respondents' views within an acceptable margin of error.

1.5 Significance of the research study

This study navigates how POPIA influences privacy matters encountered by online shoppers. However, the personal decisions by shoppers are based on weighing benefits against risks, and the perceived control they have on personal information as protected by POPIA (Baloyi & Kotze, 2017). This study's significance within the body of knowledge lies in the result of the level of POPIA privacy protection using the lens of online shoppers' perceptions of the prior-POPIA and post-POPIA periods. The model used for this study, adapted from Al-Fedaghi (2006), adds value by permitting the exploration of the correlation between consumer POPIA knowledge and privacy concerns among related variables and constructs.

1.6 Organisation of the research report

Listed below are the chapters in this research report:

Chapter one: Introduction:

This chapter gives the background and context of the study and then goes on to state the research problem, purpose statement, objectives, questions, delimitations, assumptions, and significance of the study.

Chapter two: Literature review:

This chapter serves to provide a holistic literature review of the problem, the past studies, and the conceptual framework.

Chapter 3: Methodology:

This chapter discusses research strategy, design, procedures, reliability, and validity measures as well as limitations.

Chapter 4: Data Findings:

This chapter presents the empirical results obtained from the collected data.

Chapter 5: Data Analysis:

This chapter is a deep analysis of the data findings about the interrogation of the research questions, leading to the conclusions of the study.

Chapter 6: Summarises and concludes the research:

This chapter gives a summary of the research, conclusions, contributions of the study and ends by giving recommendations to practice and management.

2 LITERATURE REVIEW

2.1 Introduction

This chapter provides an in-depth discussion of concepts on privacy concerns for personal information protection and the RSA POPIA, and the impact of the act on privacy concerns based on past studies, theories, and legal documents. The discussion includes the agreements and disagreements within the body of knowledge and a highlight of the gaps in the literature that this study intends to fill. The chapter ends with a conceptual framework that guides the research process.

2.2 Theoretical concepts and foundation

2.2.1 Online shopping concept

Online shopping is also known as e-commerce and is defined by Daroch et al. (2021, p.39) as the act of purchasing a product or a service over the internet directly from a seller without any intermediary. Aseri (2021) further argues that product purchasing through online platforms has become popular because of the convenience that it brings given that the consumer has access to the product regardless of their location. (*ECommerce Market South Africa - Data, Trends, Top Stores*, n.d.) lists South Africa at number 41 in e-commerce markets of the world in 2021, and it had a revenue of five billion US dollars in the same year with an expected growth rate of 8% for the next 4 years.

According to Rudansky-Kloppers (2014), the advantages of online shopping include convenience as the main one and also being able to shop from anywhere, home or work, time-saving factor for online shopping since travel and queueing are eliminated, elimination of trading hours, online shopping is 24-7, 365 days, ease of product browsing and comparison of prices amongst multiple stores, and available options for methods of payments and where products can be delivered to. However, Rudansky-Kloppers (2014) also states that a major reason why many online consumers choose not to engage in online shopping is that they fear being defrauded or their credit card information being stolen. Yet, according to Vasić, Kilibarda, and Kaurin (2019), the disadvantages of online shopping include: a perceived lack of security for online shopping, shoppers are unable to physically see

or try the product first to make judgments on its actual characteristics before making the purchase.

2.2.2 Personal Information concepts through Moore's theory

According to Veiga et al. (2019), online shoppers have specific hopes when sharing their data with companies. However, with POPIA in place, organisations, on the other hand, have a legal responsibility when processing consumer information. Miltgen, Henseler, Gelhard, and Popovič (2016) refer to the social contract of privacy as when a consumer provides their personal information to an organisation. Furthermore, Miltgen et al. (2016) argue that a breach of this social contract occurs when the organisation shares the personal information of the consumer with third parties or does not give the consumer the option to decide how the information is to be used. However, the POPI Act exists to protect consumers or individuals from the breach of this social contract of privacy.

The POPIA (2013, p.14) regulation defines personal information as any data that allow an information user to recognise a data subject who can be a justice or natural person. Such data about an individual includes telephone number, email address, online identifier, beliefs, disability, religion, ethnic background, pregnancy, sex, gender, health, marital status, and race (POPIA, 2013, p.14). Similarly, De Bruyn (2014, p.1315) defines personal information as any information that has the following attributes that enable the information user to identify the data subject with regards to information related to race, gender, sex, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, health data, well-being, disability status, religion, belief, culture, language, and the birth of the person; information related to the education or the medical, financial, criminal, or employment history; any identifying number and symbols such as email address, physical address, telephone number, geo-location, and online identifier; and any biometric information.

Al-Fedaghi (2006, p.158), defines a personal information theory using the following model:

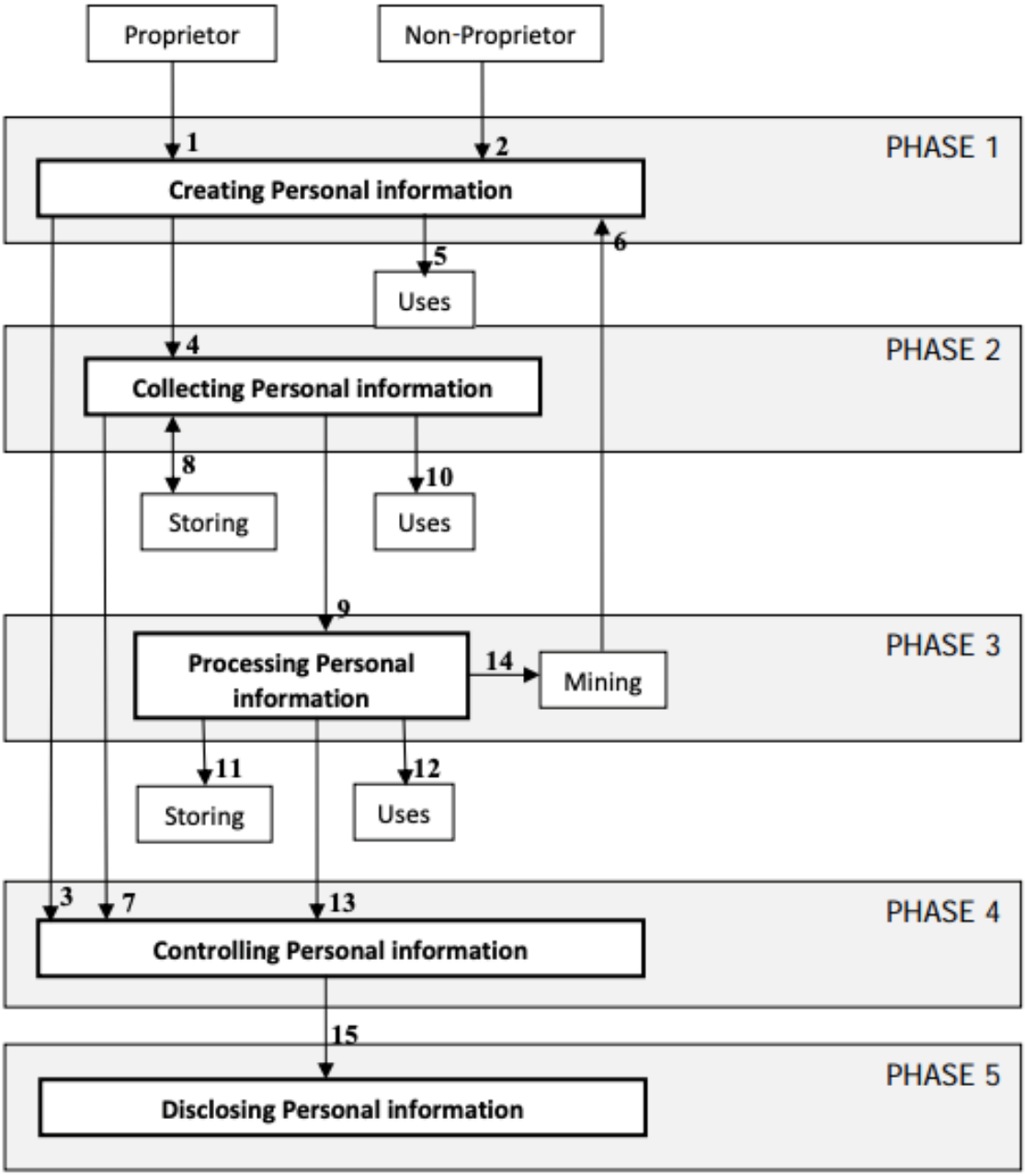

Figure 1: Personal Information Flow Model

Source: (Al-Fedaghi, 2006, p.158)

The Personal Information Flow Model (PIFM) by Al-fedaghi (2006), which depicts the five phases of how individual data is disclosed, controlled, processed, collected, and created, can virtually be used to define the protection of personal information. Baloyi and Kotze (2017) contend that the volumes at which personal information is collected, shared, and processed has increased enormously, therefore the risk to privacy has become critical. The PIFM states that any individual data disclosure

must be disclosed to authorised users only within a restricted time and certain usage (Al-Fedaghi, 2006). Disclosing individual data means that the data is to be given to other parties, and those parties can be either internal or external, known, or unknown (Ghani & Sidek, 2009).

Similarly, Ghani and Sidek (2009, p.12) define individual data privacy as a person's claim to control the conditions under which the data attributable to a person is used, disclosed, and acquired. Dv (2022) also argues that information privacy is how an individual has control over their personal information. The protection of personal information is concerned with the security and protection of personal details against people who might use it unlawfully. Since we are living in the technological era personal information can be easily stolen and used without your concern.

According to Appel, Grewal, and Hadi (2020), personal information can be collected and administered by various companies once people purchase products or services, post and share their information on social media platforms, or when people enter their details in competitions. Electronic devices are permitting a vast amount of individual information to move in various platforms without knowing it (Livingstone, Stoilova & Nandagiri, 2018). As a result, the right to privacy is violated. Individuals have little or no control over how their data is stored or used. Therefore, mishandling personal information such as administrating, storing, using, collecting, and exchanging can violate human rights (Martin, Borah & Palmatier, 2016).

This study is underpinned on the social contract theory of privacy by (Martin, 2016). In the social contract theory of privacy implementation, a company that collects individual data is regarded as fair, if the owner of such information is given control over their data and consulted every time the company wants to make use of such information (Martin et al., 2016). Within data privacy, the social contract arises when agreeing parties reach a consensus about how personal data is to be shared or utilised (Martin, 2016). As such, the social contract theory gives specific guidelines on client personal data sharing and exchange to guide against potential harm or risk to the client (Martin & Murphy, 2017). Therefore, when consumers buy online and leave their information with the organisation based on the social contract, the data subject remains with control over how their personal information is shared or utilised.

2.3 POPIA

2.3.1 Overview of the POPI Act

Countries around the world have legislations in place to secure and protect personal information. In South Africa the Protection of Personal Information (POPI) Act 2013 was signed into law in November 2013 (POPIA, 2013). The Act describes personal information as any information concerning an identifiable, living, natural, or juristic person. Section 9 of the Constitution of South Africa asserts that information should be processed in a manner that promotes confidentiality and does not hinder the right to privacy (de Bruyn, 2014). In addition, the SA Constitution Section 14, gives rights to individual privacy (RSA Government, 1996). Hence, the POPIA (2013) was brought into law to further regulate individual rights to privacy by giving individual data protection when given to other responsible parties (De Bruyn, 2014).

The sections of the POPI Act were enacted in phases from 2013 until 1 July 2020. The information regulator was only appointed on 7 September 2016, and on the issuance of final sections, companies were given a one-year grace period to align processes and comply with the POPIA provisions by 30 June 2021 (POPIA. n.d.). The start date of sections 113, 112, and section 1(a) (v) was 11 April 2014 and on 1 July 2020, all other sections were enacted excluding sections 114(4) and 110. (POPIA,n.d.).

The POPIA Act guides organisations and individuals and sets on how personal information must be handled. The POPIA (2013, p.15) defines data subjects as “someone to whom the individual data is owned”. Responsible parties are public or private entities or individuals who decide the manner or purpose in which personal data is to be handled (POPIA, 2013, p.15). POPIA (2013) consists of eight conditions that one must have satisfaction with before individual data is handled legitimately, as shown in Table 1.

Table 1: Eight conditions of POPIA as adapted from RSA Government (2013)

Condition	Description
Accountability	The Act prescribes that it is the onus of the responsible party to establish an environment that facilitates the lawful processing of personal information.
Processing limitation	The Act specifies that the processing of personal information can only commence if the purpose specifies the required information for an activity to be accomplished. The information should be sourced from the data subject directly.
Purpose specification	The Act specifies that information of a personal nature should be collected for a lawful, specific and clearly spelt-out purpose related to the mandate of the responsible party.
Further processing limitation	Further processing of information must be directly linked with the purpose of collection as per the initial agreement with the data subject.
Information quality	The responsible party has to guarantee that personal information is accurate, complete and not misleading.
Openness	It should be brought to the attention of individuals that a responsible party is collecting personal information from them.
Data subject participation	POPIA specifies that a data subject should be allowed to access information that they have supplied and be able to make corrections to it.
Security safeguards	It is the onus of the responsible party to put in place measures that ensure that the confidentiality and integrity of the information is preserved.

Source: Zenda et al. (2020, p.118)

These conditions were found to be in harmony with those of other nations with privacy laws (Botha et al., 2017). Additionally, the conditions also include provisions to do with unsolicited e-commerce communication and direct marketing (Zenda et al., 2020).

2.3.2 Consequences for violation of the POPI Act

The violation of the POPI act can be a punishable offence in South Africa. The Act permits individuals to institute civil proceedings in certain circumstances if there has been an interference with the protection of their personal information (Swartz & Da Veiga, 2016). According to POPIA (2013) chapter 11 (offences, penalties, and administrative fines), the Information Regulator may enforce imprisonment of fewer than 10 years or a fine of up to R10 million or a combined imprisonment and a fine, for violation of the Act (POPIA, 2013). The Act is fully operational and court cases have been held enforcing the provisions of the POPIA. This involves “balancing the right to privacy against other rights, particularly the right of access to information; and protecting important interests, including the free flow of information within the Republic and across international borders” (de Bruyn, 2014, p.159).

