PRE-PRINT
Da Veiga, A. 2022. A study on information privacy concerns and expectations of demographic groups in South Africa, Computer Law & Security Review, 47(2022): 105769, https://doi.org/10.1016/j.clsr.2022.105769

A study on information privacy concerns and expectations of demographic groups in South Africa

Adéle da Veiga [0000-0001-9777-8721]

School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida, Johannesburg, South Africa
dveiga@unisa.ac.za

Abstract

Globally, there is growing concern over transparency and fairness when processing personal information and upholding the privacy of individuals. South Africa faces specific challenges in defining and implementing privacy policies and guidelines while meeting individuals' expectations as to how their personal information is handled. There is limited data available about individual concerns and expectations for privacy in South Africa across demographic groups. Such data can aid in informing privacy policies and guidelines and addressing differences and sensitivity among demographical groups concerning information privacy. This paper explores the information privacy concerns and expectations of individuals in South Africa. Data were collected through a cross-sectional survey using the Information Privacy Concern Instrument (IPCI) that was developed in previous studies in line with the Protection of Personal Information Act (POPIA) No. 4 of 2013 of South Africa. Privacy concern was found to be high in South Africa, while confidence in organisations meeting data privacy principles was low. Statistically significant differences showed that older participants, females and white participants had higher privacy expectations than Generation Y participants, males and black participants, who were more confident that organisations were meeting privacy principles. A visual index for information privacy concerns and expectations is proposed to comprehend it across demographic groups and to monitor change going forward. The recommendations provided can serve as input for further development of privacy guidelines by stakeholders such as the South African Information Protection Regulator and responsible parties handling personal information while considering differences among demographical groups in South Africa concerning information privacy.

Keywords

Information privacy; concern for information privacy; expectations; South Africa; POPIA; IPCI

1. Introduction

Organisations have to exercise good judgement when processing personal information of customers. The processing of personal information should be conducted in line with data privacy laws and regulations; however, the expectations of customers must also be considered. Respecting an individual's expectations about the manner in which their personal information is processed is integral to privacy (Internet Society and the Commission of the African Union, 2018). Individuals (i.e. consumers, citizens and end users) care about the privacy of their information and have been found to have high expectations for privacy (Auxier, Raine, Anderson, Perrin, Kumar & Turner, 2019; Da Veiga & Ophoff, 2020b; Degirmenci, 2020; Longerman Research, 2020; Rath & Kumar, 2021; Republic of South Africa, 2019) when they share their personal information with organisations. This also brings about concern for information privacy (Degirmenci, 2020; Kokolakis, 2017; Rath & Kumar, 2021), whereby individuals are concerned about the security, sharing and use of their personal information by those who collect and process it. The privacy concerns and expectations of individuals are informed by the perceptions of individuals and groups of individuals (Rath & Kumar, 2021), who could be customers of an organisation, a wider community or a nation (Kosmala, 2020). While individuals have an expectation that their personal information should be processed in line with both privacy laws and regulations, as well as their expectations (ISF 2004), these

expectations could vary based on demographical factors such as age or national culture (Arslan & Dayyala, 2017; Lee, Wong, Oh & Chang 2019). Organisations should obtain an understanding of the privacy expectations of their customers to aid in minimising concern for information privacy and to address privacy expectations across different demographical groups.

In South Africa, personal information is regulated under the Protection of Personal Information Act (POPIA) No. 4 of 2013 (Republic of South Africa, 2013) which commenced in 2021. Public and private organisations in South Africa have to process personal information in line with POPIA, which specifies conditions for the collection, use and protection of personal information. While South African organisations are implementing measures to comply with POPIA, the privacy expectations of their customers should also be considered, and privacy concerns must be addressed to demonstrate due diligence and to maintain customer trust. South Africans have been found to have a high expectation for privacy when sharing their personal information with organisations; yet, individuals have indicated that their privacy preferences are not met by organisations, resulting in information privacy concerns (Baloyi & Kotze, 2017b; Da Veiga & Ophoff, 2020b).

Various studies have been conducted in South Africa to measure concern for information privacy, with limited studies to establish the privacy expectations of individuals and if the expectations vary across demographical groups. In one of the earlier studies, Zukowski and Brown (2007) used the Internet Users' Information Privacy Concerns (IUIPC) scale of Malhotra, Kim and Agarwal (2004) to identify the influence of demographical factors in South Africa regarding concern for information privacy. However, this study did not incorporate privacy expectations and in addition the privacy concerns and perceptions of South Africans could have changed over time, as this study was conducted more than 10 years ago. Research has shown that over time, concern for information privacy can change due to various influences such as new or changed privacy laws, personal experiences of a data breach, or attendance of privacy education and training (Koohikamali, French & Kim, 2019; Hong, Chan & Thong, 2021). While later studies on information privacy concerns in South Africa have been conducted (Baloyi & Kotze, 2017b; Blauw & Von Solms, 2017; Jordaan & Ndhlovu, 2017; Mapande & Dagada, 2017; Parker & Van Belle, 2016; Tshiani & Tanner, 2018; Van der Merwe & Van Staden, 2015), the researchers did not use a validated privacy concern instrument incorporating all the conditions of POPIA and did not include a focus on privacy expectations in their studies.

The Information Privacy Concern Instrument (IPCI) questionnaire (Da Veiga, 2017; Da Veiga, 2018a, Da Veiga, 2018b, Da Veiga 2020a, Da Veiga & Ophoff 2020b) was developed and validated in more recent studies, and was applied in South Africa to measure both information privacy concerns and expectations in the context of POPIA principles. While both the concern for information privacy and expectations were measured in previous South African IPCI studies, the results were not analysed across demographic groups. It is important to understand if there are varying levels of privacy concerns and expectations among different demographical groups (e.g., gender and age) to aid in protecting the privacy of individuals as well as to put privacy policies in place that address unique characteristics (Lee et al, 2019) of demographical groups. More data are required to understand the privacy concerns and expectations of individuals in South Africa across demographical groups in order to direct and tailor interventions for each group to address specific concerns identified as well as to improve compliance with POPIA.

2. Research Objectives

The first objective of this study was to expand the understanding of information privacy concerns and expectations in South Africa across demographical groups. The IPCI was used in this study to conduct a cross-sectional survey and the data were analysed in terms of age, gender and race in order to propose recommendations to address privacy concerns and expectations of the demographic groups as well as to propose recommendations across the POPIA conditions to improve compliance.

The second objective was to determine if there was a change in the privacy perceptions compared with data of an earlier study where the IPCI was developed and applied to collect data in South Africa (Da Veiga 2017, Da Veiga, 2018a). The earlier study was conducted with 1007 participants and the results showed that South Africans had

high expectations for privacy but organisations failed to meet the expectations in practice (Da Veiga 2017, Da Veiga, 2018a). T-tests and analyses of variance (ANOVAs) were used to compare the data of the earlier study (Da Veiga 2017, Da Veiga, 2018a) and the data collected in this study. The data collected in this study were further used to propose an index to depict the data derived from the IPCI visually to aid in further comprehending the results. The results were quantified using the total privacy scores derived and portrayed on the index to ascertain the level of the information privacy concerns and expectations across four proposed segments.

3. Background

This section provides an overview of information privacy and a background to data protection in South Africa and POPIA.

3.1 Information privacy

The concept of privacy initially focused on the protection of a person and the property of a person (tangible possession of a person, e.g. land), which over time incorporated "the right to be let alone" (Warren & Brandeis 1890: p. 193). While the initial understanding of privacy related only to physical aspects of a person's life or property, the concept of the right to let alone expanded to the right of life and freedom, which include intangible aspects. Today privacy is still understood as the right to be let alone, but it has been further expanded to incorporate more interpretations and dimensions on privacy such as data or information privacy. Personal information falls within the definition of information privacy, whereby a person's personal information should receive protection. Clarke (1999) explains that privacy can be grouped into four dimensions, comprising privacy of a person, behaviour privacy, communications privacy and personal data privacy. The Information Security Forum (ISF) (2004) also presents privacy as four dimensions, namely bodily privacy, territorial privacy, communications privacy and data privacy (ISF 2004). Both these categorisations of privacy dimensions incorporate the concepts of communications privacy and data privacy. The dimensions of communications privacy and data privacy have become interrelated, and these two concepts are often jointly referred to as information privacy (ISF, 2004; Malhotra et al., 2004). Information privacy is defined by Stone, Gueutal, Gardner and McClure (1983: p. 459) as "the rights of individuals to control information about themselves". The information about oneself (namely personal information) is information relating to an identifiable, living and natural person, and in the case of POPIA also includes a juristic person. POPIA (Republic of South Africa 2013: p. 14) includes a comprehensive definition of personal information that applies to this study, namely:

> "(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
> (b) information relating to the education or the medical, financial, criminal or employment history of the person;
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
> (d) the biometric information of the person;
> (e) the personal opinions, views or preferences of the person;
> (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
> (g) the views or opinions of another individual about the person; and
> (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."

If individuals believe they do not have adequate control over their personal information, it can result in concern (Lee et al., 2019; Malhotra et al., 2004) which are referred to as information privacy concern or concern for information privacy. The perceptions and beliefs about fair control over personal information varies between

individuals due to influences or external sources, and have been studied using various concerns for information privacy questionnaires (Malhotra et al., 2004) – of which an overview is presented in section 3.2.3.

3.2 Data privacy in South Africa

This research study was conducted in South Africa and hence background is provided in this section about the privacy legislation of the country. The Bill of Rights included in the Constitution of the Republic of South Africa, 1996 provides for the right to privacy in section 14 of chapter 2, namely: "Everyone has the right to privacy, which includes the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; (d) the privacy of their communications infringed" (Republic of South Africa, 1996: p. 7). To address the right to privacy in the constitution, POPIA was promulged in 2013 as the data protection law of South Africa. The objective of POPIA is to regulate the processing of personal information in harmony with international standards for the processing thereof by public and privacy bodies in South Africa in order to address the right of privacy and to provide individuals with rights and remedies to protect their personal information in line with the conditions of the Act (Republic of South Africa, 2013).

3.2.1 Protection of Personal Information Act No. 4 of 2003 of South Africa: Status

The sections of POPIA became effective on an incremental basis. Some sections were effective as early as 11 April 2014, namely section 1 (Definitions and Purpose), sections 39 to 54 in Part A of Chapter 5 (Information Regulator), section 112 (Regulations) and section 113 (Procedure for making Regulations). That was followed by the commencement of the other sections (except for sections 110 and 114[4]) on 1 July 2020. Sections 110 and 114(4) relate to the amendment of laws and the effective transfer of functions of the Promotion of Access to Information Act (PAIA) No. 2 of 2000 (Republic of South Africa, 2000) from the South African Human Rights Commission to the Information Regulator of South Africa and came into effect on 30 June 2021. While the commencement date of POPIA was 1 July 2020, a one-year grace period to comply was allowed. That period ended on 30 June 2021. In anticipation of the final effective date of POPIA on 1 July 2021, developments in the Office of the Information Regulator resulted in the following commencement dates for the regulations issued in terms of section 112(2) of POPIA: Regulation 5 pertaining to the "Applications for issuing code of conducts" became effective on 1 March 2021 and Regulation 4 pertaining to the "Responsibilities of Information Officers" became effective on 1 May 2021.

The conditions included in POPIA were originally included in chapter VIII of the South African Electronic Communications and Transactions Act (ECTA) No. 25 of 2002 (Republic of South Africa, 2002). Although the chapter merely establishes a voluntary system for the protection of personal information and only applies to electronic transactions, conditions or principles for the protection of personal information are provided in nine statements of the Act, including: processing should be for a lawful purpose, the specific purpose of processing should be disclosed in writing, collected data should not be used for alternative purposes and any personal information collected should not be disclosed to a third party without written consent.

Multinational organisations in South Africa with operations in other jurisdictions or that process data of individuals residing in other data protection jurisdictions had to comply with data protection conditions in terms of the data privacy laws of those jurisdictions prior to the commencement of POPIA. As such, many organisations were in effect already preparing for POPIA compliance long before the legislation became effective. The status of regulation and compliance in South Africa is seen as moderate (DLA Piper, 2022). However, this could change going forward with the commencement of the conditions of POPIA and their enforcement by the Information Regulator. POPIA includes penalties for non-compliance with the Act whereby the Information Regulator can issue fines to a maximum of R10 million (approximately €5 851 900) or imprisonment for a maximum of 10 years (section 107).

3.2.2 Protection of Personal Information Act No. 4 of 2013 of South Africa: Conditions

There are common information privacy principles or conditions that are covered in most regulatory frameworks for data privacy, such as:

- **Fair Information Practice Principles** (FIPPS, n.d.): FIPPs originated from the work of Westin in 1967, which was followed by a proposal of similar principles by the United States Department of Health, Education and Welfare (HEW) that were later incorporated in the United States Privacy Act of 1974 (Teufel, 2008). The eight FIPPs are accountability, notice/transparency, individual participation/choice, data quality/integrity, security, use limitation, purpose specification and collection limitation.
- **Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines** (OECD, 2013): The HEW privacy principles were also considered in Europe and the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were initially drafted in 1980 by the OECD (Teufel, 2008), also informed by the original FIPPs (Harper, 2021). The guidelines include limitation, collection limitation, purpose specification, data quality, openness, accountability, individual participation and security safeguards.
- **Asia-Pacific Economic Cooperation (APEC) Privacy Framework** (APEC, 2005): The framework incorporates the initial FIPPs and extended it to the concept of preventing harm (Harper, 2021). It covers preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access, and correction and accountability.

The data protection principles covered in the frameworks above are adopted in data privacy laws and incorporated in POPIA as conditions. The conditions in POPIA also resemble the privacy principles of the European Union (DTTL, 2017; Taplin, 2021) and General Data Protection Regulation (Regulation [EU] 2016/679) (GDPR) (OneTrust DataGuidance, 2020). While there are similarities between POPIA and the GDPR (e.g., definitions and data subject rights) there are also differences, for example the GDPR refers to the right of data portability, defines pseudonymised data and makes provision for a data protection impact assessment, whereas POPIA does not (OneTrust DataGuidance, 2020). POPIA incorporates juristic persons and there are differences in what is defined as special or sensitive data, responding to data breaches and the penalties that can be issued (OneTrust DataGuidance, 2020). However, from a privacy principle perspective, there are alignment between POPIA and the GDPR.

POPIA encompasses eight data privacy conditions that must be implemented by responsible parties for the processing of the personal information of data subjects. Table 1 outlines the eight POPIA conditions, including a mapping thereof to the FIPPs, the OECD Privacy Guidelines and the APEC Privacy Framework with the objective of illustrating the alignment of POPIA with international privacy best practice principles from the initial FIPPs through to later developments such as that of the OECD and APEC. While the FIPPs serve as the foundation for the privacy guidelines, the OECD has been found to influence policy and legislation in the OECD member states and beyond (OECD, 2011). The APEC Privacy Framework is of relevance to the Asia-Pacific region for the transfer or personal information (OECD, 2011). Table 1 includes a mapping of the POPIA, FIPPs, OECD Privacy Guidelines and APEC Privacy Framework to illustrate how the IPCI maps to POPIA as well as to the aforementioned principles and frameworks that enable utilisation of the IPCI in regions where any of these frameworks or guidelines are used by organisations for easier adoption and integration. The "POPIA section included in IPCI" column indicates whether the respective condition of POPIA is incorporated in the IPCI questionnaire, utilised in this study for data collection, with the objective of illustrating the completeness of the scope of the IPCI in terms of the POPIA conditions and similarity to international best practice privacy principles. This allows for the adoption and utilisation of IPCI in other jurisdictions whereby it can be further customised for alignment (the IPCI questionnaire is discussed in section 4).

With reference to the terms used in the table, the term "data subject" is used in POPIA when referring to the individual whose personal information is processed and "responsible party" (controller) is the organisation that

processes the personal information of data subjects and determines the purpose of collection. "Processing" of personal information refers to the handling of personal information by the responsible party and includes the "*(a)* collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; *(b)* dissemination by means of transmission, distribution or making available in any other form; or *(c)* merging, linking, as well as restriction, degradation, erasure or destruction of information" (Republic of South Africa, 2013: p. 14) of personal information in electronic and paper records.

Table 1: POPIA conditions and mapping to FIPPs, OECD Privacy Guidelines, APEC Privacy Framework and IPCI

POPIA condition	Description based on POPIA	POPIA section	POPIA section included in IPCI	FIPPs	OECD Privacy Guidelines	APEC Privacy Framework
Condition 1: Accountability	The responsible party should ensure that the conditions in POPIA are implemented when personal information is processed.	Section 8	Y	Accountability	Accountability	Accountability
Condition 2: Processing limitation	Lawfulness of processing includes that personal information must be processed lawfully and in a reasonable manner, and should not infringe data subject privacy; minimality (must be adequate, relevant and not excessive); consent, justification and objection conditions apply; and collection directly from the data subject is covered under processing limitation.	Section 9 to 12	Y	Use limitation	Use limitation	Collection limitation Uses of personal information
Condition 3: Purpose specification	Purpose specification includes collection of personal information for a specific, explicitly defined and lawful purpose, together with retention and restriction of records requirements.	Section 13 & 14	Y	Purpose specification	Purpose specification	Uses of personal information
Condition 4: Further processing limitation	Further processing limitation focuses on ensuring that further processing is compatible with the original purpose of collection.	Section 15	Y	Individual participation/Choice	Individual participation to an extent	Uses of personal information/Choice
Condition 5: Information quality	The responsible party should ensure that personal information	Section 16	Y	Data quality/Integrity	Data quality	Integrity of personal information

POPIA condition	Description based on POPIA	POPIA section	POPIA section included in IPCI	FIPPs	OECD Privacy Guidelines	APEC Privacy Framework
	is complete, accurate, not misleading and updated where necessary to ensure information quality.					
Condition 6: Openness	Openness includes documentation of all processing under PAIA. It further includes notification to the data subject when collecting personal information with specific aspects that the data subject must be made aware of.	Section 17 & 18	Y	Notice/Transparency	Openness	Notice
Condition 7: Security safeguards	The security safeguards condition focuses on the integrity and confidentiality of personal information against loss, damage and unlawful access. Information security assurance of personal information processed by operators (third parties) and notification of security compromises are included.	Section 19 to 22	Y	Security	Security safeguards	Security safeguards
Condition 8: Data subject participation	Data subject participation gives rights to data subjects to access and request correction of personal information under certain conditions.	Section 2, 24 & 25	Y	Individual participation	Individual participation	Access and correction
Direct marketing	Chapter 8 includes data subject rights regarding direct marketing using unsolicited electronic communications, directories and automated decision making. Direct marketing is prohibited unless certain conditions apply. The opt-in principle is applicable.	Section 69 to 71	Y	-	-	-
Transborder information flows	Chapter 9 covers transborder information flows.	Section 72	Y	-	-	-

POPIA condition	Description based on POPIA	POPIA section	POPIA section included in IPCI	FIPPs	OECD Privacy Guidelines	APEC Privacy Framework
	Responsible parties within South Africa may not transfer personal information of a data subject to a foreign country unless certain conditions apply such as binding corporate rules, consent or necessity for the performance of a contract.					
Sensitive/Special personal information	Parts B and C of POPIA cover the requirements for the processing of sensitive or special personal information (e.g., religious, health, trade union membership and children information) which is prohibited if certain conditions do not apply.	Section 26 to 35	Y	-	-	-

Condition 7 (security safeguards) focuses on the integrity and confidentiality of personal information, including the implementation of technical and organisations' measures to prevent loss, damage or unauthorised access to personal information. The implementation of technical measures should be considered in the context of other information, communications and technology (ICT) laws in South Africa. While POPIA specifically regulates the security of personal information, the other ICT laws in South Africa provide for regulations on aspects such as access to and interception of information which include personal information. Section 2 of POPIA states, "If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3 then, the extensive conditions prevail". Organisations should thus follow an integrated compliance approach whereby requirements relating to information processing and security in other legislation are also integrated. ICT laws that should also be consulted are for example PAIA, giving effect to section 32 of the constitution; the Electronic Communications and Transactions Act No. 25 of 2002; the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002; the Electronic Communications Act No. 36 of 2005; and the Independent Communications Authority of South Africa Act No. 13 of 2000. The Cybercrimes Act No. 19 of 2020 defines cybercrime and provides for the regulation and investigation of cybercrime. The Cybercrimes Act should also be considered in future, but is yet to commence. It should be noted that the scope for this study is limited to POPIA and the specific requirements for each of the conditions of POPIA only.

3.2.3 Related work: Concern for information privacy studies

Studies on concern for information privacy are discussed to provide an overview of the initial concern for information privacy questionnaires that were developed and why these questionnaires were not adequate to achieve the objectives of this study. The discussion illustrates the necessity of obtaining additional data on concern for information privacy across all data privacy principles in South Africa with specific motivation to use the IPCI questionnaire.

Concern for information privacy relates to individuals (the data subjects) who have certain concerns about the processing of their personal information by organisations or governments (responsible parties) and who experience anxiety over the loss of their privacy (Smith, Milberg & Burke, 1996). Various studies have been conducted to measure concern for information privacy; however, most of these studies did not include all the information privacy principles in the questionnaire (scales) but rather focused on specific contexts, resulting in an incomplete view of concern for information privacy across data privacy principles.

The Concern for Information Privacy (CFIP) questionnaire (Smith et al., 1996) and the IUIPC scale (Malhotra et al., 2004) are regarded as the most influential privacy concern instruments (Morton & Sasse, 2014). The CFIP questionnaire (15 items) measures an individual's concern over the practices of organisations when processing their personal information. It depicts information privacy concern as concern over the extensive collection and storing of personal information; unauthorised secondary use whereby collected information is used for purposes other than the purpose it was collected for; improper access by unauthorised persons; and concern over protection against errors (accidental and deliberate); computer anxiety and behavioural intention. These concerns create psychological anxiety that could prevent individuals from sharing personal information or interacting in cyberspace (Cheah, Lim, Ting, Liu & Quach, 2020). The IUIPC scale, comprising 10 items (Malhotra et al., 2004), is based on the social contract theory and incorporates internet user concerns relating to collection, control and awareness. Through structural equation modelling, the study of Malhotra et al. (2004) confirmed that the IUIPC scale, together with the CFIP questionnaire, are valid for measuring internet users' privacy concerns. However, these questionnaires do not cover all the privacy principles in POPIA and not that of, for example, the FIPPs or the OECD Privacy Guidelines but rather measure concern for information privacy relevant to organisational privacy practices and internet users' privacy concerns. As such, these two questionnaires were not found to be all inclusive of the privacy principles and could not be used as the questionnaire to measure concern for information privacy across the POPIA conditions for the purposes of this study.