Further clarity is afforded in POPIA (2013) section 3(1) (a), which applies to individual data processing by responsible parties who make use of non-automated or automated data. This means the Act extends to individual data also processed in manual form and not only on the internet, as long as it is part of the official filing system of the responsible party. In addition, POPIA (2013) takes a modern, encapsulating perspective, since across the country's borders, individual data flows freely. POPIA (2013) Section 3(1) (a) thus stipulates that it applies to individual data handling where the responsible parties are (a) "domiciled in the Republic; or (b) not domiciled in the Republic but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic."

Empirical studies on POPIA compliance include a study by Zenda et al. (2020) on compliance with POPIA by insurance companies, it was found that 92% of the sample were not complying with POPIA provisions on sending direct marketing material to individuals without obtaining prior consent, and sharing information with third parties. This shows that most companies are not complying with POPIA. In another study by Parker and Flowerday (2021), it was found that personal information users can disregard online shoppers' privacy concerns because of apathetic and resigned behaviour towards privacy. However, organisations with more awareness tend to value individual data when they have encountered privacy violations before encouraging them to protect consumers' confidential data (Zenda et al., 2020). Nevertheless, no studies were found that measure the relationship between POPIA knowledge and online shopping privacy concerns. Hence, the need for this study to investigate the impact of POPIA on online consumer privacy concerns in South Africa.

2.3.3 Right to privacy and data protection

The table summarises the main privacy principles in the POPIA.

Table 2: POPIA main privacy principles

No.	Core Principle
1	*Collection*: Private data collection may only be done in ways that is fair, lawful and with the knowledge and consent of the data subject.
2	*Data quality*: Private data collected must be accurate and relevant.
3	*Purpose specification*: Private data may only be collected for a specific use and the purpose must be specified at collection time.
4	*Purpose and rights notification*: Data subjects must be notified that their data will be collected and for what purpose it will be used.
5	*Uses*: The personal data may only be used or processed for the purposes that the data was originally collected, i.e. excessive processing is prohibited.
6	*Reasonable security safeguards*: The necessary technical and procedural practices should be implemented to ensure the safety of the personal data.
7	*Individual's access and correction*: Data subjects have the right to know what information on them is stored and processed by the responsible party / data controller. The responsible party / data controller have a responsibility to affect any corrections if the data subjects inform them thereof.
8	*Accountability*: It is the obligation of the responsible party / data controller to implement and monitor adherence to the conditions of the act.
9	*Data export restrictions*: Data transfers to countries may only be done to countries that have adequate data privacy legislations in place.

Source :(POPI, 2013)

Data privacy is regulated by the POPI Act of 2013 (Dv, 2022). POPIA is a South African federal data protection law enacted to protect people's privacy. This Act outlines restrictions and legalities of when an entity such as a company or individual can process another entity's personal information. As shown in Table 1, conditions for the lawfulness to process personal information by or for a responsible party are accountability, processing limitation, further processing limitation, information quality, openness, security safeguards, and data subject participation (Parker & Flowerday, 2021).

Individuals and organisations benefit from the POPI act because it regulates personal information protection. According to Martin and Murphy (2016), when a business can demonstrate to its customers that it is POPIA compliant, then customer relationships and trust are improved. In the effort to meet POPIA compliance, organisations are forced to analyse and review their databases in an effort of ensuring the personal details of their customers are correct and still relevant (Parker & Flowerday, 2021). This further improves the quality of data they keep being able to guarantee the privacy and compliance of their customer's data, and organisations

gain a competitive advantage (Martin & Murphy, 2016). POPIA empowers online shoppers or any other party to whom the personal information relates or belongs, to be able to hold any organisation accountable for the responsible safekeeping of their personal information. Thus, online consumers' privacy concerns are therefore reduced (Parker & Flowerday, 2021). POPIA (2013) gives legal data protection to an individual or corporate body as it relates to the personal data processing by another organisation or individual person.

2.4 Consumer personal information concerns before and after POPIA

2.4.1 Privacy paradox

Online consumers shop with their preconceived privacy concerns and some level of expectations towards the protection of their data. This discrepancy between their expectations and their behavioral approach toward how online consumers manage their data creates the so-called privacy paradox.

According to Dv (2022), privacy concerns on personal information arise when an individual or owner of that data believes that they do not have adequate control over their data. In most countries, information privacy is regulated by data-protection laws which legally obligate controllers or custodians of the data to implement privacy controls over the data they keep, process, or disclose. Therefore, the owners of the data rely on these information privacy protection laws and principles and expect organisations that handle or come across their data to uphold them. If there is a slight hint or let-down suspected on those expectations, then privacy confidence would decline. Before, POPIA, there was no specific Act dealing with data privacy protection in South Africa (Viega et al., 2019).

However, researchers (Dienlin & Trepte 2015; Norberg, Horne, & Horne, 2007), argue that online shoppers may be subjecting themselves to "the privacy paradox"; that is, they "claim to value their data privacy while simultaneously acting in ways that compromise their privacy" (Palmatier & Martin, 2019, p.9). A vital meaning of the privacy definition is the integrity context which reflects the key difference between "giving up" privacy rights and "giving up" personal data (Martin & Nissenbaum, 2016), a central element that also explains the privacy paradox (Palmatier & Martin,

2019). However, when online shopper shares their individual information, they are not giving up their right to privacy as they perceive an appropriate data flow to permeate within that specific context (Martin & Nissenbaum, 2016). Hence, the privacy calculus model proposes that responsible parties are always weighing the disclosure costs against related benefits to gauge whether to disclose the confidential information they keep on their clients (Krasnova, Spiekermann, Koroleva & Hildebrand, 2010). This means users only disclose personal data that brings benefits to themselves in the long term. Yet, in other moments, these users can see that the data disclosure benefits are exceeded by the risk of comprising online shoppers' privacy (Dinev & Hart, 2006). Thus, according to Acquisti, Brandimarte & Loewenstein (2015), these information users can be misguided by benefits and risk perceptions balance discrepancies.

A few researches have shown that online shoppers' privacy concerns are increasing because of inadequate data privacy protection when trading online (Daroch et al., 2021). A web user survey found that almost 95% of the users refused to give their data to websites when such data was requested (Madden & Raine, 2015). In a study by Gurung and Raja (2016), it was found that privacy and security concerns and trust beliefs had effects on risk perception of online shopping transactions to either stop them or worry about making online purchases. Similarly, a study by Fortes and Rita (2015) also found that privacy concerns on the Internet harm various beliefs about the use of electronic commerce. However, contrary to this, a study by Cvach, Kahsay, and Shamoun (2018) found that even though consumers have privacy concerns this does not stop them from transacting.

2.4.2 Personal information protection concerns

Before POPIA (2013) became law in SA, there was no extensive data protection regulation; privacy matters were dealt with using the Constitution and common law (POPIA, n.d). This means that only delictual and common law remedies were available to individuals who experienced an infringement to their privacy (Parker & Flowerday, 2021). However, other notable personal information legislation includes the Consumer Protection Act (CPA), the Electronic Communications and

Transactions Act (ECTA), and the Promotion of Access to Information Act (PAIA), (Lee, 2021).

Post-POPIA, grants individuals numerous rights relate to individual data and its' usage. Chapter 3 of the Act stipulates lawful personal information processing (POPIA, 2013). The Act also gives rights to notification for unauthorised collection, access, or acquisition of their individual information (Naude, 2015). Additionally, individual data subjects have the right to request responsible parties to give them access to their data (POPIA, 2013). Moreover, a data subject has the right to request, where necessary, the correction, destruction, or deletion of personal information. POPIA also permits individuals to refuse the processing of their confidential data (POPIA, n.d.)

Recent court cases have shown, the reliance and enforcement of POPIA against organisations in breach of the law. A case in point is the Black Sash Trust v Minister of Social Development (2017), the Constitutional Court agreed with the Information Regulator that personal information belongs to its owners and responsible parties have no right to transfer such data to other parties (Sheik, 2018). Similarly, in the case of Discovery vs Liberty judgment (2020), on information ownership, the judgment added weight to the argument that the owner of personal data and not the responsible parties possess their individual information (Giles, 2020). This means the data protection law i.e. POPIA gives individuals control and protection of their data.

2.4.3 Security concerns

Theories on Technology Acceptance Model (TAM) or Technology Readiness and Acceptance Model (TRAM) always highlight insecurity as an important factor that makes online consumers not adopt or reject technology and the feelings of insecurity related to technology are on the other hand associated with ambiguity and low usage (Panday, 2018). According to Aseri (2021), insecurity is a mental inhibitor to online consumers' acceptance of new technologies. Smit, Roberts-Lombard, and Mpinganjira (2021, p.2), define this online consumer insecurity as a "distrust of technology and scepticism about its ability to work properly".

Consumers have great concerns about data breaches or accidental information disclosure. The breach of data is the deliberate or accidental release of secured and confidential information to an untrusted environment (Schatz & Bashroush, 2016). Accidental information disclosure refers to data leaks and also data spills (Seh et al., 2020). Romanosky Hoffman and Acquisti (2014) indicated that there is an International Standards Organisation that describes data breach as a compromise of security that leads to the accidental or illicit, destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed. As such since 2005, an estimated 543 million records have been lost from over 2,800 data breaches, and the identity theft caused $13.3 billion in consumer financial loss (Kongso, 2015).

However, with the advent of POPIA, notification must be made in the event of a data security breach. This is activated by Section 24 of POPIA (2013) which hold that, “where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator; and subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.” The notification should occur “as soon as reasonably possible after the discovery that information has been compromised, taking into account the legitimate interests or needs of law enforcement or any measure reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system. (POPIA, n.d.)

The Regulator is, empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA (POPIA, n.d.) The Regulator’s powers, duties, and functions are, inter alia to provide education, including the promotion of understanding and acceptance of the conditions of lawful processing of personal information; handle and investigate complaints; issue a code of conduct from time to time; co-operate on a national and international basis with other persons and bodies concerned with the protection of personal information; facilitate cross-border cooperation in the enforcement of privacy laws with other jurisdictions; and generally,

do everything necessary to fulfil these duties, which is conducive to the protection of PI in SA. (POPIA, 2013)

It is important to note that; because POPIA has only recently taken full force and effect in the Republic, there has not been much case law in terms of which a data subject has based a claim on POPIA (POPIA, n.d.)). However, given the inevitability and certainty of a data subject instituting a claim against a responsible party for failing to comply with the provisions of the POPIA, for the civil remedies. In terms of POPIA (2013) section 99 (1): “A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.” What gives rise to a claim is outlined in section 73 as an interference with the protection of the personal information of a data subject. Such interference consists, in relation to that data subject, of— (a) “any breach of the conditions for the lawful processing of personal information as explained above; (b) non-compliance with any of sections 22, 54, 69, 70, 71 or 72; or (c) a breach of the provisions of a code of conduct issued in terms of section 60.” This provides an avenue for a data subject to seek a judicial remedy against a responsible party for failure to protect personal information. This provision also identifies what gives rise to a valid claim against a responsible party in terms of the Act. (Lee, 2021)

2.4.4 Other concerns

The following consumer concerns are highlighted based on the literature review:

2.4.4.1 Data and Identity theft

Data theft has become an issue as online merchants accumulate important client information in their databases (Madden & Raine, 2015). System administrators and other workers who are authorized to access servers can access data without the owner’s knowledge. A survey conducted by the British Retail Consortium (BRC) saw 62% of the respondents acknowledge data theft by system administrators and other workers as a threat (Jordan, Leskovar & Marič, 2018).

Identity theft is fulfilled by paying attention to the activities undertaken by an online shopper (Aseri, 2021). The crime perpetrators carefully monitor the activities of customers as they communicate with merchants via online stores so that they can be in a good position to masquerade as merchants or online shoppers (Schatz & Bashroush, 2016). Most people like online shopping but the difficulty comes when safeguarding one's information. However, online shopping is new to most consumers and trusting a new technology can take time, especially where money is involved (Kongso, 2015). As more people embrace online shopping, malicious hackers also pervade the internet scouring for sensitive data. (Gurung & Raja, 2016)

2.4.4.2 Malicious cyber security attacks

Consumers are concerned about malicious attacks on the privacy and safety of their personal information (Akhter, 2014.) The privacy and safety of data availed by online shoppers requires cyber security experts to be well-positioned to safeguard e-commerce from malicious threats that compromise the integrity of information (Ball, 2017). In most instances, the end user does not have the knowledge necessary to keep information safe when online. (Aseri, 2021)

2.4.4.3 Perceived risks

Consumer perceived risk, or 'risk', exists throughout the digital environment and is of particular interest and concern in digital retail; it is defined as "a consumer's belief about the potential losses or other negative outcomes from transacting on the Internet" (Liao, Liu & Chen, 2011:3) and creates consumer perceptions of uncertainty, riskiness, danger and negative repercussions comprising of threats to personal privacy and security (Liao et al., 2011; Kim, Ferrin, & Rao, 2009). However, according to Dimodugno, Hallman, Plaisent and Bernard, (2022) consumers' expectations of how organisations use their personal information might differ. Consumers are mostly concerned about sharing and safeguarding of their personal information. Other consumers consider a balance between the advantages and disadvantages when sharing their information before making a decision. However, other consumers believe that there is more benefit in sharing their personal information and are least protective of their privacy (Ahmed, Jamal & Top, 2021).