According to Kumaraguru and Cranor (2005), Westin (2003) developed privacy indexes from 1990 to 2003 that were used in over 30 studies to measure privacy concerns. The first index is referred to as Westin's privacy segmentation index and also as the general privacy concern index of Westin (Kumaraguru & Cranor, 2005). It comprises four questions developed as part of the Harris–Westin surveys (Kumaraguru & Cranor, 2005; Westin, 2003). The indexes were expanded to the medical privacy concern index (addition of two medical questions), the computer fear index (addition of three computer fear questions), the distrust index (addition of four questions) and the privacy concern index (use of six questions) (Kumaraguru & Cranor, 2005). Another privacy index developed by Westin (2003) was the core privacy orientation index, in accordance with which the American public were categorised as "privacy pragmatists", "privacy fundamentalists" or "privacy unconcerned". Westin (2003) measured the concerns of individuals by dividing them into three categories (high, medium and low privacy concern), with the index for distrust adhering to the same categories. Westin's (2003) questions focused on concern for threats to privacy; the view of businesses; governments' collection of personal information; privacy rights and control; and context-specific questions relating to technology or medical information. In his studies, he used different question-and-answer options to develop the indexes. The data of the indexes can therefore not be compared. The surveys developed by Westin was mostly focused on an organisational context and to influence public policy (Kumaraguru & Cranor, 2005). The privacy questions and indexes of Westin do not map to privacy principles from a legal perspective and do not incorporate all the conditions of POPIA. The objective of the Westin questionnaires was not related to privacy concerns across privacy principles, but rather a general privacy context of individual or citizen concern over government or organisational processing of their information.

Morton and Sasse (2014) defined an index that groups individuals into five categories (information controllers, security concerned, benefit seekers, crowd followers and organisational assurance seekers) in accordance with their privacy concerns and use of technology to aid in understanding users' adoption of technology services. The work of Westin and that of Morton and Sasse have been used or adapted in other information privacy concern

studies and researchers have developed additional information privacy concern instruments. Studies were for example conducted in the contexts of the internet (Heales, Cockcroft & Trieu, 2017; Rook, Sabic & Zanker, 2020), social media and websites (Adhikari & Panda, 2018; Kaushik, Kumar Jain & Kumar Singh, 2018; Osatuyi, 2015), online shopping (Pavlou, Liang & Xue, 2007), health (Esmaeilzadeh, 2019; Kuo, Talley & Ma, 2015) and mobile devices (Degirmenci, 2020). The questions and indexes developed by Westin (2003) and Morton and Sasse (2014) focus on specific study topics and therefore do not address all the information privacy principles of POPIA. These instruments and indexes were not suitable for the purpose of this study, as they do not focus on both concerns and expectations nor are they comprehensive in covering all the privacy principles of POPIA.

Studies on concern for information privacy have also been conducted in South Africa. Jordaan (2007) studied privacy awareness in South Africa in the context of direct marketing and online shopping behaviour that mapped only to section 69 of POPIA (Republic of South Africa, 2013). In that study, the dependency of privacy awareness on age, education and knowledge levels was investigated. The results showed that the level of privacy awareness (in name-removal procedures) was not dependent on age or educational levels. The study used a quantitative method, but the questions did not cover all the information privacy principles incorporated in POPIA. Concern for information privacy was also investigated among South African internet users by applying the IUIPC scale, showing that gender did not influence information privacy concern but that older people were more concerned than younger people (Zukowski & Brown, 2007). The study did not investigate race groups, and the concerns and expectations were not investigated across all the POPIA conditions. These studies were conducted in the early 2000s and individuals' perceptions about privacy could have changed since then (Hong et al., 2021; Koohikamali et al., 2019). A later study by Jordaan and Ndhlovu (2017) considered socio-demographical variables to establish concern for information privacy relevant to Facebook activities. While that study also did not cover all the privacy conditions of POPIA, the results contributed to an understanding of differences between demographic groups in South Africa such as that females were found to be less likely to share their personal information on social media sites like Facebook and that there were differences between race groups relevant to perceptions of social media concerns.

Further work related to privacy and security concerns relevant to mobile devices in South Africa was done and confirmed that users who were concerned over privacy would have less confidence in using mobile computing systems (Mapande & Dagada, 2017). Baloyi and Kotze (2017a) conducted a quantitative study to measure individuals' privacy knowledge and awareness of the collection of their personal information. They used 12 questions, two of which focused on trust in organisations. It was found that most of the participants (71.9%) did not trust organisations to secure their personal information. The questionnaire included perception questions about unsolicited messages and transborder transfer, which mapped to sections 69 and 71 of POPIA. Another study focused on information privacy concerns of South Africans in smart cities and findings showed that South Africans were concerned over privacy when considering the security of their personal information (Tshiani & Tanner, 2018). These studies in South Africa did not include all the privacy conditions of POPIA; they furthermore did not focus on both concerns and expectations and did not look at differences between demographical groups in terms of age, gender and race.

The IPCI has been used in studies in South Africa to measure information privacy concerning the processing of personal information in a general business context and was also adapted to an online context in relation to research studies in which it was referred to as the Online Information Privacy Concern Instrument (Da Veiga, 2020a) and the Online Information Privacy Culture Index Questionnaire (Da Veiga, 2018b; Da Veiga & Ophoff, 2020b). The aforementioned questionnaires comprised off the same questionnaire items and response scales, but the online context questionnaire included the words "online companies (websites)" in the questionnaire items to adapt it to the online context. The results of the IPCI studies consistently showed that individuals in South Africa had a high concern for information privacy and that their expectations across all the information privacy conditions of POPIA were not met (Da Veiga, 2017; Da Veiga, 2018a; Da Veiga, 2018b; Da Veiga, 2020a; Da Veiga & Ophoff, 2020b).

The IPCI questionnaire includes statements covering all the conditions of POPIA and incorporates concerns and expectations about privacy, making it suitable for use in this study to address the research objectives. An understanding of concern for information privacy across all the privacy conditions of POPIA will provide a complete view of concern in terms of the principles that relate to privacy in order to determine which privacy principles individuals are most or least concerned about for a comprehensive understanding thereof. In the previous IPCI studies in South Africa, data were not analysed in terms of age, gender and race to understand concern for information privacy across demographical groups and a corresponding index to display the results visually was not developed for the IPCI, which necessitated additional data collection to further understand data privacy concerns in South Africa.

4. Theoretical Perspective of Concern for Information Privacy: Expectations, Confidence and Legal Concerns

The concepts of information privacy expectations and confidence were introduced in previous studies (Da Veiga, 2017; Da Veiga, 2018a) and are expanded in this discussion in the context of this study. Individuals have expectations for privacy and believe or have confidence that organisations are indeed meeting their privacy expectations. Examples of such expectations could be that a society has a high expectation for transparency and holds the view that personal information should not be used for alternative purposes. An individual could expect organisations not to collect excessive data, to keep it up to date and not to share it with third parties. Individuals have expectations for privacy in relation to the information privacy conditions of data privacy laws. A society or individual subsequently experiences in practice whether organisations or governments meet their expectations, with resultant belief or confidence that an organisation is transparent in handling their personal information or concern that an organisation collects too much personal information.

Figure 1 provides an explanation of information privacy concerns and expectations as comprising three pillars, namely legal requirements, expectations and confidence. The three pillars are explained as follows:

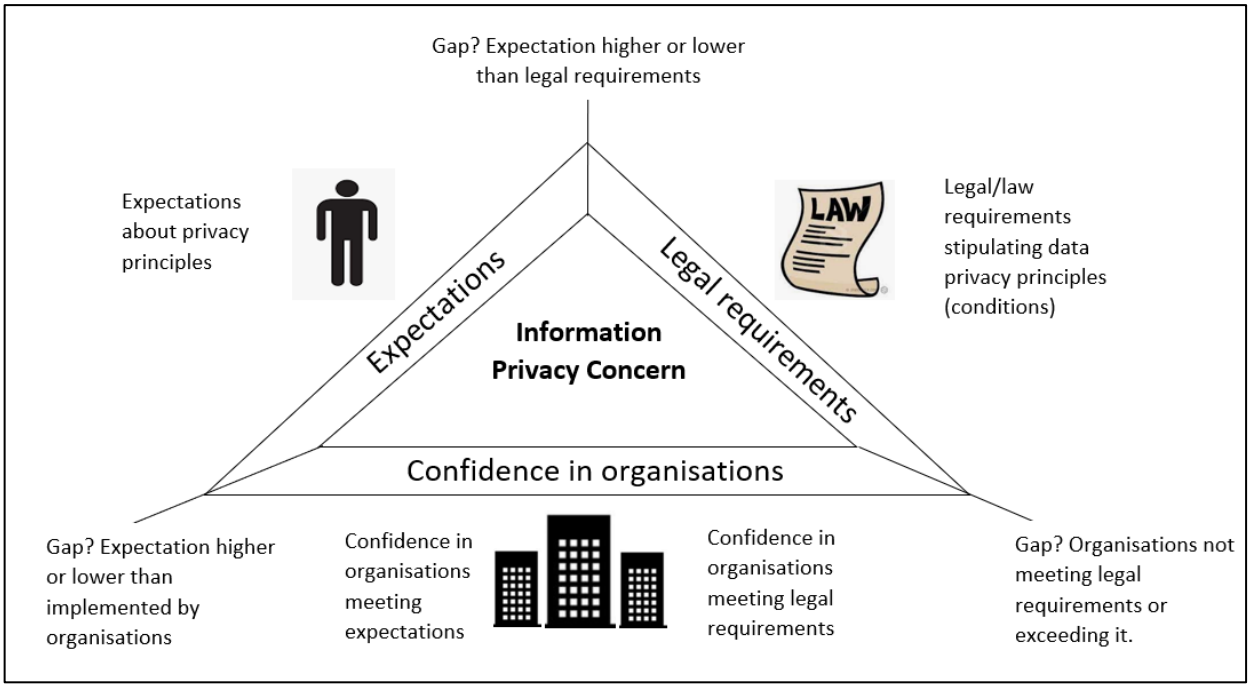
i. **Legal requirements**. Data protection law requirements, such as encapsulated in POPIA, are based on international accepted information privacy principles and must be implemented by organisations as a minimum obligation to comply with legal requirements.

ii. **Privacy expectations**. Individuals have expectations relevant to information privacy principles or conditions (such as those in POPIA) which they expect organisations to uphold. It builds trust when consumers perceive organisations to meet their privacy expectations (Weller & Leach, 2020). Their expectations could vary based on factors such as age, national culture or trust (Arslan & Dayyala, 2017), or be influenced by continued use of and exposure to applications (Koohikamali et al., 2019) or the reputation of an organisation or website (Gerber, Gerber & Volkamer, 2018). The expectations are synonymous with individuals' perceptions of or attitudes about privacy. Their expectations could be met or they could have higher or lower expectations than the minimum requirements of data privacy laws for each of the privacy principles. Furthermore, their expectations in respect of each information privacy principle are twofold (i.e., are they in line with the legal requirements of a specific privacy law like POPIA and are they met by the organisations that process their personal information). This links to the social contract theory postulated by Head and Yuan (2001). According to that theory, individuals share their personal information with responsible parties based on certain expectations and the principle that they can decide on the usage of the personal information (Phelps, Nowak & Ferrell, 2000). That is supported by the work of Martin (2016), according to which individuals have expectations prior to entering into a contract with a responsible party.

iii. **Privacy confidence**. Individuals experience in practice whether their privacy expectations are met by organisations and where it is not, it could result in a lack of trust (Martin, 2016). Organisational failure to meet such expectations indicates a gap in either not meeting the expectations from a bottom-up perspective or not meeting a regulatory requirement from a top-down perspective. That could be a representation of the level of organisational compliance with information privacy principles as

perceived by individuals. The aim is to focus on the perceptions of individuals, as that could shed light on whether organisations need to revise their privacy programmes to meet certain privacy principles or need to share more information about their privacy practices to promote a reputation of trust and be seen as being compliant as opposed to being non-compliant.

Figure 1: Information privacy expectations, confidence and concerns



4.1 The Information Privacy Concern Instrument (IPCI)

The IPCI addresses the three pillars of figure 1. The objective of the IPCI (Da Veiga, 2017; Da Veiga, 2018a; Da Veiga, 2018b; Da Veiga, 2020a; Da Veiga & Ophoff, 2020b) is to measure individuals' information privacy concern from two perspectives: expectations about privacy principles (conditions) and perception about whether individuals have confidence in organisations meeting privacy conditions. The privacy conditions are based on the conditions in POPIA and hence give a view if the legal requirement is met and if the expectation is met when comparing the perceptions of the expectations and confidence constructs. The IPCI includes all the information privacy conditions of POPIA, making it inclusive to obtain the perceptions of individuals about each privacy condition.

This questionnaire considers concern for information privacy from both an expectation and a confidence perception perspective, that is the privacy expectations of individuals (consumers) and their confidence of organisations meeting their expectations in practice. The IPCI comprises 11 constructs for expectations and 11 constructs for confidence, each with 22 statements. The statements for both the expectations and confidence were developed with a pared statement (expectation and confidence) for each POPIA condition. Two additional statements are included in the confidence section which are not paired with the expectation section. These two additional statements relate to accountability. A total of 44 paired statements are thus included in the IPCI for the purpose of comparing the means of the expectations with confidence statements in order to establish if there is a gap.

Table 2 presents the statements of the IPCI with a mapping to POPIA, the FIPPs and the OECD Privacy Guidelines to illustrate completeness in terms of POPIA conditions and completeness in terms of the international accepted privacy principles making the IPCI applicable for use in other jurisdictions. The statements in table 2 were used to collect the data for this study. The data was analysed across demographical groups to understand each group's unique concerns and expectations across the POPIA conditions. The data were further analysed in line with the POPIA conditions to make recommendations for improving compliance.

Table 2: Mapping of IPCI constructs and statements to POPIA, FIPPs, the OECD Privacy Guidelines and APEC Privacy Framework

IPCI constructs – Expectations items	IPCI constructs – Confidence items	POPIA mapping	FIPPs mapping	OECD Privacy Guidelines	APEC Privacy Framework
Expectation_Processing (use) limitation (PR)	Confidence_Processing (use) limitation (PR)	Processing limitation	Use limitation	Use limitation	Uses of personal information
Q24b. "I expect companies to use my personal information in a lawful manner (e.g. never to sell my information; publish my confidential information; never use my information for fraudulent transactions)."	Q25b. "I feel confident that companies are using my personal information in lawful ways (e.g., never sell my information, publish my confidential information or use my information for fraudulent transactions)."	Condition 2, Section 9, Processing limitation, Lawfulness	Use limitation	Use limitation	Uses of personal information
Q24c. "I expect privacy when a company has to process my personal information for services or products (e.g., never share my information with unauthorised personnel or use my information for other purposes)."	Q25c. "I feel confident that companies respect my right to privacy when collecting my personal information for services or products (e.g., never to share my information with unauthorised personnel or use my information for other purposes)."	Condition 2, Section 9, Processing limitation, Lawfulness	Use limitation	Use limitation	Uses of personal information
Expectation_Collection limitation (CL)	Confidence_Collection limitation (CL)	Processing limitation	Collection limitation	Collection limitation	Collection limitation
Q24d. "I expect companies not to collect excessive or unnecessary information from me (e.g., my children's information, my salary, my health information, my race or religion) than what is needed for them to offer me a service or product."	Q25d. "I feel confident that companies are requesting only relevant and not information other than what is needed for them to offer me a service or product. (e.g., information on my children, my salary, my health, my race or religion)."	Condition 2, Section 10, Processing limitation, Minimality	Collection limitation	Collection limitation	Collection limitation
Q24e. "I expect companies to only collect my personal information when I have given my consent or if it is necessary for a legitimate business reason."	Q25e. "I feel confident that companies are collecting my personal information only with my consent or for a legitimate business reason (e.g., not collecting my information without my consent while I browse the internet, or buying my information from other companies)."	Condition 2, Section 11, Processing limitation, Consent	Collection limitation	Collection limitation	Collection limitation
Q24f. "I expect companies to only collect my personal information from myself and not from other sources (e.g., from other companies or people I know)."	Q25f. "I feel confident that companies are collecting my personal information from legitimate sources."	Condition 2, Section 12, Processing limitation, Direct collection	Collection limitation	Collection limitation	Collection limitation
Expectations_Purpose specification (PS)	Confidence_Purpose specification (PS)	Purpose specification	Purpose specification	Purpose specification	Uses of personal information
Q24g. "I expect companies to explicitly define the purpose for which they want to use my information."	Q25g. "I feel confident that companies are explicitly defining the purpose for which they want to use my information."	Condition 3, Section 13, Purpose specification, Specific purpose	Purpose specification	Purpose specification	Uses of personal information

IPCI constructs – Expectations items	IPCI constructs – Confidence items	POPIA mapping	FIPPs mapping	OECD Privacy Guidelines	APEC Privacy Framework
Q24h. "I expect companies to only use my personal information for purposes I agreed to and never for other purposes (e.g., telemarketing or targeted advertising) than those agreed by me."	Q25h. "I believe that companies are only using my personal information for purposes I agreed to and never for other purposes (e.g., telemarketing or targeted advertising)."	Condition 3, Section 13, Purpose specification, Specific purpose	Purpose specification	Purpose specification	Uses of personal information
Q24i. "I expect companies to only keep my personal information for as long as required for business purposes or regulatory requirements."	Q25i. "I believe that companies are keeping my personal information indefinitely."	Condition 3, Section 14, Purpose specification, Retention	Purpose specification	Purpose specification	Uses of personal information
Expectations_ Processing (use limitation) (PR)	Confidence_Processing (use limitation) (PR)	Further processing	Individual participation/Choice	Individual participation	
Q24j. "I expect companies to obtain my consent if they want to use my personal information for purposes not agreed to with them."	Q25j. "I feel confident that companies are obtaining my consent to use my personal information for purposes other than those agreed to with me."	Condition 4, Section 15, Further processing limitation	Individual participation/Choice	Individual participation to an extent	Individual participation/Choice
Expectations_Openness (OP)	Confidence_Openness (OP)	Openness	Notice/Transparency	Openness	Notice
Q24a. "I expect companies to notify me before they start collecting my personal information."	Q25a. "I feel confident that companies are notifying me before collecting my personal information."	Condition 6, Section 18, Openness, Notification	Notice/Transparency	Openness	Notice
Q24k. "I expect companies to inform me of the conditions (e.g., purposes, consequences, recipients of my information, my rights and the way in which they protect confidentiality) for processing my personal information."	Q25k. "I feel confident that companies adequately inform me of the conditions (e.g., purposes, consequences, recipients of my information, my rights and the way in which they protect confidentiality) for processing my personal information."	Condition 6, Section 18, Openness, Notification to data subject when collecting personal information	Notice/Transparency	Openness	Notice
Expectations_Information (data) quality (IQ)	Confidence_Information (data) quality (IQ)	Quality of information	Data quality/Integrity	Data quality	Integrity of personal information
Q24l. "I expect companies to keep my personal information updated."	Q25l. "I feel confident that companies keep my personal information up to date."	Condition 6, Section 16, Openness, Quality of information	Data quality/Integrity	Data quality	Integrity of personal information
Expectations_ Security safeguards (SS)	Confidence_Security safeguards (SS)	Security	Security	Security safeguards	Security safeguards
Q24m. "I expect companies to protect my personal information."	Q25m. "I feel confident that companies are protecting my personal information (e.g., keep my data confidential and protect it from being accessed by unauthorised parties)."	Condition 7, Section 19, Security	Security	Security safeguards	Security safeguards
Q24n. "I expect companies to have all the necessary technology and processes in place to protect my personal information."	Q25n. "I feel confident that companies have all the necessary technology and processes in place to protect my personal information."	Condition 7, Section 19, Security	Security	Security safeguards	Security safeguards
Q24o. "I expect companies to ensure that their third parties (processing my personal information) have all the necessary technology and processes in place to protect my personal information."	Q25o. "I feel confident that companies ensure that their third parties have all the necessary technology and processes in place to protect my personal information."	Condition 7, Sections 20 and 21, Security, Operator	Security	Security safeguards	Security safeguards
Q24p. "I expect companies to inform me if records of my personal data were lost, damaged or exposed publicly."	Q25p. "I feel confident that companies inform me if records of my personal data were lost, damaged or exposed publicly."	Condition 7, Section 22, Security, Notification of security compromises	Security	Security safeguards	Security safeguards