2.4.4.4 Trust concerns

Palmatier and Martin (2019;13) defines trust in the context of business-to-consumer as the belief that allows consumers to willingly become vulnerable to online retailers, after taking into consideration their characteristics and the environment in which transactions are performed. However, studies have shown the negative influence of trust on perceived risk (Ahmed et al., 2021; Dimodugno et al., 2022; Kim et al., 2009; Liao et al., 2011).

The trusting relationship of an organisation with its consumers could be affected negatively if the social contract is breached, especially where Privacy Fundamentalists or Pragmatists are concerned. In addition, this could also result in non-compliance with data protection legislation. The Protection of Personal Information Act (POPIA) of 2013, South Africa's official data protection legislation, aims to protect the personal information of consumers when processed by organisations. POPIA recognizes the right to privacy, which relates to the unlawful dissemination and use of personal information, including unsolicited electronic communication. POPIA requires prior consent before organisations can send direct marketing material to a consumer, based on an opt-in model (s 69, (POPIA, n.d.). This is similar to privacy legislation in other countries, such as the United Kingdom (UK). The Information Commissioner, who is the Regulator in terms of the UK Data Protection Act (DPA) has issued various fines for non-compliance with the usage of personal information in the context of direct marketing (Information Commissioner Officer (ICO), 2018). Home Energy & Lifestyle Management Ltd (HELM) was fined £200 000, one of the largest fines for non-compliance with marketing calling regulations, for making more than six million automated calls (ICO, 2018). Similarly, Tetrus Telecommunication was fined £440,000 for unlawfully sending millions of text messages as part of direct marketing campaigns (ICO, 2018). However, in South Africa, not many organisations have been prosecuted yet for data breaches even though a high level of a data breaches continues to be reported (POPIA, n.d.).

2.5 Conceptual framework

The conceptual model in Figure 2 is a visualisation of the drivers or influential attributes that have an impact of online consumers' privacy concerns.

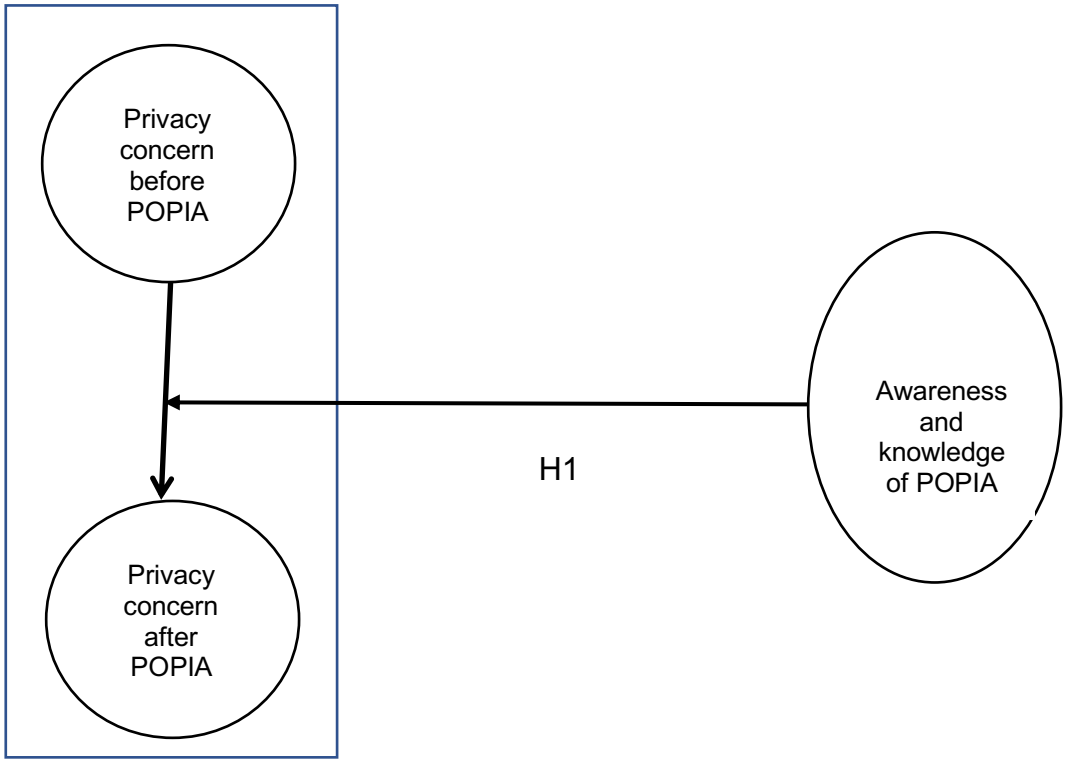

Figure 2: Conceptual model

Source: Author's Compilation

A variety of studies have shown that consumers are increasingly concerned about the lack of privacy protection during online activities. According to a survey of Web users, almost 95% of them declined to provide personal information to websites at one time or another when such information was asked (Madden & Raine, 2015). Another survey showed that 95% of Web users are worried about online privacy and 61% refused to make purchases online (Madden & Raine, 2015). Consumers' fears over the misuse of personal data have become the biggest challenge facing online retailers and online businesses (Daroch et al., 2021). Such fears lead to providing falsified personal information.

According to Kandey et al. (2018) argue that the absence of a practical guideline on how to legally process personal information of employees, customers or other juristic persons in line with the POPI Act poses a day-to-day technical challenge. The delays from 2013 to 1 December 2016 to appoint an Information Regulator of the POPI Act, meant that any privacy infringements over the period have not been successfully brought before the courts (POPIA, n.d.). The piecemeal approach of enacting the sections of the Act, which ended in 1 July 2020, meant the Act was not fully operational and commencement and effective date was only in 1 July 2021 (POPIA, n.d.). Hence, the need to understand if consumer privacy concerns changed with before and after the effective date of POPIA with the hypothesis:

Hypotheses 1 (H1): There is no difference between privacy concerns before and after POPIA effective date.

2.6 Chapter summary

In this chapter the theoretical and empirical evidence on the main concept of online shopping privacy concerns and the POPI Act were discussed. The discussion shows the agreements and disagreements found in literature leading to the research gaps. No previous studies could be found that examined the impact of POPIA on online shoppers' privacy concerns. A conceptual framework is thus developed guiding the hypothesis tested in this study. No previous studies were found testing the relationship between POPIA knowledge and online consumers' privacy concerns.
The next chapter is the research methodology.

3 RESEARCH STRATEGY, DESIGN, PROCEDURE AND METHODS

3.1 Introduction

This chapter describes the research approach, design as well as procedures and methods employed to collect, collate, and analyse the data. This chapter has the following objectives; namely, to identify and describe the research methodology (Section 3.3), the research design (Section 3.2), as well as the sampling procedure and methods (Section 3.4). The chapter also describes, the research instrument, data collection methods, data analysis methods, the reliability and validity measures (Section 3.5 to 3.9) that this research applied to make it credible as well as the technical and administrative limitations of the choices that were made (Section 3.5). Lastly, the chapter describes the ethical considerations observed during the research process (Section 3.10).

3.2 Research design

A descriptive research design was used in investigating the impact on privacy concerns for personal information shared during online purchases by the POPIAA taking effect and being a law for the protection of personal information in South Africa. According to Saunders and Lewis (2016, p.111), descriptive research seeks to describe accurately persons, events, or situations by offering descriptions, validation options, and explanations of why the phenomenon is what it is. The research design attempts to describe and explain conditions of the present by using many subjects and questionnaires to fully delineate phenomena such as consumer attitudes, perceptions, market trends, beliefs, and people's views (Sekaran & Bougie, 2016). Malhotra (2019, p.106) noted that descriptive research is suitable for studies where the researcher is not fully aware of the research problem and its dynamics but would like to be informed about the attributes of subjects, scenarios and environments and, through the collection of data, was able to state the who, what, when, where and how of the situation.

Relevant to the research questions posed in Chapter 1 (What privacy concerns for personal information data do online shoppers have when making online purchases? Has the introduction of the POPIA changed privacy concerns regarding personal

information disclosed while shopping online? Has consumer knowledge of the POPIA reduced online privacy concerns among online shoppers?), the appropriate research design was the descriptive research design. Additionally, the descriptive research design was preferred as this study made use of a large sample of online shoppers in South Africa and used statistical analysis to describe the privacy concerns and how it has been affected by the introduction of the POPIA. The descriptive research design was adopted because it supported the goal of casting light on the impact of POPIA knowledge on online shoppers' privacy concerns in South Africa through a process of data collection that enabled this study to describe online shoppers' privacy concerns more conclusively (Dudovskiy, 2018).

3.3 Research method

The motivation for a quantitative method is supported by Apuke (2017), who explains that it involves the usage and analysis of numerical data using statistical techniques in answering questions such as What, Who, How much, How many, When, Where, and How. The quantitative design allows the researcher to quantify, analyse and generalise the inferred results of relationships among variables to a population (Punch & Oancea, 2014; Streefkerk, 2021).

The quantitative method was appropriate in analysing the collected numeric data using inferential and descriptive statistics. Quantitative methods involve the use of statistical and mathematical tools to come up with results (Streefkerk, 2021). A quantitative method of research was chosen for this study because this research involved the collection and analysis of quantitative data collected on online consumer privacy concerns and POPIA knowledge. The quantitative data collected and analysed was used for understanding the impact of POPIA knowledge on online shoppers' privacy concerns as dependent and independent variables were analysed before POPIA was enacted into law and after POPIA commenced to operate as a law of the Republic of South Africa.

Another reason for choosing quantitative methods over qualitative or mixed methods was that it was identified as the most appropriate method for a descriptive study such as this one. This was a descriptive study as it intended to offer descriptions,

validation options and explanations regarding POPIA knowledge and online shoppers' privacy concerns in South Africa. This is following Thattamparambil's (2020) argument that descriptive research is employed to define people's characteristics, organise comparisons, measure data trends, and validate existing conditions.

Quantitative research was preferred for this study as it supported the scientific approach of analysis, that is, it allowed for large amounts of data to be collected and analysed statistically (Saunders et al., 2019). The quantitative method is more objective and therefore less biased as it deals with quantitative data collected for the sole purpose of answering research questions.

3.4 Population and sample

3.4.1 Population

Saunders and Lewis (2016, p.132) defined population as the complete set of group members. Zikmund, Babin, Carr and Griffin (2017, p.313) also postulated that a population is a group of any elements such as people, firms, shopping malls or high school students that have shared characteristics of data required by a researcher to conduct and complete research. For this study, the target population was the current registered Wits Postgraduate students. According to the university's 'Fact & Figures 2021-2022" publication, there were 16 624 Postgraduate students enrolled.

3.4.2 Sample and sampling method

The number of units to be used in a survey sample that enables a researcher to perform analysis and make conclusions is referred to as sample size (Malhotra, 2019). Zikmund et al. (2017) state that a sample unit is a single element or a group of elements subject to selection in the survey sample. According to Bryman and Bell (2013), the decision about sample size depends on several considerations, including time and cost. This is corroborated by Yin (2014) who argued that sample size depends on a few factors, which include statistical requirements, sample sizes in past research and the expected reliability and precision of the results.

Bryman and Bell (2013) postulated that to determine a suitable sample size, it is advisable to specify the variation or standard deviation of the population, magnitude of the acceptable error and confidence level. It was, therefore, the intention of this research to achieve a confidence level of 95% and a margin error of 5% in the research results (Zikmund et al., 2017). A review of the literature on related consumer privacy concerns used indicated adequate samples that ranged between 100 and 500 respondents (Ahmed et al., 2021; Dimodugno et al., 2022; Frik & Mittone, 2019; Shaily, 2021). Given the postgraduate population size of 16 624 above, an estimated confidence interval of ±5%, with a confidence level of 95%, the sample size for the survey was approximated at 376 respondents.

3.5 The research instrument

Questionnaires are the most popular survey instruments for collecting data to accomplish research objectives and provide answers to the research questions (Babbie, 2013; Saunders et al., 2019). Self-administered questionnaires are cheaper and quicker to administer and convenient for respondents (Bryman & Bell, 2013). Guided by Bryman and Bell (2013) and Zikmund et al. (2017), a self-administered questionnaire was designed to collect primary data from participants, ensuring it adhered to a professional aesthetic design, user-friendly, easy to understand, short and quick to administer (Appendix A). This was crucial for achieving high participant response rates.

The questionnaire followed a structured format, which contained closed-ended questions requiring participants to respond to questions by selecting a pre-determined responses option that best described their views, perceptions and circumstances (Sekaran & Bougie, 2016; Saunders et al., 2019). These were measured on a 5-point Likert scale with various descriptors.

When designing the questions in the survey instrument, it is important to operationalise the constructs being studied. Baker and Charvat (2016) referred to operationalisation as the procedure whereby the chosen variables are turned into measurable observations. Using operationalisation, a researcher can systematically collect data on systems and phenomena that aren't directly observable (Bhandari,

2020). Bhandari (2020) suggested three guiding principles on how to operationalise concepts as follows: (1) Identify the main concepts of interest in studying (2) Choose a variable to represent each concept (3) Select indicators for each of your variables. The dependent variable in this research was identified as the POPIA Knowledge in South Africa whilst some of the independent variables (research constructs) were identified as privacy concerns. This questionnaire (Appendix 2) consists of demographics, online purchasing, POPIA knowledge, privacy concerns before POPIA, and privacy concerns post-POPIA measurement items.

3.6 Procedure for data collection

An online survey was utilised in administering the questionnaires through electronic mail obtained from the Wits Business School database for registered students. An informed consent document was part of the electronic mail sent out to all study participants.

3.7 Data analysis and interpretation

Bryman & Bell (2013, p.312) suggested that to ensure accuracy in statistical analyses, it is recommended to use IBM SPSS, Minitab, SAS, StatView or MS Excel to input, categorise and analyse data. Therefore, the IBM SPSS version 27.0 software and MS Excel were used in this research to perform both descriptive and inferential statistical analysis on the data collected from the questionnaires. This research is based on a quantitative method of undertaking the research and therefore the data analysis methods employed were descriptive and inferential statistical analysis. Descriptive statistics describe a sample and use summary statistics and graphs to present the group properties (Frost, 2018). For instance, in this research, the demographic data for gender, age, monthly income, and race were analysed with frequencies and percentages. Inferential statistics make inferences about the larger population from which the sample was drawn (Frost, 2018). Descriptive statistical analyses for central tendency (mean, mode, median) and dispersion (standard deviation, kurtosis and skewness) were performed in this study using IBM SPSS. Central tendency and dispersion measures were analysed for

research constructs (Privacy Concerns, POPIA knowledge) to examine patterns of response and distribution. Zikmund et al. (2017) suggest the use of analysis of variance (ANOVA) to compare statistical differences in the mean between groups of data. In this research, respondents were grouped in clusters according to their demographics. ANOVA was used to examine the means of the various clusters, i.e. age, and gender.

Inferential statistics techniques used T-test for testing the difference in the data set groups and regression analysis to test whether the introduction of POPIA lowered privacy concerns for personal information for online shoppers.

3.8 Limitations of the study

These are potential influences that the researcher has no control over, which may eventually affect the actual study results, and the conclusions of that particular study (Theofanidis & Fountouki, 2019). Thus, these should therefore be acknowledged. Therefore, this study had the following limitations:

- Research sample and selection

The use of only students to gather the sample might harm the research given that not all students might have money to do online shopping.

- Possible exclusion of certain group ages from the respondents to the study

Because the sample population was only the university students within the Wits Business School, there is a possibility of this investigation ignored groups such as older people and much younger people that do not form part of the school.

3.9 Validity and reliability

According to Cooper and Schindler (2016), reliability is upheld when data is consistent and without bias. Saunders & Lewis (2016) agree and state that for data to pass a reliability test, they should produce consistent results with minimal errors and biases. Reliability was upheld in this research by analysing Cronbach's alphas for internal consistency among the constructs.

To ensure good internal consistency among constructs, it is recommended to aim for Cronbach's alphas (α) equal to .70 and above (Hair, Black, Babin & Anderson, 2013). According to Olaniyi (2019), Cronbach's alphas range between .0 (no consistency in measurement) and 1.0 (perfect consistency in measurement). Cronbach's alphas of .70 and higher are acceptable for exploratory research and those .80 and .90 are acceptable for basic research and applied research, respectively. Table 3 below is an illustration of Cronbach's alpha thresholds and their internal consistency.

Table 3: Cronbach's alphas thresholds

Cronbach's alpha value	**Internal consistency**
α >= 0.90	Excellent
0.80 =< α < 0.90	Good
0.70 =< α < 0.80	Acceptable
0.60 =< α < 0.70	Questionable
0.50 =< α < 0.60	Poor
α < 0.50	Unacceptable

Source: (Zikmund, Babin, Carr, & Griffin, 2017)

According to Cooper and Schindler (2016), a questionnaire is one of the most extensively used research data-collecting tools, particularly within the social sciences. He further argues that the foremost goal of the questionnaire in a research study is to gain pertinent records most reliably and validly. Therefore, validity and reliability which are the accuracy and consistency measures form a big component of the research methodology. In simple terms, validity measures how correct the results of a research investigation or experiment are, according to (Bryman *& Bell, 2013*) and they can be internally and externally valid. The research investigated two constructs; firstly, privacy concerns for personal information shared during online purchases, and secondly, the impact of the Protection of Personal Information Act (POPIA) on those privacy concerns affect the Act took effect.

3.9.1 Internal validity

Internal validity is used to gauge whether the chosen research methodology follows the standard steps of the scientific method and whether the process followed in the study makes logical sense (Bryman & Bell, 2013.). Because the questionnaire to be used follows a logical structure concerning the order of the questions themselves, then internal validity was met. The sequence of the questions is privacy concerns on personal information shared during online purchases followed by a measure of the knowledge of POPIA law and then repeating the questions for privacy concerns after the Act has been turned into law. The research measured two variables, the level of privacy concerns for personal information shared during online purchases as the first one, and then the level of privacy concerns for personal information shared during online purchases post-POPI Act. Since the research examined the relationship between these two variables, then the causal relationship between the two variables was already assumed. Because POPIA was enacted to protect privacy rights to personal information, therefore it was justified to assume that internal validity was achieved.

3.9.2 External validity

External validity measures whether the findings and conclusions of the study are real explanations for the phenomenon in the wider world. It also seeks to determine whether there are exciting alternatives to the results obtained Bryman & Bell, 2013.). The choice and sample size of the study aid in improving the external validity of this research given that Wits Business School students are the sample, and all are doing their postgraduate studies (*Overview - Wits Business School*, n.d.). Then, are a much higher chance of them being both internet and online shoppers. This assumption is also backed up by the fact that during the early days of Covid-19 when hard national lockdowns were imposed, students were forced to do learning online. As such, they were also forced to do online purchases for some of the products/services related to their studies. If these assumptions are to be proven correct, then it would be valid to assume a high external validity for this research.

3.9.3 Reliability

Reliability is a measure of how repeatable the investigation or experiment is, checking whether the results are similar when the experiment is conducted multiple times. To improve the reliability of this investigation, all questions found on the questionnaire were derived directly from research objectives. Because most questions in the questionnaire used Likert scales, the Cronbach Alpha coefficient was used to measure internal consistency reliability. The choice of scales in use for this questionnaire is adapted from previously used ones within the same field of research topic/s to achieve high reliability.

3.10 Ethical considerations

Sekaran and Bougie (2016) noted that to produce a credible research study, ethical standards and guidelines that govern the rights of participants in the data collection process must always be adhered to. Ethical considerations were upheld in this research by obtaining an ethical clearance certificate from the WBS Ethics Committee that enabled the collection of data from participants in an ethical manner. The method of data collection was to interact with students who were requested to complete a self-administered questionnaire at WBS in Gauteng, South Africa. To ensure confidentiality and anonymity, participants' real names and ID numbers were not required to be indicated on the questionnaire. This was a way of not linking any response to any individual and the participants were informed of this fact before participating in the research. Participants were assured about the voluntary nature of the questionnaire and that they had the right to refuse participation and could withdraw at any time. In the cover letter of the questionnaire, the particulars of this researcher and those of the supervisor were made available to participants to enable them to contact the researcher or the supervisor for any clarity required or raise any ethical concerns. The presentation of research results was done ethically without misrepresenting or manipulating the data in any shape or form as suggested by Yin (2014).

3.11 Chapter summary

The research methodology presented in this paper adopted a quantitative method approach as a method for data analysis. This was deemed appropriate for a descriptive study such as this one. Population, sampling techniques, and survey instruments chosen were discussed in this chapter. Ethical considerations were outlined in the last section of the chapter. An attempt was made to comprehensively explain the research strategy, designs, procedures and methods which was used to achieve the research aim of the study, that is, to investigate the impact of POPIA on inline shoppers' privacy concerns in South Africa. The researcher depicted each component of the research in detail and then committed to a choice of what to do in each component. The choice was justified using existing literature, feasibility and fulfilling the aims and objectives of the study. In addition, the benefits and disadvantages of the research design, strategy, procedures and methods were outlined. Validity and reliability measures were elucidated together with the limitations of the study. The results and findings of the research are presented and discussed in the following chapter.

4 PRESENTATION OF RESEARCH RESULTS

4.1 Introduction

The results of the survey captured from 132 questionnaires are presented in this chapter. Data collected from the sample of students was coded and captured and processed using SPSS 27. The respondent profile summarises the demographic characteristics of the respondents and the differences between students' views pre and post-POPIA are inferred from the results of descriptive statistics and a paired sample t-test. The results of each question and hypothesis are presented from the analysis are presented in the preceding sections

4.2 Response rate

The study achieved a 94.3% response rate wherein 132 of 140 targeted responses were collected. This surpasses Best's (2009) acceptable threshold of 45% for purposes of running statistical permutations.

4.3 Respondent profile

The demographic data are presented and analysed in Table 6.

Table 4: Respondents Profile

Attribute	Description	Frequency (%) N=132
Age	Below 18 years	0%
	18-24 years	6%
	25-34years	37%
	35-44 years	46%
	45- 54 years	11%
Gender	Male	41%
	Female	59%
Employment Status	Self-employed	7%
	Employed	74%
	Unemployed	5%
	Student	14%
Education Level	High school	0%
	Diploma	4%

	First degree	55%
	Post-graduate	41%
Race	Asian	2%
	Black	77%
	Indian	8%
	white	10%
	Prefer not to say	3%

Source: Author's Compilation

Table 4 shows that the majority of the respondents were female (59.10%), had a bachelor's degree (55.30%), employed (73.48%), black (77.27%), and aged from 35-44 years (46.21%). This means the sample used was made up of mature and educated individuals able to handle the questions in the study.

4.3.1 Frequency of online shopping

To further validate whether the respondents were active online shoppers, Figure 3 shows the responses on the frequency of online shopping conduct.

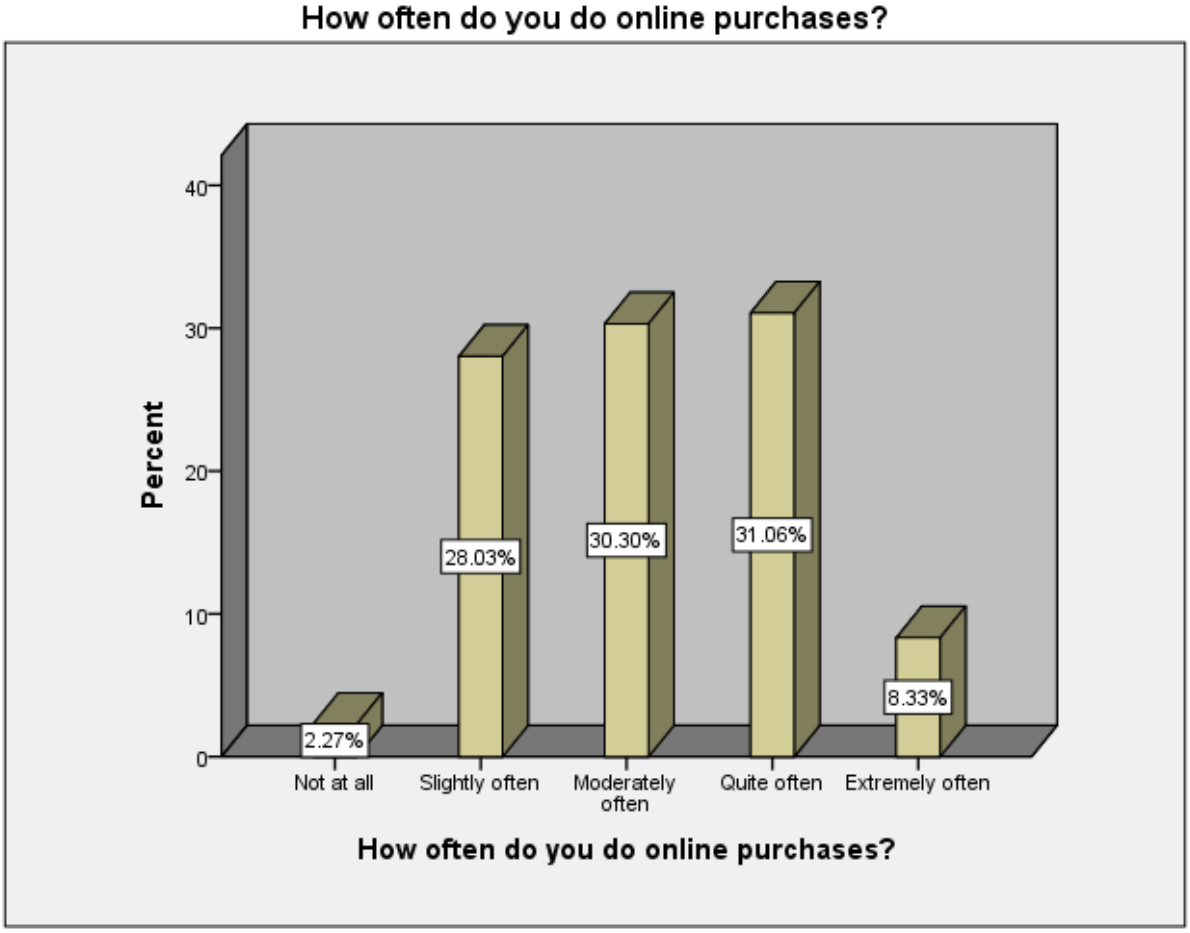

Figure 3: Frequency of Online Shopping

Source Primary Data

Figure 3 shows that 31.06% of the respondent shop online quite often, 30.30% shop moderately often, 28.03% shop online slightly often, and 8.33% shop online extremely often. This shows that most of the respondents take part in shopping online and understand the issues around privacy concerns and personal information protection. However, 2.27% of the respondents indicated not to have used online shopping at all. This group was regarded as insignificant to impact on the result and assumed to know the issues but deliberately avoid shopping online.

4.4 Reliability and validity tests

The Cronbach test was used as highlighted in the following sections:

4.4.1 Cronbach Alpha Test

The Cronbach test was carried out to ensure consistency and reliability within the research instrument questions using SPSS. Table 5 below populates the Cronbach alpha of the instrument used in this study.

Table 5: Reliability Statistics

Reliability Statistics	
Cronbach's Alpha	Number of Items
0.761	20

Source: Primary Data

It is shown that the Cronbach alpha was 0.76 reflecting the internal consistency and reliability of the items in the research instrument. It is recommended to aim for Cronbach's alphas (α) equal to .70 and above (Hair, Black, Babin & Anderson, 2013). Additionally, according to Olaniyi (2019), Cronbach's alphas range between .0 (no consistency in measurement) and 1.0 (perfect consistency in measurement). Similarly, according to Tebra (2018), a Cronbach test gives an alpha statistic that demonstrates that the scale and test adopted and constructed in a study are appropriate for the purpose and hence an indicator of the research instrument's quality, validity and reliability. Since the research instrument of this study had a Cronbach alpha above 0.7, the instrument had internal consistency and reliable constructs.