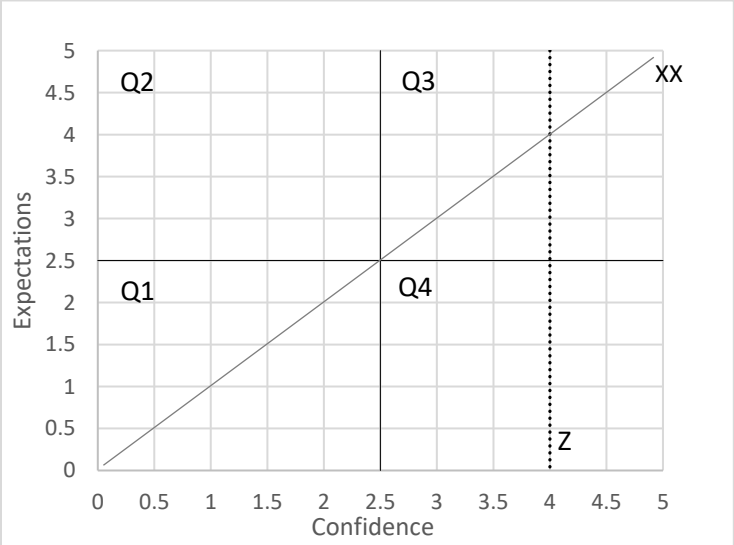
IPCI constructs – Expectations items	IPCI constructs – Confidence items	POPIA mapping	FIPPs mapping	OECD Privacy Guidelines	APEC Privacy Framework
Expectations_Data subject participation (DS)	Confidence_Data subject participation (DS)	Access to information	Individual participation/Choice	Individual participation	Access and correction
Q24q. "I expect companies to tell me what records of personal information they have about me when I enquire about it."	Q25q. "I feel confident that companies can tell me what records or personal information they have about me."	Condition 8, Section 23, Data subject participation, Access to information	Individual participation/Choice	Individual participation	Access and correction
Q24r. "I expect companies to correct or delete my personal information at my request."	Q25r. "I feel confident that companies will correct or delete my personal information at my request."	Condition 8, Section 24, Data subject participation, Correction of personal information	Individual participation/Choice	Individual participation	Access and correction
Expectations_ Sensitive (special) personal information (SP)	Confidence_Sensitive (special) personal information (SP)	Special information	-	-	-
Q24s. "I expect companies not to collect sensitive personal information (e.g., information on my children, religious beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal record or biometric information) about me with my explicit consent."	Q25s. "I feel confident that companies only collect sensitive personal information (e.g., information on my children, religious beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal record or biometric information) about me with my explicit consent."	Section 26-35, Special information	-	-	-
Expectations_Unsolicited marketing (UN)	Confidence_Unsolicited marketing (UN)	Direct marketing	-	-	-
Q24t. "I expect companies to honour my choice if I decide not to receive direct marketing."	Q25t. "I feel confident that companies honour my choice if I do not want to receive direct marketing."	Section 69, Direct marketing by means of unsolicited electronic communications	-	-	-
Q24u. "I expect companies to give me a choice if I want to receive direct marketing from them."	Q25u. "Companies always give me a choice to indicate if I want to receive direct marketing from them."	Section 69, Direct marketing by means of unsolicited electronic communications	-	-	-
Expectations_Cross-border transfers (CB)	Confidence_ Cross-border transfers (CB)	Transborder information flows	-	-	-
Q24v. "I expect companies to protect my information when they have to send it to other countries."	Q25v. "I feel confident that companies protect my information if they have to send it to other countries."	Section 72, Transborder information flows	-	-	-
	Confidence_ Accountability (AC)	Accountability	Accountability	Accountability	Accountability
	Q25w. "I feel confident that if I submit a complaint, it will be dealt with appropriately by the relevant authorities."	Section 40, Information Regulator duties	Accountability	Accountability	Accountability
	Q25x. "I believe that organisations take their responsibility seriously to protect my personal information."	Condition 1, Section 8, Accountability	Accountability	Accountability	Accountability

Note: Questionnaire items from Da Veiga, 2018a. The question numbering reflects the numbering format used in the online survey of this study.

The data derived from the IPCI are used in this study to propose an index with four quadrants for the IPCI (displayed in figure 2). The data derived from the IPCI are plotted, with the x-axis representing the overall

confidence mean and the y-axis the overall expectations mean. Individual statement means can also be plotted on the index.

Figure 2: Information Privacy Concern and Expectation Index



The four quadrants represent the information privacy concern across an expectations and confidence axis as follows:

- **Q1: Compliance confidence low; expectations low.** In this quadrant, individuals have a low expectation for privacy and experience that organisations do not meet privacy conditions in practice – which could be higher or lower than their privacy expectations. However, there might not be a match between their expectations and compliance confidence, which could result in concern for information privacy.
- **Q2: Compliance confidence low; expectations high.** Individuals in this quadrant have a high expectation for privacy, but experience that in practice organisations do not meet the privacy conditions. Hence, their privacy expectations are never met in this quadrant, which represents a gap. In this quadrant, the individual's expectation for privacy is always higher than their compliance confidence. That gives rise to concern for information privacy.
- **Q3: Compliance confidence high; expectations high.** Here individuals have high privacy expectations and their experience in practice is that organisations are mature in meeting the privacy principles, hence their confidence in compliance is higher. However, there might still not be a match between their expectations and their compliance confidence. Again, concern for information privacy is experienced where a gap is identified.
- **Q4: Compliance confidence high; expectations low.** This quadrant reflects a culture or society where the experience in practice of whether organisations are complying with privacy conditions is always higher than the individual's expectation for privacy.

The diagonal line (0:0; 5:5) reflects the points on the graph where the information privacy expectations and confidence are in balance; thus, the privacy expectations of individuals are met by organisations that implement the privacy conditions in line with the individuals' expectations. However, this line does not signify that the manner in which organisations meet the privacy conditions aligns with privacy best practice or the conditions (principles) of data privacy laws. Dotted line Z (4:0; 4:5) on the graph indicates the scores where organisations meet the privacy conditions of data privacy laws and consequently comply with the minimum score for each data protection principle. This represents "4 – agree" or "5 – strongly agree" on the Likert scale for the IPCI items. The aim is to have a minimal information privacy concern that can be plotted to the right of line Z for the compliance confidence mean in Q3 or Q4. That would indicate that individuals' experience that both the privacy conditions and their expectations are met when organisations process their personal information. The proposed index is illustrated in section 7.5, with the data derived from this research study.

5. Research Methodology

The research methodology is discussed in this section. An overview is provided of the approach followed and the results.

5.1 Research approach

A quantitative approach was followed for the research study. Surveys with questionnaires have been found to be useful in measuring perceptions in social and information system studies related to this study (Saunders, Lewis & Thornhill, 2016). A cross-section survey was conducted using the IPCI in an online survey.

5.2 Research instrument

The IPCI (Da Veiga, 2018a) statements of table 2 were used in this study to collect the data. The questionnaire comprised four sections:

i. **Section A**, consisting of eight demographical questions focusing on province, race, year born, gender, qualification, employment status, industry and income.
ii. **Section B**, consisting of 16 questions about technology use and privacy concerns (e.g.: Which devices are mostly used and for what purpose? How concerned are respondents about the protection and sharing of their personal information and different categories of personal information? How do respondents rate their knowledge about privacy rights? Where do they obtain information about their privacy rights? Has their personal information ever been misused?). The question scales include "Yes" and "No" responses as well as Likert scales (e.g.: *Not concerned*, *Somewhat concerned*, *Neutral*, *Concerned* and *Extremely concerned*).
iii. **Section C**, consisting of 22 privacy expectation statements applying a Likert scale about the 11 constructs in the IPCI (e.g.: *I do not expect this*, *I sometimes expect this*, *I am neutral*, *I mostly expect this* and *I always expect this*).
iv. **Section D**, consisting of 22 privacy confidence statements applying a Likert scale about the 11 constructs in the IPCI (e.g.: *Not at all confident*, *Somewhat confident*, *Neutral*, *Quite confident* and *Very confident*). Two additional questions are included, focusing on condition 1 which relates to accountability, giving a total of 24 statements.

5.3 Data collection

The target sample comprised 400 individuals in South Africa across the demographic profile of the country as follows: race group – Black (African), Coloured, Indian/Asian, White; age – above 18 years; and gender – male and female. The race group of black South Africans is referred to as "African" or "Black African" in South Africa.

For clarity purposes, so as not to confuse the terminology “African” with citizens from other African countries, the term “Black” is used in the remainder of this paper to only include black South Africans.

The market research company InSites Consulting South Africa was used to develop and send out the online survey for online data collection. The research project obtained research ethical clearance from UNISA. Participation in the survey was voluntary and answers were submitted anonymously. The participants provided consent for the data to be used in the research study. The market research company monitored participation in the survey to ensure that the required number of responses was obtained, whereafter the survey was closed.

6. Results

The results of the online survey are discussed in the next sections. The biographical information is presented first, followed by the results of the different IPCI sections. Finally, the data are depicted on the proposed index for the IPCI. The Statistical Package for the Social Sciences (SPSS) was used to analyse the data.

6.1 Biographical information

The biographical information of the respondents is shown in table 3, with a total of 400 participants (respondents) in the survey.

Table 3: Biographical information of participants (respondents)

Race group	**Frequency**	**%**
Black	258	65
Coloured	44	11
Indian/Asian	20	5
White	78	20
Year born	**Frequency**	**%**
1925–1945 Post-war group	3	1
1946–1954 Baby Boomers 1	11	3
1955–1964 Baby Boomers 2	29	7
1965–1980 Generation X	92	23
1981–2000 Millennials/Generation Y	265	66
Gender	**Frequency**	**%**
Male	208	52
Female	192	48
Education	**Frequency**	**%**
Below Grade 12 in high school	22	6
Grade 12 in high school	153	38
Diploma	95	24
Three-year university degree	46	12
Higher diploma	24	6
Postgraduate certificate	24	6
Honours qualification	19	5
Master’s qualification	13	3
Doctoral qualification	0	0
None	4	1

6.2 Results: Section B – Technology use and privacy concern questions

The results indicate that the participants were very concerned over the processing of their personal information and specifically the protection thereof. Yet, they were significantly less concerned (3.97 mean; 73%) over time to share their information with companies over the internet compared with the results of a previous study (4.09 mean; 79%) (Da Veiga, 2018a). This could be due to familiarity with websites over time (Koohikamali et al., 2019) or due to the appointment of the Information Regulator in South Africa to regulate POPIA. Most of the respondents also seemed not to be too concerned about sharing their personal information with companies in everyday business transactions not involving the internet (3.51 mean; 57%).

However, the majority of the participants remained concerned about their financial (4.49 mean; 90%), health (4.07 mean; 74%) and identification information (4.57 mean; 92%), which corresponds with concern about financial details, addresses, dates of birth and phone numbers among Australians (Van Souwe, Gates, Bishop & Dunning, 2017). Similarly, individuals in Europe were concerned about their financial information (Republic of South Africa, 2019).

Most participants (60%) knew someone who had experienced misuse of their personal information. That could be as a result of the various data breaches that have occurred in South Africa in recent years (Mohapi, 2020). When individuals experience breaches of their personal information, concern for information privacy and specifically concern for financial information result (Mlaba, 2020).

The participants used websites as their main source of information about privacy and privacy rights. Other sources were banks, family, and the organisations they worked for or provided information to, as well as television/radio and schools/universities. Schools played a smaller role, although there have been initiatives to incorporate cyber awareness in school curriculums that could aid awareness from an early age (Department of Basic Education, 2010; Kritzinger, 2017). The preferred method of acquiring information on privacy was in line with the places where it was obtained. Only 42% of the respondents indicated that they had good knowledge about their privacy rights, indicating that more awareness and education were required to ensure that everyone was aware of their rights.

6.3 Results: Sections C and D – Expectations and confidence

The overall privacy expectation among participants was high, with a mean of 4.52 for the items on expectations. Privacy confidence relating to respondents being confident that organisations indeed met privacy conditions was lower than expectations at an overall mean of 3.00 for the confidence items. This indicates that organisations did not meet privacy conditions, which supports the perception of non-compliance with the conditions of POPIA. The gap between expectations and confidence reflected an overall score of 1.52.