4.5 Descriptive and hypothesis statistics

Descriptive and hypothesis testing statistics are utilised in presenting the results as guided by the research questions. The descriptive statistics were used to answer the questions: What privacy concerns for personal information data do online shoppers have when making online purchases? and the question: Has the introduction of the POPIA changed privacy concerns regarding personal information disclosed while shopping online? The hypothesis testing was used to answer the question: Has consumer knowledge of the POPIA reduced online privacy concerns among online shoppers?

4.5.1. General privacy concerns online shoppers had before the POPIA became effective

4.5.1.1 Means and standard deviations on privacy concern items before POPIA

To assist in answering the research question: What privacy concerns for personal information data do online shoppers have when making online purchases before POPIA? Means and standard deviations were computed as shown in Table 6.

Table 6: Descriptive Statistics for Privacy Concerns before POPIA

	N	Mean	Std. Deviation
Do you know what your privacy rights are to protect your personal information when providing it to a company?	132	3.08	1.288
How often do privacy concerns prevent you from making online purchases?	132	3.50	1.207
Are you concerned about being over-charged on your credit card whilst making online purchases?	132	3.74	1.363
Are you concerned about your privacy at all whilst doing online purchases?	132	4.14	1.110
Are you concerned about your personal information being sold to a 3rd party when sharing it for online purchases?	132	4.33	.992
Are you concerned about giving too much personal information when making online purchases?	132	4.36	1.006
Are you concerned about online identity theft?	132	4.38	1.067
Are you concerned about online organisations not being whom they claim they are?	132	4.41	.932
Are you concerned about your credit card information being obtained/intercepted by someone else whilst making online purchases?	132	4.48	.920

Source: Primary Data

Table 6 shows the frequency distribution of the questionnaire items on online shoppers' privacy concerns before POPIA. The highest mean was recorded on the item, "Are you concerned about your credit card information being obtained/intercepted by someone else whilst making online purchases?" (M=4.48, SD=0.920). This means online shoppers' most privacy concern is credit card information interception. The item with the second highest mean was "Are you concerned about online organisations not being whom they claim they are?" (M=4.41, SD=0.932) and the item with the third highest mean was, "Are you concerned about online identity theft?" (M=4.38, SD=1.067). The lowest mean was recorded on the item, "Do you know what your privacy rights are to protect your personal information when providing it to a company?" (M=3.08, SD=0.687). This means online shoppers are least concerned about their privacy rights to protect personal information. However, the results show a strong strength mean value score of more than 3 for all the measurement items (Bhana & Bayat, 2020).

4.5.1.2 Privacy concerns whilst shopping online

Table 7: Privacy concerns whilst shopping online

		Frequency	Percent
Valid	Not at All	4	3.0
	Not Really	15	11.4
	Undecided	4	3.0
	Somewhat	45	34.1
	Very Much	64	48.5
	Total	132	100.0

Source: Primary Data

Table 7 shows that the majority of the respondents were still prevented by privacy concerns before POPIA with 48.5% indicating "very much" and 34.1% indicating "somewhat". However, at least 3% of the respondents were undecided about this

question, yet 3% reflected no effect at all of the privacy concerns stopping them from shopping online and 11.4% of the respondents indicated not being concerned about privacy concerns to make online purchases before POPIA was enacted into law in South Africa.

4.5.2 The effects of the POPIA on online shoppers' concerns about personal information gathered during online purchases

4.5.2.1 Means and standard deviations on the consumer privacy concerns post- POPIA

To assist in answering the research question: What privacy concerns for personal information data do online shoppers have when making online purchases post POPIA?, and further answer the question: Has the introduction of the POPIA changed privacy concerns regarding personal information disclosed while shopping online? Means and standard deviations were computed as shown in Table 8.

Table 8: Descriptive Statistics for Privacy Concerns post-POPIA

	N	Mean	Std. Deviation
How knowledgeable are you about the Protection of Personal Information Act (POPIA)?	132	2.95	1.058
How often do privacy concerns prevent you from making online purchases post-POPIA?	132	3.53	1.220
Are you concerned about being over-charged on your credit card whilst making online purchases post-POPIA?	132	3.73	1.230
Are you concerned about your privacy at all whilst doing online purchases post-POPIA?	132	3.98	.969
Are you concerned about giving too much personal information when making online purchases post-POPIA?	132	4.11	1.043
Are you concerned about your personal information being sold to a 3rd party when sharing it for online purchases post-POPIA?	132	4.14	1.032
Are you concerned about your credit card information being obtained/intercepted by someone else whilst making online purchases post-POPIA?	132	4.20	.986
Are you concerned about online identity theft post-POPIA?	132	4.21	.965
Are you concerned about online organisations not being who they claim they are post-POPIA?	132	4.21	.989

Source: Primary Data

Table 8 shows the frequency distribution of the questionnaire items on online shoppers' privacy concerns after POPIA. The highest mean was recorded on two items, "Are you concerned about online organisations not being whom they claim they are post POPIA?" (M=4.21, SD=0.989) and item "Are you concerned about online identity theft post-POPIA?" (M=4, 21; SD=0.965). This means online shoppers' most privacy concerns after POPIA was enacted are the impostors of online organisation and online identity theft. The item with the second highest mean was "Are you concerned about your credit card information being obtained/intercepted by someone else whilst making online purchases post POPIA?" (M=4.20, SD=0.986). This means after POPIA is enacted, credit card information interception and online identity theft are still major concerns to online shoppers/shoppers. The lowest mean was recorded on the item, "How knowledgeable are you about the Protection of Personal Information Act (POPIA)?" (M=2.95, SD=1.058). This means online shoppers are least concerned about knowing what POPIA entails. However, the results show a strong strength mean value score of more than 3 for all the measurement items (Bhana & Bayat, 2020) except for the item on POPIA knowledge (M=2.95, SD=1.058).

4.5.2.2 Severity of privacy concerns preventing online shopping post-POPIA

Table 9: Online Shoppers' Privacy Concerns on shopping online post-POPIA

		Frequency	Percent
Valid	Not at All	9	6.8
	Not Really	22	16.7
	Undecided	23	17.4
	Somewhat	46	34.8
	Very Much	32	24.2
	Total	132	100.0

Source: Primary Data

Table 9 shows that the majority of the respondents are still prevented by privacy concerns post-POPIA with 34.8% indicating "somewhat" and 24.2% indicating "very much". However, at least 17.4% of the respondents were undecided about this

question, yet 16.7% reflected no effect of privacy concerns stopping them from shopping online post-POPIA period.

4.5.2.3 Personal information safety post-POPIA

To assess the effectiveness of POPIA to ensure personal information safety, the respondents were asked about their degree of confidence in information protection after shopping online.

Table 10: Personal Information Safety post-POPIA

		Frequency	Percent
Valid	Not at all confident	36	27.3
	Slightly confident	36	27.3
	Moderately confident	37	28.0
	Quite confident	19	14.4
	Extremely confident	4	3.0
	Total	132	100.0

Source: Primary Data

Table 10 above shows that most respondents are not entirely confident, their personal information is safe after making an online purchase with 27.3% indicating "not at all confident", 27.3% indicating "slightly confidence" and 28% moderately confident. However, only 3% expressed confidence in personal information protection, whilst 14% were quite confident, their information remained safe after making an online purchase.

Furthermore, to understand consumer perceptions of personal information safety post-POPIA, the respondents were asked if they have concerns about giving too much personal information when making online purchases.

Table 11: Concerns on Giving Personal Information post-POPIA

		Frequency	Percent
Valid	Not at All	3	2.3
	Not Really	14	10.6
	Undecided	5	3.8
	Somewhat	54	40.9
	Very Much	56	42.4
	Total	132	100.0

Source: Primary data

Table 11 shows that the majority of consumers are very concerned with giving too much personal information with 42.4% indicating "very much concerned", and 40.9% indicating "somewhat concerned". However, 3.8% were undecided about this question, 10.6% were not concerned about giving too much information and 2.3% were not at all concerned to give out personal information.

4.5.3 The extent to which knowledge of the POPIA has reduced online privacy concerns

4.5.3.1 Knowledge of POPIA privacy rights

To assess how knowledgeable the respondents were about the POPIA, the results in Table 12 show the responses to the question on their POPIA knowledge.

Table 12: Online Shoppers' Knowledge of POPIA

		Frequency	Percent
Valid	Not at all knowledgeable	7	5.3
	Slightly knowledgeable	44	33.3
	Moderately knowledgeable	42	31.8
	Quite knowledgeable	27	20.5
	Extremely knowledgeable	12	9.1
	Total	132	100.0

Source: Primary Data

Table 12 shows that the majority of the respondents are not very knowledgeable about POPIA with 33.3% indicating having slight knowledge, 31.8% having moderate knowledge and 5.3% having no knowledge at all about POPIA. However, at least 9.1% of the respondents indicated having extreme knowledge of POPIA and 20.5% were quite knowledgeable about POPIA.

4.5.3.2 Hypothesis testing

The main hypothesis to test in the study to ascertain whether privacy concerns have changed after POPIA was: H1: there is no difference between privacy concerns before and after POPIA effective date.

To answer the H1 hypothesis, the sample t-test was conducted. The average values were computed for the privacy concerns pre-POPIA and privacy concerns post-POPIA, which led to a new variable for each participating individual in the survey. This resulted in an average pre-POPIA score and an average post-POPIA score.
Table 13 below shows the mean values of the average scores on privacy concerns pre and post-POPIA.

Table 13: Pre-POPIA and Post-POPIA Average Means

Statistics

		Privacy Concerns Pre-POPIA	Privacy Concerns Post-POPIA
N	Valid	132	132
	Missing	0	0
Mean		4.2619	4.0133

Privacy Concerns Pre-POPIA			Privacy Concerns Post-POPIA		
Average Value	Frequency	Percent	Average Value	Frequency	Percent
5.00	31	23.5	5.00	16	12.1
4.86	12	9.1	4.88	11	8.3
4.71	14	10.6	4.75	9	6.8
4.57	14	10.6	4.63	8	6.1
4.43	5	3.8	4.50	6	4.5
4.29	6	4.5	4.38	8	6.1
4.14	2	1.5	4.25	1	.8
4.00	12	9.1	4.13	4	3.0
3.86	6	4.5	4.00	15	11.4
3.71	5	3.8	3.88	9	6.8
3.57	4	3.0	3.75	9	6.8
3.43	5	3.8	3.63	2	1.5
3.29	1	.8	3.50	3	2.3
3.14	3	2.3	3.38	4	3.0
3.00	2	1.5	3.25	5	3.8
2.86	2	1.5	3.13	3	2.3
2.57	1	.8	3.00	6	4.5
2.43	2	1.5	2.88	3	2.3
2.29	2	1.5	2.75	1	.8
2.14	2	1.5	2.50	1	.8
1.29	1	.8	2.38	1	.8
Total	132	100.0	2.25	2	1.5
			2.13	3	2.3
			1.63	1	.8
			1.38	1	.8
			Total	132	100.0

Source: Primary Data

After computing the mean of the two as shown above in the table, the average for privacy concerns pre-POPIA was 4.2619 while privacy concerns post-POPIA was 4.0133. However, to ascertain if there is any statistically significant difference between the two means, the paired sample t-test was computed.

Table 14: pre-POPIA and post-POPIA Paired Sample T-Tests

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Privacy Concerns Pre-POPIA	4.2619	132	.78765	.06856
	Privacy Concerns Post-POPIA	4.0133	132	.82516	.07182

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Privacy Concerns Pre-POPIA & Privacy Concerns Post-POPIA	132	.762	.000

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	Privacy Concerns Pre-POPIA - Privacy Concerns Post-POPIA	.24865	.55694	.04848	.15275	.34454	5.129	131	.000

Source: Primary Data

Based on the results shown in Table 14, the mean for privacy concerns pre-POPIA (M=-4.2619, SD=0.78765) is greater than the mean for privacy post-POPIA (M=4.0133, SD=0.82516). There is a positive correlation (0.762, $p<0.05$) between privacy concerns pre-POPIA and privacy concerns post-POPIA. Furthermore, the difference in means (0.24865) is statistically significant, t (131) =5.129, p=0.000. The 2-tailed significance value of 0.000 which is less than the p-value of 0.05, shows that there is no significant difference between the means of privacy concerns pre-POPIA and post-POPIA. According to Samuels (2014), the null hypothesis of a paired sample test has rejected the sig (2-tailed) p-value is less than 0.05. Hence, the null hypothesis Ho is rejected and H1: There is no difference between privacy concerns before and after POPIA effective date, is supported. There is strong evidence ($t=5.129$, $p<0.05$) that there is no difference between privacy concerns before and after POPIA effective date.

4.6 Chapter summary

The findings are presented and show that online shoppers' privacy concerns have not changed before and after POPIA. Online shoppers are still concerned about the safety of their information safety when transacting online. Credit card and identity information theft and online organisation identity is online shoppers' most privacy concern preventing online shoppers from making purchases due to privacy concerns. Most online shoppers are not knowledgeable about personal information protection afforded to them through the POPIA.

The next chapter presents the discussions.

5 DISCUSSION

5.1 Introduction

The chapter's objective is to discuss the research results to understand the impact of POPIA on online shoppers' privacy concerns. The quantitative results are discussed and linked to the literature to enable conclusions to be made. The discussions consider past empirical results and theory to demonstrate how the findings fill in the lacuna and extend knowledge on online shoppers' privacy concerns and existing POPIA personal information protection legislation and its impact. The chapter discussions are guided by the main research objectives which are: to explore general privacy concerns online shoppers had before the POPIA became effective, to analyse the effects of the POPIA on online shoppers' concerns about personal information gathered during online purchases, and to determine the extent to which knowledge of the POPIA has affected online privacy concerns.

5.2 Privacy concerns for online shoppers' personal information before POPIA

The results show that before POPIA was enacted, online shoppers were more concerned about credit card information interception (M=4.48), online organisation impostor (M=4.41), and online identity theft (M=4.38). This is supported by Rudansky-Kloppers (2014) finding that many online shoppers choose not to engage in online shopping is that they fear being defrauded or their credit card information being stolen. Online shoppers' using card payment send their card numbers to payment processing systems. This means an online shopper is at great risk of losing bank card information if the information security becomes compromised in any way. (Aseri, 2021). According to Madden and Raine (2015), online shoppers also leave other vital data about themselves when shopping online other than bank card details. This means consumers have great concern about a data breach or accidental information disclosure. This happened when cases of data breaches were rising and being widely reported. Therefore, online shoppers' concerns about credit card information, identity theft and bogus organisations they were dealing with were valid and important for their safety and security when transacting online.

This study results also show that the majority of online shoppers were prevented by privacy concerns from purchasing online before the government introduced the POPIA. This is supported by Frik and Mittine's (2019) concern that online shoppers' privacy concerns lead to an unwillingness to use the internet, shop online or share private data. This is because the main disadvantage of online shopping includes a perceived lack of security (Vasic et al., 2019). Before POPIA was enacted, the way responsible parties processed clients' data lead to more privacy concerns (Xu et al., 2011). Before 2013, South Africa lacked comprehensive data protection regulations and only the common law could be used to solve privacy matters (POPIA, n.d). This means only delictual and common law remedies were available for infringement of personal privacy (Parker & Flowerday, 2021). According to Akher (2014), privacy concerns became more noticeable because of big data collection of personal information over the internet with clients losing control to online merchants over their individual private information. Therefore, according to Parker and Flowerday (2021), individual data privacy remains a big concern among online shoppers.

In a study by Gurung and Raja (2016), it was found that privacy and security concerns and trust beliefs had effects on risk perception of online shopping transactions to either stop them or worry about making an online purchase. Similarly, a study by Fortes and Rita (2015) also found that privacy concerns on the Internet harmed various beliefs about the use of electronic commerce. However, contrary to this, a study by Cvach, Kahsay and Shamoun (2018) found that even though consumers have privacy concerns this does not stop them from transacting. Yet, it was found in a survey that 95% of Web users are worried about online privacy and 61% refused to make purchases online (Madden & Raine, 2015). Alternatively, some online shoppers end up taking a risk and disregarding privacy concerns because of their apathetic attitudes (Parker & Flowerday, 2021). Here, consumers overlook potential risks to their information to avoid social isolation and sanction and proceed to make online purchases (Zenda et al., 2020). Yet, according to Martin and Nissenbaum (2016), when online shopper shares their individual information, they are not giving up their right to privacy as they perceive an appropriate data flow to permeate within that specific context (Martin & Nissenbaum, 2016). Hence, the privacy calculus model proposes that responsible parties are always weighing the disclosure costs against related benefits to gauge whether to disclose the

confidential information they keep on their clients (Krasnova et al., 2010). This means users only disclose personal data that brings benefits to themselves in the long term. In these instances, these users can see that the data disclosure benefits are exceeded by the risk of comprising online shoppers' privacy (Dinev & Hart, 2006).

5.3 Introduction of the POPIA changes to privacy concerns regarding personal information disclosed while shopping online

The result shows that after POPIA was enacted, online shoppers are more concerned about online identity theft (M=4.21), online organisation impostors (M=4.21) and credit card information interception (M=4.20). This is supported by Palmatier and Martin's (2019) argument that some online organisations acting as impostors create a privacy paradox whereby a false claim to value personal information privacy is done whilst at the same time behaving in a manner that compromises own privacy. These impostor organisations then perform identity theft carried out through observation of online shoppers' shopping activities (Aseri, 2021). In addition, according to Schatz and Bashroush (2016), this is a form of criminal activity when online shoppers' activities whilst shopping online are monitored by fake online merchants. This means even with POPIA being in place, most people who like to shop online still find it difficult to safeguard their personal information. However, according to Kongso (2015), online shopping is still a new technology to many people trust it on monetary issues. There is also an increased risk of more threats to malicious hacking of sensitive information as more individuals shop online (Gurung & Raja, 2016). This means personal information safety and security remain a huge concern even with POPIA in place.

The result also indicates that after POPIA was enacted, the majority of online shoppers are prevented from making online purchases because of privacy concerns (somewhat and very much-59%). This is supported by Daroch et al. (2021) findings that the misuse of individual private information is a major online shopping problem. Hence, online shoppers have become less willing to disclose or share their sensitive data with online merchants (Dinev & Hart, 2006). Instead, consumers are concerned about the need to control the sharing of their data and with privacy, they can protect

personal and sensitive information against misuse (Acquisti, et al., 2016). However, in the post-POPIA era, several data protection rights now exist for online shoppers' data collected by online merchants (Parker & Flowerday, 2021). POPIA (2013), chapter 3, specifies conditions to be followed when using and collecting individual private data thus giving online shoppers adequate privacy protection.

The findings show that after POPIA was enacted, online shoppers are not confident about the safety of their personal information (not at all and slightly confident-54.6%). This is because online shoppers are not giving up their privacy when they share their personal information online (Palmatier & Martin, 2019). According to Martin and Nissenbaum (2016), when online shopper shares their individual information, they are not giving up their right to privacy as they perceive an appropriate data flow to permeate within that specific context.

Thus, post-POPIA period, online shoppers in this study showed their huge concern about giving too much information when making online purchases (very much and somewhat concerned-83.3%). This is because consumers are concerned about malicious attacks on the privacy and safety of their personal information (Akhter, 2014.) This means cyber security is required to give online shoppers confidence in the safety of the private information they share with online merchants (Ball, 2017). In addition, the increasing advancement in technology and the internet of things means an increase in more sophisticated data security challenges in the dissemination and collection of online shoppers' private data (Aseri, 2021). According to Veiga et al. (2019), individuals' private information accumulating online has high exposure to information hackers, which makes online shoppers exposed to risks which consist of but are not restricted to malicious websites, online scams, internet fraud and phishing.

5.4 Consumer knowledge of the POPIA changes to online privacy concerns among online shoppers

The results show that online shoppers remain very unknowledgeable about POPIA (not at all, slightly and moderately knowledgeable-70.7%). This is happening when data privacy is categorically regulated by the POPIA of 2013 in South Africa (Dv,

2022). According to Parker and Flowerday (2021), POPIA empowers online shoppers or any other party to whom the personal information relates or belongs, to be able to hold any organisation accountable for the responsible safekeeping of their personal information. Thus, this means online shoppers are ignorant of the rights and privileges in POPIA. This also means online shoppers are not aware of the Act that gives legal personal data protection.

In the post-POPIA era, several data protection rights now exist for online shoppers' data collected by online merchants (Parker & Flowerday, 2021). POPIA (2013), chapter 3, specifies conditions to be followed when using and collecting individual private data thus giving online shoppers adequate privacy protection. Moreover, a data subject has the right to request, where necessary, the correction, destruction or deletion of personal information. POPIA also affords online shoppers the right to refuse or object to the processing or usage of their private data (POPIA, n.d.).

The study result ascertains that privacy concerns have not changed due to POPIA enactment and knowledge through hypothesis one. The t-tests result shows that there is no significant difference between privacy concerns before and after POPIA was enacted ($t=5.129$; $p <0.05$). Online shoppers have a legal recourse directly in terms of the POPIA in situations where organisations breach their data privacy (Romanosky et al., 2014). POPIA gives better personal data control and more specific rights to online shoppers. Online Shoppers can file their complaints and institute civil action through the Information Regulator in cases of privacy infringement (Jones, 2022). With the advent of POPIA, the notification must be made in the event of a data security breach. This is activated by Section 24 of POPIA (2013) which hold that, "where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator; and subject to subsection (3), the data subject, unless the identity of such data subject cannot be established." However, according to Skolmen and Gerber (2015), the SA POPIA introduction allays such concerns if the Act is not appropriately applied and made known to consumers. It is therefore imperative to ensure the implementation of POPIA included much consumer awareness of the legal privacy protection covered.

5.5 Chapter summary

This chapter provided a discussion on the main findings and revealed that online shoppers lack knowledge of POPIA and consequently remain afraid of personal information theft when shopping online. The increased cases of data breaches and accidental information disclosure by online organisations have also affected online consumers' information concerns and activities on the internet. Additionally, online shoppers' privacy concerns have remained unchanged regardless of the government introducing POPIA as legislation that guides online organisations on how they manage personal information protection including the penalties for any data breach and failure to uphold the human right to privacy. In the Post-POPIA era, online shoppers have data protection rights. However, online shoppers still have concerns about identity theft, credit card information interception and dealing with impostor online organisations. Online shoppers remain worried about giving too much personal information and the safety of the information they share with online organisations.

The next chapter presents the conclusions, limitations and recommendations of the study

6 SUMMARY, CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter presents the conclusions and recommendations of the study. The study aimed to examine the impact of POPIA on online shoppers' privacy concerns in South Africa. This chapter shows that the objectives of the study were achieved, which were to explore general privacy concerns online shoppers had before the POPIA became effective, to analyse the effects of the POPIA on online shoppers' concerns about personal information gathered during online purchases, and to determine the extent to which knowledge of the POPIA has affected online privacy concerns. The chapter also presents the contributions and limitations of the study.

6.2 Summary of the findings

The main study findings are summarised according to the objectives as follows:

6.2.1 General privacy concerns online shoppers had before the POPIA became effective

The study found that online shoppers were mainly concerned about credit card information, identity theft and dealing with online impostor organisations. According to Rudansky-Kloppers (2014), many online shoppers choose not to engage in online shopping is that they fear being defrauded or their credit card information being stolen. In addition, online shoppers leave their sensitive data on websites when shopping online (Madden & Raine, 2015). With the rise in cases of data breaches and accidental information disclosure, online shoppers had great concerns about their safety and security before POPIA was effectuated into law to offer them protection and civil rights for infringement against their privacy under common law.

Most of the respondents indicated the issue of privacy concerns often prevented them from conducting online transactions before POPIA was affected. This is supported by Frik and Mittine's (2019) concern that online shoppers' privacy concerns lead to an unwillingness to use the internet, shop online or provide their sensitive data. Online shopping is generally perceived as insecure (Vasic et al., 2019). Consumers generally have no control over personal data after providing it to online companies and thus worry about their information privacy (Smith et al., 2011).

According to Martin and Nissenbaum (2016), when online shopper shares their individual information, they are not giving up their right to privacy as they perceive an appropriate data flow to permeate within that specific context. Thus, empirical studies (Fortes & Rita, 2015; Gurung & Raja, 2016) found that privacy concerns influence consumer use of the internet for shopping. However, some consumers end up purchasing online after they weigh the benefits (Diney & Hart, 2006; Krasnova et al., 2010), social isolation (Zenda et al., 2020); giving false personal information (Maiden & Raine, 2015), taking risk (Parker & Flowerday, 2021).

6.2.2 The effects of the POPIA on online shoppers' concerns about personal information gathered during online purchases

The study found that online shoppers are still concerned about online identity theft, card information interception and online organisation impostors after POPIA. According to Aseri (2021), the increasing advancement in technology and the internet of things means an increase in more sophisticated data security challenges in the dissemination and collection of online shoppers' private data. Individuals' private information accumulating online has high exposure to information hackers, which makes online shoppers exposed to risks which consist of but are not restricted to malicious websites, online scams, internet fraud and phishing. (Veiga et al., 2019). The study results show that online shoppers are not confident about the safety of their personal information and are concerned about giving too much information when purchasing online. This is because, according to Martin and Nissenbaum (2016), when online shopper shares their individual information, they are not giving up their right to privacy as they perceive an appropriate data flow to permeate within that specific context. Consumers are concerned about malicious attacks on the privacy and safety of their personal information (Akhter, 2014.) However, in the post-POPIA era, several data protection rights now exist for online shoppers' data collected by online merchants (Parker & Flowerday, 2021). POPIA (2013), chapter 3, specifies conditions to be followed when using and collecting individual private data thus giving online shoppers adequate privacy protection.

6.2.3 The extent to which knowledge of the POPIA has affected online privacy concerns

The study found that online shoppers are not knowledgeable of the POPIA. Consequently, it was found that there is no significant difference between privacy concerns before and after the POPIA enactment. Online shoppers have a legal recourse directly in terms of the POPIA in situations where organisations breach their data privacy (Romanosky et al., 2014). POPIA affords control of personal data and gives data protection rights to online shoppers (Parker & Flowerday, 2021). This information would reduce their online shoppers' privacy concerns. However, online shoppers lack knowledge of POPIA. Therefore, according to Skolmen and Gerber (2015), the SA POPIA introduction allays such concerns if the Act is not appropriately applied and made known to consumers. It is therefore imperative to ensure the implementation of POPIA included much consumer awareness of the legal privacy protection covered.

6.3 Conclusions

The introduction of POPIA in South Africa has made little or no effect on online shoppers' privacy concerns. Online shoppers have the same privacy concerns before and after POPIA was enacted. Online shoppers lack knowledge of their full rights under the POPIA and thus remain concerned about the same privacy concerns they had before the Act was introduced. This means online shoppers are ignorant of the rights and privileges in POPIA that afford them legal personal data protection against abuse. It is therefore imperative to ensure the implementation of POPIA includes much consumer awareness of the legal privacy protection covered.