The paired statements were compared, resulting in a statistically significant (two-tailed) p-value of 0.000 for all the paired statements. That correlated with the findings of Da Veiga 2018a and showed that the respondents had a very high expectation for privacy across all 11 information privacy conditions. However, they felt that none of the information privacy conditions were met in practice and as such their expectations were not met, resulting in the gap that also illustrates the perception of non-compliance with the conditions of POPIA.

Table 4 shows the privacy condition in column 1, with the related expectation and confidence means in columns 2 and 3. The t-values for the significance test are included for each pair under “t”. The gap column provides the difference between the expectations and the confidence means. The results of table 4 show that the expectation for privacy was very high, but that the level of confidence that expectations and privacy conditions were met in

practice was low. The results thus reflect a gap in terms of the paired statements, with a significant difference for all the statement pairs.

Table 4: Significant differences between statement pair means

Privacy condition of combined expectation and confidence item concept	Privacy expectation mean	Mean for confidence items	t	Gap
"a. Notify me before they start collecting my personal information."	4.54	3.03	18.555	1.51
"b. Use my personal information in a lawful manner."	4.63	2.97	19.357	1.66
"c. Privacy when a company has to process my personal information for services or products."	4.63	3.02	18.875	1.61
"d. Not to collect excessive or unnecessary information from me."	4.23	3.08	12.637	1.15
"e. Only collect my personal information when I have given my consent or for a legitimate business reason."	4.56	3.08	17.258	1.48
"f. Only collect my personal information from myself and not from other sources."	4.48	2.96	17.386	1.52
"g. Explicitly define the purpose for which they want to use my information."	4.60	3.01	20.180	1.59
"h. Only use my personal information for purposes I agreed to and never for other purposes."	4.60	2.92	19.160	1.68
"i. Only keep my personal information for as long as required for business purposes or regulatory requirements."	4.39	3.34	13.933	1.05
"j. Obtain my consent if they want to use my personal information for purposes not agreed to with them."	4.55	2.86	19.676	1.69
"k. Inform me of the conditions."	4.56	2.93	20.425	1.63
"l. Keep my personal information updated."	3.93	2.98	12.348	0.95
"m. Protect my personal information."	4.76	3.01	22.476	1.75
"n. Organisations to have all the necessary technology and processes in place to protect my personal information."	4.69	3.10	20.541	1.59
"o. Ensure that third parties have all the necessary technology and processes in place to protect my information."	4.52	2.94	19.019	1.58
"p. Inform me if records of my personal data were lost, damaged or exposed publicly."	4.69	2.88	21.731	1.81
"q. Inform me what records or personal information they have about me."	4.54	3.07	19.097	1.47
"r. Correct or delete my personal information at my request."	4.54	3.06	18.407	1.48

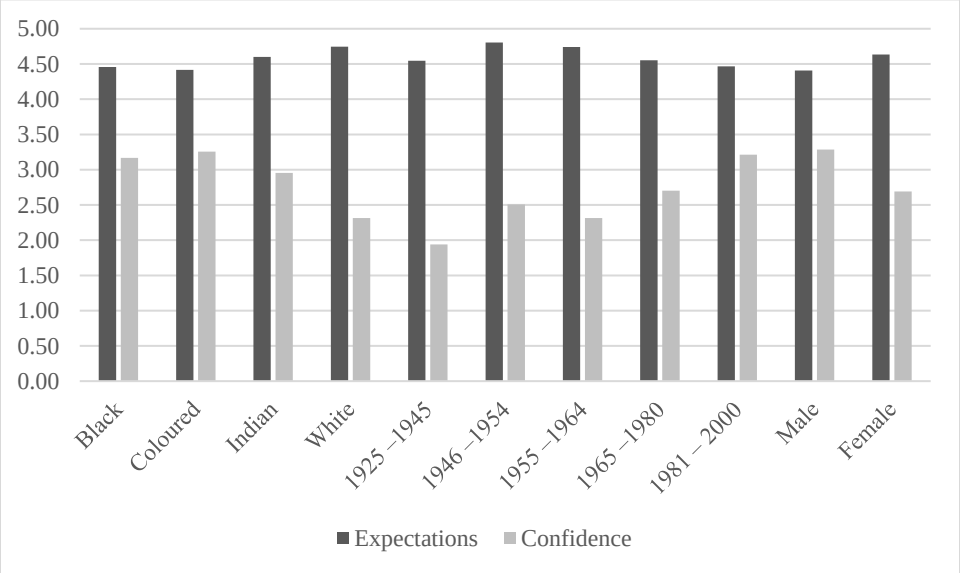
Privacy condition of combined expectation and confidence item concept	Privacy expectation mean	Mean for confidence items	t	Gap
"s. Do not collect sensitive personal information about me."	4.26	2.86	17.019	1.4
"t. Honour my choice if I decide not to receive direct marketing."	4.56	2.95	19.023	1.61
"u. Give me a choice whether I want to receive direct marketing from them."	4.52	3.10	16.961	1.42
"v. Protect my information when they have to send it to other countries."	4.63	2.90	21.520	1.73

(Statements of the IPCI (Da Veiga, 2018a)

6.4 Results: Sections C and D – Expectations and confidence of demographical groups

The expectations and confidence means for the age, gender and race groups are shown in figure 3. The groups with the highest privacy expectations were Baby Boomers 1 (1946–1954), females and white participants. The groups with the lowest privacy expectations were the Generation Y group, males, Coloured participants and black participants. All the groups reflected a discrepancy between the expectation for privacy and confidence that organisations were meeting privacy principles. The groups that were the most negative in this regard were the Post-war group, Baby Boomers 2 (1955–1964), females and white participants; the Generation Y group, males, black participants and Coloured participants were more positive.

Figure 3: Expectations and confidence of demographical groups



Comparisons of column proportions were conducted in SPSS to identify significant differences ($p > .05$) based on two-sided tests for the age, gender and race groups, with the results in table 5 in the appendix. The table in the appendix displays the statements for three sections of the IPCI with the corresponding means for the items that had significant differences for the age, gender and race groups. A summary of the key findings for the significant differences is provided below.

Age

- **Technology use and privacy concern questions**: The results of this study show one significant difference concerning age. A significantly higher percentage of Generation X (1965–1980) than Baby Boomers 2 (1955–1964) knew someone whose personal information had been misused.
- **Expectations:** There were no significant differences between the age groups in the expectations section.
- **Confidence:** The confidence section revealed 13 significant differences. While still reflecting a negative perception, the Generation Y (1981–2000) group had significantly more confidence that companies were meeting privacy conditions than the other age groups, specifically participants belonging to the Generation X and Baby Boomers 2 groups.

Studies in Europe found that people in the age group 45 to 60 years (Baby Boomers) had a higher concern about privacy, while younger people (19–24 years/Generation Y) were less concerned about privacy (Miltgen & Peyrat-Guillard, 2014) – which is in line with the results of this study. A study in the Western Balkans also indicated that older people were more concerned about privacy (Budak, Rajh & Anić, 2015), which also supports the results of this study. All the age groups in this study had equally high privacy expectations. However, while the Generation Y participants were not confident that companies were meeting privacy principles, they were more positive about it than the Generation X and Baby Boomer participants.

Gender

- **Technology use and privacy concern questions**: Males in this study were significantly more positive than females about their knowledge of privacy rights. However, they experienced significantly greater loss or harm due to misuse of personal information than females.
- **Expectations:** There were 18 significant differences in the expectations section. Females had a significantly higher expectation for privacy than males for the respective privacy principles.
- **Confidence:** There were 13 significant differences in the confidence section where, apart from one item, all the items reflected a significant difference between males and females concerning greater positivity that organisations were meeting their privacy expectations.

Previous studies found that females were more concerned about their privacy than males and that females would implement more measures to protect their privacy (Baruh, Secinti & Cemalcilar, 2017; Gerber et al., 2018; Regan et al., 2013; Tifferet, 2019). In contrast, a study in Croatia (Anic, Škare & Milaković, 2019), supported by a study in Hong Kong (Hong et al., 2021), found no difference between gender and age groups for online privacy concern. The significant differences among gender groups in this study show that the female participants in South Africa had significant higher expectations for privacy and significant lower confidence that privacy was met in practice than their male counterparts.

Race groups

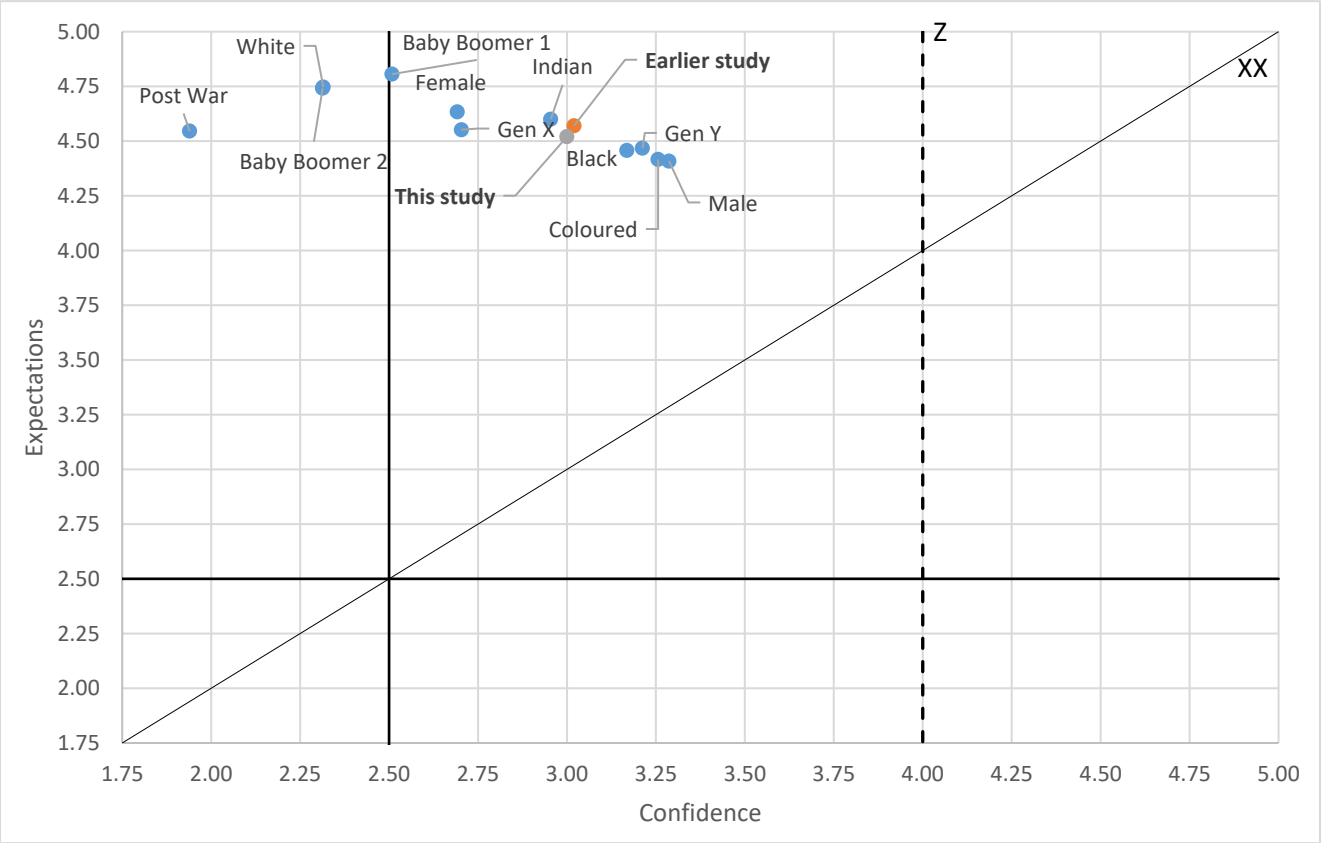
- **Technology use and privacy concern questions**: Black participants in this study were significantly more concerned about the protection of their personal information, specifically their health information. They also experienced greater loss due to information misuse than white participants.
- **Expectations:** The expectations section showed 14 significant differences among race groups. Of all the groups, the white participants had a higher expectation for privacy than the black participants.
- **Confidence:** There were 13 significant differences in the confidence section, with the black and coloured participants significantly more confident than the white participants that organisations were meeting privacy principles.