6.4 Contributions of the study

The study reveals that consumers are not knowledgeable about the POPIA despite its introduction in 2013 (Dv, 2022) and its effective legitimacy in 2021. This evidence is important to policymakers and implementers in public awareness of new legislation. This means online shoppers are not aware of the POPIA that gives legal

personal data protection to an individual private data processing or usage by another party.

It appears online shoppers still fear the safety of their personal information after POPIA was introduced and operational. This is vital information for the online organisation to improve their online platforms and afford customers safe and secure transactions. This is because online shoppers are not giving up their privacy when they share their personal information online (Palmatier & Martin, 2019).

Online shoppers' privacy concerns before and after the POPIA's introduction have remained the same. Since online shoppers lack knowledge of their various rights under POPIA, their privacy concerns have remained unchanged. This means online shoppers are ignorant of POPIA which enables affected online shoppers to take civil court action for damages against organisations in breach of their privacy (Jones, 2022, Romanosky, 2014). Additionally, POPIA empowers online shoppers or any other party to whom the personal information relates or belongs, to be able to hold any organisation accountable for the responsible safekeeping of their personal information. However, due to a lack of knowledge, online shoppers' privacy concerns remain unchanged.

The study was able to test whether there were significant changes in online shoppers' concerns before and after POPIA was introduced using grouped data. This study was able to show that there is strong evidence ($t=5.129$, $p<0.05$) that there is no difference between privacy concerns before and after POPIA effective date for the two-tailed test. This result is important to lawmakers and evokes necessary action to ensure the effectiveness and usefulness of new legislation to citizens.

6.5 Limitations

This study was conducted just a year after the POPIA operational date. This period might be too short to test for significant changes in consumer behaviours and concerns. The study was able to show that not many individual consumers have taken litigation against organisations where data breaches under POPIA have occurred, although many incidents of data breaches have been reported in South

Africa. Furthermore, the sample used was not large enough for the results to be generalised to a wider population of online shoppers in South Africa. However, a large sample can bring more insights into the knowledge and perceptions of the POPIA.

6.6 Recommendations

6.6.1 Recommendations for other researchers

This study has managed to ascertain the impact of privacy concerns before and after POPIA has been made operational showing no significant change in privacy concerns before and after POPIA's effective date. Future studies can be carried out using longitudinal studies with larger samples since this study was cross-sectional in nature. This study could only try and measure the impact based on consumers' perceptions. Thus, there is also a need for other studies to be conducted that will measure the actual impact the knowledge of POPIA policy has on customers' privacy concerns using other metrics such as the actual impact on the market.

6.6.2 Recommendations for policymakers

The following are recommendations for policymakers:

6.6.2.1 Public awareness of the POPIA

There is a need for more public awareness of the POPIA Act to ensure online shoppers are fully knowledgeable to exercise their rights of personal data information protection. Television (TV) and Radio advertisements, roadshows, and online advertisements are effective ways for policymakers to ensure the public is aware of the new existing legislation that protects individual rights.

6.6.2.2 Awareness of POPIA case laws

The information Regulator can showcase and publicise leading case laws to show the public the relevancy of POPIA. In this way, an individual's knowledge is enhanced of the legal effect of the Act. This effectively shows evidence of the enforcement of the Act against offenders.

6.6.3 Recommendation for management

The following are management recommendations:

6.6.3.1 Training and development in organisations

Both government and private sectors can ensure employees are educated and trained on data protection. Training and development specific to POPIA should be earmarked in organisations to ensure every employee is aware as organisations ensure compliance with the Act.

6.6.3.2 Organisational POPIA compliance efforts

Managers must become more robust in ensuring personal information is protected by putting evaluation of present systems or data mapping. Dedicated employees or departments in charge of POPIA compliance and employee awareness can be put in place. Outside consultants can be hired to bring more awareness of what POPIA entails for individuals and organisations. New employees can undergo training during induction. Supplier and customer agreements can include POPIA provisions. To avoid lawsuits, organisations need to comply with POPIA by informing data subjects about the information they have collected and how they use it and get their informed consent. Businesses must also notify individuals of any data breaches within stipulated timelines.

6.6.3.3 Secure platforms

Organisations should make use of POPIA to improve their online platforms and make them more secure and safe against identity theft, data breach, and credit card information interception. The business can invest in sophisticated software and employ cybersecurity professionals able to create and maintain complex firewalls against hacking and other criminal online activities.

6.7 Chapter summary

In this period of increasing incidents and challenges of cybersecurity and the need to protect individuals against human rights to privacy violations, this is study was able to ascertain if the introduction of POPIA has been effective in reducing online shoppers' privacy concerns. The study reveals that online privacy concerns have not changed for unknowledgeable online shoppers with concerns about identity theft,

credit card theft and online impostor organisations. This calls for attention from organisational leaders and policymakers to bring awareness to the public of personal information protection mechanisms afforded to them through POPIA. Organisations play a critical role to conscientise employees about POPIA as they increase their compliance to minimise PI protection risks and avoid possible litigation through training and development initiatives and developing more secure online platforms for clients.

7 REFERENCES

Abdulrauf, L.A. & Fombad, C.M. (2016). The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa? *Journal of Media Law*, 8(1), 67-97, DOI: 10.1080/17577632.2016.1183283

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *Science*, 347(1), 509-514. Doi: 10.1126/science.aaa1465

Akhter, S.H. (2014). Privacy Concern and Online Transactions: The Impact of Internet Self-efficacy and Internet Involvement. *Marketing Faculty Research and Publications*. 135(1): 1-21. https://epublications.marquette.edu/market_fac/135

Al-Fedaghi, S. S. (2006). *Aspects of Personal Information Theory*. 2006 IEEE Information Assurance Workshop, 155–162. https://doi.org/10.1109/IAW.2006.1652090

Ahmed, S.Y., Jamal, B. & Top, C. (2021). Understanding the Impact of Trust, Perceived Risk, and Perceived Technology on the Online Shopping Intentions: Case Study in Kurdistan Region of Iraq. Journal of Contemporary Issues in Business and Government, 27(3), 1-18. DOI:10.47750/cibg.2021.27.03.264

Appel, G., Grewal, L. & Hadi, R. (2020). The future of social media in marketing. Journal of the Academic Marketing. 48(1), 79–95. https://doi.org/10.1007/s11747-019-00695-1

Apuke, O. D. (2017). Quantitative Research Methods: A Synopsis Approach. Kuwait Chapter of Arabian Journal of Business and Management Review, 6(11), 40–47. https://doi.org/10.12816/0040336

Aseri, A. (2021). Security Issues For Online Shoppers. *International Journal of Scientific & Technology Research*. 10(1), 112 - 116.

Babbie, E. (2013). The Practice of Social Research. 13th ed. Belmont, California. Cengage.

Baker, A.J.L & Charvat, B.S. (2016). Research methods in child welfare. Illustrated edition. Columbia University Press.

Ball, K.M. (2017). Introductory Note To African Union Convention On Cyber Security And Personal Data Protection. *American Society of International Law*. 56(1), 164-192.

Baloyi, N., & Kotze, P. (2017). *Do users know or care about what is done with their personal data: A South African study*. 2017 IST-Africa Week Conference (IST-Africa), 1–11. https://doi.org/10.23919/ISTAFRICA.2017.8102301

Bhandari, P. (2020). A guide to operationalization [Online] Available from: https://www.scribbr.com/dissertation/operationalization/ [Accessed on 20 Apr 2022]

Belen-Saglam, R., Nurse, J.R.C. & Hodges, D. (2022). An Investigation Into the Sensitivity of Personal Information and Implications for Disclosure: A UK Perspective, Frontiers in Computer Science, 4(1), 124-137. DOI=10.3389/fcomp.2022.908245.

Bleier, A., Goldfarb, A. & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*. 37(1), 23-33. 10.1016/j.ijresmar.2020.03.006.

Botha, J., Grobler, M. M., Hahn, J., & Eloff, M. (2017). *A high-level comparison between the South African Protection of Personal Information Act and international data protection laws*. Pretoria: Council for Scientific and Industrial Research (CSIR).

Bryman, A., & Bell, E. (2013). Research Methodology: Business and Management Contexts. South Africa. Oxford University Press.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165. https://doi.org/10.1002/asi.20459

Cooper, D.R. & Schindler, P.S. (2016). Business Research Methods. 15th ed. London: McGraw-Hill.

Cvach, M., Kahsay, S. & Shamoun, M. (2018). *Privacy online: Exploring consumers' evaluation of privacy issues in relation to personalised advertisement when buying online*. Stockholm: Jonkoping University.

Daroch, B., Nagrath, G., & Gupta, A. (2021). A study on factors limiting online shopping behaviour of consumers. *Rajagiri Management Journal*, 15(1), 39–52. https://doi.org/10.1108/RAMJ-07-2020-0038

De Bruyn, M. (2014). The Protection Of Personal Information (POPI) Act—Impact On South Africa. *International Business & Economics Research Journal (IBER*), 13(6), 1315. https://doi.org/10.19030/iber.v13i6.8922

Dienlin, T., & Trepte, S. (2015), Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours. *European Journal of Social Psychology*. 45(1), 285– 297. doi: 10.1002/ejsp.2049.

Digital 2022. (n.d.). South Africa—DataReportal – Global Digital Insights. Retrieved June 18, 2022, from https://datareportal.com/reports/digital-2022-south-africa

Dinev, T. & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research, 17(1): 61-80. https://EconPapers.repec.org/RePEc:inm:orisre:v:17:y:2006:i:1:p:61-80.

Dimodugno, M., Hallman, S., Plaisent, M. & Bernard, P. (2021). The effect pf privacy concerns, risk, control, trust on individuals' decisions to share personal information: a game theory based approach. Journal of Physics, 20(1). 1-13. DOI: doi:10.1088/1742-6596/2090/1/012017

Dudovskiy, J. (2018). Descriptive Research. [Online] Available from: https://research-methodology.net/descriptive-research/ [Accessed on 13 Jan 2022].

Dv, A. (2022). An Information Privacy Concerns and Expectations Study of Demographic Groups in South Africa. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4109421

Ecommercedb. (n.d.). The eCommerce Market in South Africa—Data, Trends, Top Stores. Retrieved June 19, 2022, from http://ecommercedb.com/en/markets/za/all?q=%2Fen%2Fmarkets%2Fza%2Fall

Etheridge, J. (2018), “Hawks, SSA probing major ‘leak’ of personal data of SA drivers who use ViewFines”, News24, available at: https://www.news24.com/SouthAfrica/News/hawks-ssa-probing-major-leak-of-personal-data-of-sa-drivers-who-use-viewfines-20180524 (accessed 14 December 2022).

Fortes, N. & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*. 22(1), 55-68. 10.1016/j.iedeen.2016.04.002.

Frik, A. & Mittone, L. (2019). Factors Influencing the Perception of Website Privacy Trustworthiness and Users’ Purchasing Intentions: The Behavioral Economics Perspective. Journal of theoretical and applied electronic commerce research, 14(3), 89-125. DOI: 10.4067/S0718-18762019000300107.

Frost, J. (2018). Difference between Descriptive and Inferential Statistics [Online] Available from: https://statisticsbyjim.com/basics/descriptive-inferential-statistics/ [Accessed on 15 Mar 2022].

Ghani, N. A., & Sidek, Z. M. (2009). Controlling and Disclosing your Personal Information. *Information Science and Applications*, 6(3), 11-28.

Giles, J. (2020). Discovery vs Liberty judgment: Data ownership. https://www.michalsons.com/blog/tag/popia-judgments

Greenleaf, G. (2017). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. *Privacy Laws Research*, 145, 17-45, Available at SSRN: https://ssrn.com/abstract=2993035

Gurung, A. & Raja, M.K. (2016), "Online privacy and security concerns of consumers", *Information and Computer Security*, 24(4), 348-371. https://doi.org/10.1108/ICS-05-2015-0020

Hair, J.F., Black, W.C., Babin, B.J. & Anderson, R.E. 2013. Multivariate Data Analysis. 7th Ed. Pearson.

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, DOI: 10.1080/13600834.2019.1573501

Information Commissioner Office (ICO). (2018). A guide to the General Data Protection Regulation (GDDPR). London: ICO.

https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Isite Computers. (2021). *Data breaches in South Africa: What you need to know*. Retrieved from: https://isite.co.za/data-breaches-south-africa/

Jefferson, M. & Despard, P. (2018). South African M&A: The impact of data protection laws. Pretoria: DLA Piper.

Jones, B. (2022). Is POPIA Bad Business For South Africa? Comparing The GDPR To POPIA And Analyzing POPIA's Impact On Businesses In South Africa, Journal of International Affairs, 10(1): 21-38. Available at: https://elibrary.law.psu.edu/jlia/vol10/iss1/11

Jordan, G., Leskovar, R., & Marič, M. (2018). Impact of Fear of Identity Theft and Perceived Risk on Online Purchase Intention. *Organizacija*, 51(2), 146–155. https://doi.org/10.2478/orga-2018-0007

Kandeh, A.T., Botha, R.A., & Futcher, L.A. (2018). Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. South African Journal of Information Management, 20(1), 1-9. https://dx.doi.org/10.4102/sajim.v20i1.917

Kim, D.J., Ferrin, D.J. & Rao, H.R. (2009) Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration. Information Systems Research, 20, 237-257.

http://dx.doi.org/10.1287/isre.1080.0188

Kongso, F.J. (2015). Best Practices to Minimize Data Security Breaches for Increased Business Performance. New York: Walden University.

Krafft, M., Arden, C. & Verhoef, P. (2017). Permission Marketing and Privacy Concerns - Why Do Customers (Not) Grant Permissions? *Journal of Interactive Marketing*. 31(1), 1-21. Doi:10.1016/j.intmar.2017.03.001.

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, 25(1),. 109-125. 10.1057/jit.2010.6.

Liao, C., Liu, C. & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. Electronic Commerce Research and Applications. 3(1):1-14. DOI: 10. 702-715. 10.1016/j.elerap.2011.07.003.