There are limited studies on privacy concerns among race groups in South Africa. Studies have been conducted in the United States, where it was found that white people tended to be less concerned about privacy than black people (Regan et al., 2013). More recent industry surveys showed that there were different perceptions about privacy issues between white and black adults in the United States. The study of Auxier et al. (2019) showed that black American adults were more concerned about what others knew about them compared with white adults; whereas the results of this study showed that, compared with the black participants, the white participants had a significantly higher expectation for privacy and were significantly less confident that organisations were meeting privacy principles in practice.

6.5 Index for the information privacy concerns and expectations

Figure 4 reflects the index for the IPCI based on the data of this study and the data of an earlier study of Da Veiga 2018a where 1007 participants participated. The data were plotted, with the x-axis representing the confidence means and the y-axis the expectation means. The values of the survey in this study (3.00; 4.52) and those of the earlier study (3.02; 4.57) are closely aligned, as reflected in quadrant 3. The index also shows the means of the demographical groups based on the data of this study only as the earlier study did not include an analysis of the data across demographical groups. The South Africans participating in this study had a high expectation for privacy. However, their experience in practice was that organisations were not mature in meeting the principles of privacy. Hence, their confidence in compliance was low, which represents a gap between expectations and compliance confidence, contributing to concern for information privacy across all the demographic groups.

Figure 4: Index for the information privacy concerns and expectations



A gap concerning expectation and compliance confidence means presented for all the demographic groups. Had there been a match between the compliance confidence and expectation means, the two survey points would have been on diagonal line XX. The survey points are to the left of line Z, hence the gap between the compliance experienced by participants and the minimum data protection requirements, indicating a gap between perceived organisational compliance and POPIA and that privacy expectations were not met.

The slight differences between the means of the two surveys relate to changes in perceptions. Compared with the first study (significant difference $p < 0.05$), the respondents in this study's survey showed significantly less concern over four of the statements in sections C and D relating to expectations that companies should only collect personal information when consent is given or if it is necessary for a legitimate business reason (4.64; 4.56); that companies should ensure that their third parties (e.g. suppliers and vendors) have the necessary technology and processes in place for the processing and security of personal information (4.64; 4.52); and that companies should honour the choice of individuals to either opt out of (4.66; 4.56) or opt in (4.67; 4.52) to receive direct marketing.

The graph in figure 5 aids in comprehending the perceptions of different demographic groups. Organisations could leverage this information to improve their privacy programmes and awareness initiatives based on the market segment targeted. For example, if Baby Boomer 2s are part of the customer profile of an organisation, specific and more attention should be given to improve the confidence of that group that the organisation would indeed protect their privacy compared with, for example, Generation Y customers.

7 Discussion and Implications

An objective of this study was to expand the understanding of information privacy concerns and expectations in South Africa across demographical groups. An understanding of the relevant privacy concerns and expectations was achieved by conducting an online survey in South Africa using the IPCI questionnaire. Significant differences were identified for age, gender and race groups. The results of the survey show that participating South Africans had very high privacy expectations while not perceiving in practice that organisations were meeting their expectations. Furthermore, they had the perception that organisations were not meeting the regulatory requirements of POPIA. All the paired statements in the survey had a statistically significant difference between expectations and confidence. A further objective was to determine if there was a change in the privacy perceptions of this study compared with data of an earlier study (Da Veiga, 2017, Da Veiga 2018a) where the IPCI was originally developed and applied to collect data in South Africa. South Africans were very concerned about the protection of their personal information in both studies. The perception remained consistent over time, with a slight decrease in the means from the earlier survey to the survey conducted in this study, but not statistical significant. The results of the information privacy concerns and expectations in South Africa across demographical groups as well as the means of this survey and the earlier survey (Da Veiga 2017, Da Veiga 2018a) were depicted on the proposed index for the information privacy concerns and expectations as illustrated in figure 4. Organisations establish trust with consumers if they respect and protect customer data, whereas the consequences of a weak privacy posture and the lack of respect for personal data of consumers have negative consequences for organisations (ISACA, 2021) and results in a lack of trust (Martin, 2016). Consumer trust in privacy measures is critical and organisations need to illustrate that they are protecting privacy and meeting privacy expectations.

South Africa is classified as "moderate" in respect of privacy regulation and enforcement (DLA Piper, 2022). While POPIA came into effect on 1 July 2020, the grace period for compliance only elapsed on 30 June 2021. As such, the Information Regulator could only start to enforce the conditions of the Act actively from 1 July 2021. It

is expected that views on privacy and compliance with POPIA will mature over time as organisations implement their data protection compliance programmes and the Information Regulator enforces POPIA requirements. Similarly, information privacy concerns and expectations might change over time as individuals become more aware of their privacy rights and experience data breaches or become more conscious of the lawful processing of their personal information by organisations. The data of this study provide a baseline for benchmarking information privacy concerns and expectations after commencement of POPIA and for continuous monitoring over time. The benefit is that recommendations can be identified to direct interventions in order to uphold privacy requirements and to meet individual information privacy expectations as well as to address areas of non-compliance or concern as perceived by individuals across the demographic groups.

8.1 Practice implications

The practice and managerial implications of this study relate to the findings that organisations are perceived as not complying with POPIA and not meeting consumers' privacy expectations. To address this, organisations should prioritise the implementation of the data privacy requirements of POPIA to meet privacy expectations and privacy regulatory requirements. A privacy principle framework is seen as one of the most effective assets to assist organisations in achieving privacy compliance (ISACA, 2021). According to ISACA, the General Data Protection Regulation, National Institute of Standards and Technology (NIST) Privacy Framework, and ISO/IEC 27002:2013 Information Technology-Security Techniques – Code of Practice for Information Security Control are the three most-used frameworks to manage privacy in organisations that can also be used by organisations in South Africa. Participants in this study perceived organisations as not meeting the POPIA conditions across all 11 constructs of the IPCI. The perceptions about the practices of organisations thus indicate a view of non-compliance with POPIA. Since the IPCI does not constitute a compliance audit, it is recommended that organisations review their data processing practices and implement privacy programmes to meet the privacy regulatory requirements by considering POPIA as well as related ICT laws and regulations in South Africa for the protection of personal information.

Governance of privacy in existing structures should also be implemented and internal oversight should be ensured (OECD, 2013). The privacy conditions should be implemented across the full life cycle of personal information processes, including all formats and systems. Such a programme should extend to third parties processing personal information on behalf of the responsible party. Furthermore, employee training and awareness should be implemented (Weller & Leach, 2020). Privacy impact assessments, self-assessments, audits and privacy by design are also important aspects requiring incorporation (Debos, 2021; ISACA, 2021). Organisations should implement redress mechanisms for their customers to aid in giving customers control of their information processing. Consequently, organisations would also comply with the human rights requirement of meeting privacy rights in the digital age (CIPESA, 2018). In addition, section 5 of POPIA (pertaining to codes of conduct) is now effective. South African organisations and industries are therefore urged to participate in developing codes of conduct. The South African universities and researchers embarked on such a project when Universities South Africa (which represents public universities in South Africa) drafted a code of conduct (Universities South Africa, 2020). The Academy of Science of South Africa is also developing a code of conduct for research, focusing on aspects such as consent and social media in research (Adams, Veldsman, Ramsey & Soodyall, 2021).

Furthermore, organisations should ensure that customers are aware of the practices and controls implemented to protect their information by communicating it in their terms and conditions as well as in their privacy policies on data processing. They should also implement communication and awareness programmes to inform customers of

their practices to uphold privacy. That would aid in increasing trust in organisations, as would organisations meeting the privacy expectations of individuals when handling their personal information. Failure to meet privacy expectations could, however, be perceived as harmful by individuals (Martin, 2016). Privacy information should continue to be shared using the preferred information sources as indicated in the results of this study (namely websites; banks and organisations; television/radio; and schools, colleges and universities) to create awareness about privacy rights and the practices organisations implement to comply with POPIA and meet individual privacy expectations.

Several specific recommendations for South African public and privacy bodies to concentrate on have been identified based on the IPCI statements that scored the lowest in the study. For the recommendations to be addressed successfully, organisations should ensure that there is an accountable role for privacy in the organisation such as a chief information officer or chief privacy officer. Such roles will aid in ensuring that resources and support are made available to implement the regulatory requirements for privacy (ISACA, 2021). The relevant recommendations are the following:

- **Demographical groups**. Governments and organisations need to pay special attention to the privacy preferences and expectations of race, age and gender groups. While all groups in this study displayed negative perceptions about their privacy expectations being met, the Baby Boomers 2 group, the Generation X group, females and white participants were significantly more negative compared with the other groups. The Generation Y group, as well as males, black participants and coloured participants were significantly more positive that organisations were implementing the privacy principles. The concern for privacy differs from one study to the next, from one country to the next, and from one demographical group to the next. It is therefore recommended that organisations establish the privacy concerns and expectations of their customers to develop tailored interventions for each group in order to minimise privacy concern and meet privacy expectations using for example customer awareness and communication to address unique expectations and concerns of the various demographic groups. Similarly, regulators should determine the privacy concerns of their citizens to inform strategy and policy. Researchers are called on to conduct more research in this area, as there are limited studies on privacy concern across demographical groups in South Africa.
- **Breach notification process**. Respondents indicated that that they were not confident that organisations would inform them if their personal data were lost, damaged or exposed publicly (2.88). There were no significant differences between the demographic groups for confidence in whether organisations would inform them of a data breach of personal information. However, from an expectations perspective, females had a significant higher expectation that organisations should inform them if their personal information were lost, damaged or exposed publicly. Section 22 of POPIA requires public and private organisations to have a notification process in the event of a security compromise (e.g., access to personal information by an unauthorised person). The study participants also indicated that they were not confident that organisations would inform them if their data had been breached. Organisations should define such a process in line with the requirements of section 22 of POPIA. Multinational organisations should also ensure compliance with data privacy laws of other jurisdictions, such as the GDPR in terms of which organisations could face up to 4% of their total global turnover in the event of a fine.
- **Further processing and consent**. Participants neither felt positive that their personal information was only used for purposes they had agreed to and not for other purposes (2.92), nor that their consent was obtained for further processing (2.86). White participants had a significant higher expectation than the

black and coloured participants, and females had significant higher expectation than males, that consent should be obtained for further processing of their personal information; however, the results show that they had significant less confidence that organisations were obtaining their consent for further processing. In addition, Generation X was significantly less confident than Generation Y that organisations were obtaining their consent for further processing. In terms of section 15 under condition 4 of POPIA, further processing of personal information may only occur if it is in line with the original purpose of the collection. Where that is not the case, several requirements apply, such as consent for the further processing.