Livingstone, S., Stoilova, M. & Nandagiri, R. (2018). Children's data and privacy online growing up in a digital age: An evidence review. Media and Communications. 3(1), 1-57.

Lee, A.W. (2021). An Analysis Of The Protection Of Personal Information Act (Popia) And The European Data Protection Framework: Suggestions For South Africa. Durban: UKZN.

Lwin, M., Williams, J. & Wirtz, J. (2017). Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science*. 35(1), 572-585. DOI: 10.1007/s11747-006-0003-3.

Madden, M. & Raine, F. (2015). Americans' Attitudes About Privacy, Security and Surveillance, New York: Pew Research Center.

Malhotra, N.K. (2019). Marketing research: an applied orientation. 6th ed. New Jersey: Pearson.

Malinga, S. (2018), "*Information Regulator is hard at work*", ITWeb, available at: https://www.itweb.co.za/content/KWEBb7yax8D7mRjO (accessed 14 November

2022).

Martin, K. (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 137(1), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Martin, K., Borah, A. & Palmatier, R. (2016). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*. 81, 34-51. DOI:10.1509/jm.15.0497.

Martin, K. & Murphy, P. (2016). The Role of Data Privacy in Marketing. *Journal of the Academy of Marketing Science*. 45(1), 112-129. Doi: 10.1007/s11747-016-0495-4.

Martin, K. & Nissenbaum, H.F. (2015). Measuring Privacy: An Empirical Test Using Context To Expose Confounding Variables. *Columbia Science and Technology Law Review*, 1(1), 1-40. http://dx.doi.org/10.2139/ssrn.2709584

Miltgen, C.L., Henseler, J., Gelhard, C. & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model, Journal of Business Research, 69(10), 4659-4666. https://doi.org/10.1016/j.jbusres.2016.04.015.

Mprem, (2016). Practical challenges of complying with POPI, viewed 05 January 2017, from http://mprem.co.za/Publications/post/practical-challenges-of-complying-with-popi

Mutimukwe, C., Kolkowska, E. & Grönlund, Å. (2019). Information privacy practices in e-government in an African least developing country, Rwanda. *Electronic Journal for Information System in Developing Countries*, 20(1), 9-27. https://doi.org/10.1002/isd2.12074

Naude, A. (2015). Data Protection in South Africa: The Impact of POPIA and Recent International Developments. Pretoria: University of Pretoria.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Olaniyi, A.A. (2019). Application of Likert Scale's Type and Cronbach's Alpha Analysis in an Airport Perception Study, Scholar Journal of Applied Sciences and Research, 2(4):1-5.

Onetrust Dataguidance. (2021). *Comparing Privacy laws: GDPR vs POPIA*. Pretoria: Onetrust Dataguidance.

Palmatier, R. & Martin, K. (2019). The Intelligent Marketer's Guide to Data Privacy: The Impact of Big Data on Customer Trust. Seattle: Sage Publishers. Doi: 10.1007/978-3-030-03724-6.

Panday, R. (2018). The Effect of Technology Readiness on Technology Acceptance in Using Services Delivery of Academic Information System. 12th UBAYA International Annual Symposium on Management, 12 September 2018, New Delhi.

Parker, H. & Flowerday, S. (2021). Understanding the disclosure of personal data online. *Information & Computer Security*, 17(1), 24-41. Doi: 10.1108/ICS-10-2020-0168.

POPIA. (n.d.). Protection of Personal Information Act (POPIA). https://www.popiact-compliance.co.za/popia-information/17-conditions-for-lawful-processing-of-personal-information

Protection of Personal Information Act (POPIA). (2013), viewed 27 December 2020, from http://www.justice.gov.za/legislation/acts/2013-004.pdf

Punch, K.F. & Oancea, A. (2014). Introduction to Research Methods in Education. 2nd ed. SAGE Publications.

Romanosky, D. Hoffman & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1), 74-104.

Rudansky-Kloppers, S. (2014). Investigating Factors Influencing Customer Online Buying Satisfaction in Gauteng, South Africa. *International Business & Economics Research Journal (IBER*), 13(5), 1187. https://doi.org/10.19030/iber.v13i5.8784

Samuels,P.(2014). *Paired Sample t-tests*. Birmingham: Birmingham City University.

Saunders, M., & Lewis, P. (2016). *Doing Research in Business & Management: An Essential Guide to Planning Your Project*. Essex. Pearson.

Saunders, M.N.K., Lewis, P. and Thornhill, A. (2019) Research Methods for Business Students. 8th Edition, Pearson, New York.

Schwartz, P.M. & Solove, D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86, 1814-1836. https://ssrn.com/abstract=1909366

Sekaran, U. & Bougie, R.J. (2016). *Research Methods For Business: A Skill Building Approach*. 7th ed. Hoboken, New Jersey. Wiley.

Shaily, S. (2021). Data-Privacy Concerns and Its Influence on Consumer Purchasing Intention in Bangladesh and India. International Journal of Marketing Studies. 13. 26910, 1-17. DOI:10.5539/ijms.v13n1p26.

Smit, C., Roberts-Lombard, M. & Mpinganjira, M., (2018). Technology readiness and mobile self-service technology adoption in the airline industry: An emerging market perspective', Acta Commercii 18(1), 1-17. https://doi.org/10.4102/ac.v18i1.580

Southern African Legal Information Institute (SAFLII). (2020). Discovery Ltd and Others v Liberty Group Ltd (21362/2019) [2020] ZAGPJHC 67; [2020] 2 All SA 819 (GJ); 2020 (4) SA 160 (GJ); 2020 BIP 351 (GJ) (15 April 2020) https://www.saflii.org/za/cases/ZAGPJHC/2020/67.html

Southern African Legal Information Institute (SAFLII). (2017). Black Sash Trust v Minister of Social Development and Others (Freedom Under Law NPC Intervening) (CCT48/17) [2017] ZACC 8; 2017 (5) BCLR 543 (CC); 2017 (3) SA 335 (CC) (17 March 2017) http://www.saflii.org/za/cases/ZACC/2017/8.html

Schatz, D. & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security*. 24(1), 73-92. 10.1108/ICS-03-2014-0020.

Skolmen, D. & Gerber, M. (2015). Protection of Personal Information in the South African Cloud Computing environment: A framework for Cloud Computing adoption. Electrical and Electronics Engineers. 5(1), 11-32. Doi: 10.1109/ISSA.2015.7335049.

Sekgweleo, T. & Mariri, M., (2019). Critical analysis of POPIA within the organisation', *International Journal of Computer Science and Information Security (IJCSIS*), 17(9), 64–69.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Sheik, S. (2018). Black Sash Trust v Minister of Social Development. https://www.michalsons.com/blog/tag/popia-judgments

Smith, H.J., Dinev, T. & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly Theory and Review, 35(4), 989-1014.

Streefkerk., R. (2021). Qualitative vs. quantitative research [Online] Available from: https://www.scribbr.com/methodology/qualitative-quantitative-research/#:~:text=Quantitative%20research%20deals%20with%20numbers%20and%20statistics%2C%20while%20qualitative%20research,ideas%20and%20experiences%20in%20depth. [Accessed on 15 Mar 2022].

Swartz, P. & Veiga, A. (2016). POPIA -opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment. *Electrical and Electronics Engineers*, 20(16), 9-24. Doi:10.1109/ISSA.2016.7802923.

Thattamparambil, N. (2020). How to choose the research methodology best suited for your study. [Online] Available from: https://www.editage.com/insights/how-to-choose-the-research-methodology-best-suited-for-your-study [Accessed on 20 Apr 2022]

Theofanidis, D. & Fountouki, A. (2019). Limitations and Delimitations in the Research Process. *Perioperative nursing (GORNA*), 7(3), 155–162. http://doi.org/10.5281/zenodo.2552022

Vasić, N., Kilibarda, M. & Kaurin, T. (2019). The Influence of Online Shopping Determinants on Customer Satisfaction in the Serbian Market. *Journal of theoretical and applied electronic commerce research*, 14(2), 13-26.

Veiga, A., Vorster, R., Li, F., Clarke, N. & Furnell, S. (2019). Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements. *Information & Computer Security*. 1(1), 1-23. DOI: 10.1108/ICS-11-2018-0135.

Xu, H., Dinev, T., Smith, J. & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances, *Journal of the Association for Information Systems*, 12(12), 1-15. DOI: 10.17705/1jais.00281

Yin, R.K. (2014). Case Study Research: Design and Methods. 5th ed. Thousand Oaks, California: Sage Publications.

Workpool .(2017). 'What is POPI: The Protection of Personal Information (POPI) act explained', Workpool Site, viewed 05 November 2022, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=71001

Wu, K., Huang, S.Y., Yen, D.C. & Popova, I. (2015). The effect of online privacy policy on consumer privacy concern and trust, *Computers in Human Behaviour*, 28(3), 889-897. https://doi.org/10.1016/j.chb.2011.12.008.

Zenda, B., Vorster, R. & Viega, A. (2020). Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. *South African Computer Journal*, 32(1), 113-132. https://dx.doi.org/10.18489/sacj.v32i1.712

Zikmund, W.G., Babin, B.J., Carr, J.C. & Griffin, M. (2017). Business research methods. 8th ed. Cincinnati, Ohio, U.S.A: South-Western College Publishing.

Borena, Berhanu & Belanger, France & Dedefa, Dejene. (2015). Information Privacy Protection Practices in Africa: A Review through the Lens of Critical Social Theory. Proceedings of the Annual Hawaii International Conference on System Sciences. 2015. 3490-3497. 10.1109/HICSS.2015.420

Botha, J., Grobler, M. M., Hahn, J., & Eloff, M. (2017). A high-level comparison between the South African Protection of Personal Information Act and international data protection laws, In ICMLG2017 5th International Conference on Management Leadership and Governance. Pretoria: Council for Scientific and Industrial Research (CSIR).

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, DOI: 10.1080/13600834.2019.1573501

Onetrust Dataguidance. (2020). Comparing Privacy laws: GDPR vs POPIA. Pretoria: Onetrust Dataguidance.

Zenda, Benson, Vorster, Ruthea, & Viega, Adele Da. (2020). Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. South African Computer Journal, 32(1), 113-132. https://dx.doi.org/10.18489/sacj.v32i1.712

8 APPENDICES

Appendix 1: Informed Consent

STUDY TITTLE: The self-completion online survey on the impact of the recent POPIA on online consumers' privacy concerns

The purpose of this research is to investigate the impact on privacy concerns for personal information that online consumer shares when making online purchases of goods or services post coming to effect of the Protection of Personal Information Act (POPIA) in South Africa.

About completing the survey:

- Completion of the survey is voluntary.
- You may choose to stop participating from the survey at any point and time.
- There will be no personal identifiers or personal information collected to keep your identity anonymous.
- The data collected will be kept confidential.
- It should take approximately 10-15 minutes to complete all the survey questions.

To participate, you must meet the following criteria:

- You must have done online shopping and made an actual online purchase before

Appendix 2: Sample of Questionnaire

Questionnaire Questions

A. Demographics
1. What is your gender? a) Male b) Female c) Prefer not to say
2. What would best describe you? a) Asian b) Black c) Coloured d) Indian e) White f) Prefer not to say
3. What age group are you in? a) 18-24 b) 25-34 c) 35-44 d) 44-54 e) Above 54
4. What is your current employment status? a) Self-employed b) Employed c) Unemployed d) Student e) Retired

5. What is the highest level of education you have completed?

a) Less than High School
b) High School
c) Diploma
d) Bachelor's degree
e) Masters degree
f) Doctoral degree

B. Online Shopping Experiences

6. How often do you do online purchases?

1 = Not at all
2 = Slightly often
3 = Moderately often
4 = Quite often
5 = Extremely often

7. To what an extend are you confident that your personal information is kept confidential when making online purchases?

1 = Not at all confident
2 = Slightly confident
3 = Moderately confident
4 = Quite confident
5 = Extremely confident

8. Do you know what your privacy rights are to protect your personal information when providing it to a company?

1 = Very unconfident
2 = Fairly unconfident
3 = neutral
4 = Fairly confident
5 = Very confident

C. Online privacy concerns questions

9. Scale used (1 = Not at All, 2 = Not Really; 3 = Undecided; 4 = Somewhat; 5 =Very Much)

a) Are you concerned about your privacy at all whilst doing online purchases?
b) Are you concerned about giving too much personal information when making online purchases?
c) Are you concerned online identity theft?
d) Are you concerned about online organisations not being who they claim they are?
e) Are you concerned about your credit card information being obtained/intercepted by someone else whilst making online purchases?
f) Are you concerned about being over charged on your credit card whilst making online purchases?
g) Are you concerned about your personal information being sold to a 3rd party when sharing it for online purchases?
h) How often do privacy concerns prevent you from making online purchases?

D. POPIA knowledge

10. How knowledgeable are you about Protection of Personal Information Act (POPIA?

1 = Not at all knowledgeable
2 = Slightly knowledgeable
3 = Moderately knowledgeable
4 = Quite knowledgeable
5 = Extremely knowledgeable

E. Privacy concerns post POPIA

11. Scale user (1 = Not at All, 2 = Not Really; 3 = Undecided; 4 = Somewhat; 5 = Very Much)

a) Are you concerned about your privacy at all whilst doing online purchases post POPIA?
b) Are you concerned about giving too much personal information when making online purchases?
c) Are you concerned online identity theft post POPIA?
d) Are you concerned about online organisations not being who they claim they are post POPIA?
e) Are you concerned about your credit card information being obtained/intercepted by someone else whilst making online purchases post POPIA?
f) Are you concerned about being over charged on your credit card whilst making online purchases post POPIA?
g) Are you concerned about your personal information being sold to a 3rd party when sharing it for online purchases post POPIA?
h) How often do privacy concerns prevent you from making online purchases post POPIA?