- **Transborder information flows**. Participants felt that information was not necessarily protected when sent across the borders of South Africa (2.9). Females had a significant higher expectation than males that organisations should protect their information when sending it to other countries. Responsible parties are prohibited from transferring personal information to a foreign country unless several conditions are met. Therefore, organisations should ensure that transborder flow of information – whether via internal organisational systems, the cloud, e-mail or other electronic platforms – complies with the Act and individuals are made aware of protection mechanisms as part of awareness exercises. Such mechanisms should also be included in terms and conditions and related privacy policies.
- **Third-party protection**. The perception of study participants was that their information was not protected adequately when responsible parties sent it to third parties (2.94). White participants had a significant higher expectation than black participants; and females had a significant higher expectation than males, that companies should ensure that their third parties had all the necessary technology and processing in place when sharing personal information with them. Section 20 of POPIA stipulates that responsible parties must have a written contract in place with third parties (the "operator") in which security measures to protect the processing of personal information are agreed to. Organisations must review third-party contract processes to ensure that all third parties have contracts in place that stipulate applicable privacy and security requirements. Individuals should also be made aware of the third-party categories with which their information is shared, as required in section 23 of the Act.
- **Direct marketing**. The respondents indicated that their choice to opt out of direct marketing was not honoured (2.95). White participants had a significant higher expectation than black participants and coloured participants that companies should give them a choice if they wanted to receive direct marketing; similarly, females had a higher expectation of this than males. Section 69 of POPIA requires that individuals only be contacted for similar products or services if their personal information was obtained in the context of the sale of a product or service together with other provisions of section 69. Individuals can opt out of future direct marketing and potential customers may only be contacted once, whereafter they must opt in for future direct marketing. Studies showed that the opt-in and opt-out choices of customers are not met (Zenda, Vorster & Da Veiga, 2020). As such, organisations should review their marketing processes and implement measures to comply with the direct marketing requirements of the Act.
- **Openness**. Participants expected organisations to inform them of the conditions (e.g., purpose and consequences of data collection, recipient categories, their rights, and confidentiality and security protection) for processing personal information and they felt that was not done (2.93). The gender group was the only group where there was a significant difference for expectations, with females having a significant higher expectation than males that organisations should information them of the processing conditions of their personal information. The white participants were significantly less

confident compared to all the other race groups that companies were adequately informing them of processing conditions; females were also significantly more negative than males; and Generation X and Baby Boomers 2 were significantly less confident than Generation Y in this regard. Section 23 of POPIA stipulates that data subjects have the right to ask responsible parties what personal information they hold about them. In South Africa, organisations must furthermore abide by the provisions of PAIA. Responsible parties must also ensure that data subjects are aware of the list of specific information detailed in section 18 of POPIA when their personal data are collected. That list includes the name and address of the responsible party, whether data provision is voluntary or mandatory, and privacy rights. Organisations must update their application forms, terms and conditions, and privacy policies to reflect this requirement.

- **Sensitive personal information collection**. Respondents indicated that they were not confident that organisations only collected sensitive personal information with their consent (2.86). White participants had a significant higher expectation than black participants that organisations should not collect sensitive personal information about them, and females had a significantly higher expectation than males in this regard. Individuals need to trust organisations to not collect unnecessary personal information (in line with the minimality principle) or special personal information as outlined in section 26 of POPIA, for example information about children or health, unless such collection meets the requirements of POPIA. Organisations should review the content of online and hard-copy data collection forms, whether on paper or in electronic format, and verify that no unnecessary personal information is collected. Forms should be updated and additional controls should be implemented in the event of special personal information being collected.
- **Collection from data subject**. Section 12 under condition 2 of POPIA requires responsible parties to collect personal information directly from data subjects, except if certain conditions are met. Organisations should review their data collection processes whereby individual data are collected from third parties to ensure that the relevant conditions are met, since respondents did not perceive that as happening in practice (2.96). White participants had a significantly higher expectation than black participants; and females had a significant higher expectation than males, that organisations should collect their personal information directly from them.

The IPCI can further be mapped to the data privacy laws of other jurisdictions to measure the as-is information privacy concerns and expectations, and to plot the latter on the proposed index. That could be beneficial in providing insight into the privacy concerns and expectations of various jurisdictions and how responsible parties could align their data processing with applicable regulatory requirements. It could also shed some light on the expectations of individuals to improve compliance and minimise information privacy concerns. Regulators could furthermore benefit from the outcome of this assessment by using the results obtained as input for policy, strategic planning and awareness, training and implementation guidance for responsible parties. That would be of specific value where organisations have a global presence with customers across jurisdictions, each with possible different privacy expectations. Understanding the customer base and implementing different strategies to meet privacy expectations could aid in addressing privacy concerns.

8.2 Theoretical implications

From a theoretical contribution perspective, the study illustrates that age, gender and race groups have different privacy expectations and confidence levels. Interventions to address information privacy concern should not be generic across a population or customer base, but should be tailored to different age, gender and race groups.

Understanding customer concerns and preferences could aid organisations in understanding market trends and meeting the demands of different customer groups more successfully. The proposed index for the IPCI could be used in future studies to assist in comprehending information privacy concerns and expectations visually and to monitor change over time, not only in South Africa but also in other jurisdictions. The IPCI and the corresponding index could furthermore be used to identify improvement actions to address information privacy concerns among individuals and different groups of individuals in a population, thereby aiding to improve trust and compliance with regulatory requirements for data privacy. The index for the IPCI provides a novel approach to understanding concern for information privacy in the context of privacy expectations aligned with privacy principles.

9. Limitations and Future Research

It is acknowledged that this study was conducted prior to the commencement of POPIA and that the sample size was 400 therefore representing the perception of respondents in this study and should be repeated to further monitor changes in privacy concerns and expectations. That would enable researchers to monitor changes in perceptions and compliance maturity among organisations. It would also provide additional data for a longitudinal study. It is recommended that further studies be conducted in other jurisdictions to allow comparison of information privacy concerns and expectations between individuals in different jurisdictions that can provide input to guidelines for cross-border transfers. It is acknowledged that a correlation analysis between the demographical groups was not conducted and that it should be included in future studies. The scope of the IPCI is limited to POPIA and other ICT regulations and laws were not incorporated. Future research can be conducted to further expand the IPCI with incorporation of relevant ICT regulations and laws that might be applicable to the protection and security of personal information such as the Cybercrimes Act of South Africa which is still to commence.

10. Conclusion

This study aimed to expand the understanding of information privacy concerns and expectations in South Africa across demographical groups. An online survey was conducted using the IPCI. The results indicate that privacy concern remains high in South Africa, while confidence in organisations meeting data privacy principles remains low. Differences between age, gender and race groups were investigated, which showed that white participants had higher privacy expectations than black participants and less confidence that organisations were meeting privacy requirements; females had higher expectations for privacy than males, and they had less confidence in organisations meeting privacy principles; and the Generation Y group had lower expectations for privacy than older participants, but more confidence that organisations were meeting privacy principles. Specific recommendations are made for organisations to address information privacy concerns and compliance aspects relating to POPIA conditions. The proposed IPCI index portrays the information privacy concerns and expectations of the demographical groups visually and aids in understanding relevant differences (that is, that each group indeed had different privacy expectations and varying confidence in organisations meeting privacy conditions). The proposed index for the IPCI can be used to conduct further information privacy concern studies to track changes over time, not only in South Africa but also in other jurisdictions for comparison studies.

Grant
National Research Foundation, Research Development Grant for Y-rated Researchers, Grant number 105735.

Declaration of competing interest

The author declares that she has no conflict of interest in relation to this paper.

References

Adams, R., Veldsman, S., Ramsay, M., & Soodyall, H. (2021). Drafting a code of conduct for research under the Protection of Personal Information Act No. 4 of 2013. *South African Journal of Science*. 117(5/6), 1–3.

Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing*, 31(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

Anic, I. D., Škare, V., & Kursan Milaković, I. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications*, 36(2019), Article 100868. https://doi.org/10.1016/j.elerap.2019.100868

Arslan, F., & Dayyala, N. (2017). Cultural and generational influences on information privacy concerns within online social networks: An empirical evaluation of the Miltgen and Peyrat-Guillard Model. *Journal of Information Privacy and Security*, 13(4), 1–22. https://doi.org/10.1080/15536548.2017.1412114

Asia-Pacific Economic Corporation (APEC). (2005). APEC Privacy Framework, APEC Secretariat, Singapore. https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and privacy: Concerned, confused, and feeling a lack of control over their personal information. *Pew Research Center*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Baloyi, N., & Kotze, P. (2017a). Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? In *Proceedings of the 2017 IST-Africa Week Conference, IST-Africa*, 2017, pp. 1–11. https://doi.org/10.23919/ISTAFRICA.2017.8102340

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

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

Blauw, F. F., & Von Solms, S. (2017). Towards quantifying and defining privacy metrics for online users. In *Proceedings of the IST-Africa Week Conference, IST-Africa*, 2017, pp. 1–9. https://doi.org/10.23919/ISTAFRICA.2017.8102366

Budak, J., Rajh, E., & Anić, I. D. (2015). Privacy concern in Western Balkan countries: Developing a typology of citizens. *Journal of Balkan and Near Eastern Studies*, 17(1), 29–48. https://doi.org/10.1080/19448953.2014.990278

Cheah, J. H., Lim, X. J., Ting, H., Liu, Y., & Quach, S. (2022). Are privacy concerns still relevant? Revisiting consumer behaviour in omnichannel retailing. *Journal of Retailing and Consumer Services*, 65(c), 1–12. https://doi.org/10.1016/j.jretconser.2020.102242

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60–67.

Collaboration on International ICT Policy in East and Southern Africa (CIPESA). (2018). State of internet freedom in Africa 2018. Privacy and data protection in the digital era: Challenges and trends in Africa. https://iapp.org/resources/article/privacy-and-data-protection-in-the-digital-era-challenges-and-trends-in-africa/

Da Veiga, A. (2017). An Information Privacy Culture Index Framework and Instrument to measure privacy perceptions across nations: Results of an empirical study. In S. Furnell & N. Clark (Eds.), *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA)* (pp. 196–209). Plymouth University.

Da Veiga, A. (2018a). An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information & Computer Security*, 26(3), 338–364. https://doi.org/10.1108/ICS-03-2018-0036

Da Veiga, A. (2018b). An online information privacy culture. *2018 Conference on Information Communications Technology and Society (ICTAS)*, 2018, pp. 1–6. https://uir.unisa.ac.za/bitstream/10500/25048/1/ICTAS2018_paper_49%2014022018.pdf

Da Veiga, A. (2020). Concern for information privacy in South Africa: An empirical study using the OIPCI. In H. Venter, M. Loock, M. Coetzee, M. Eloff, J. Eloff J & R. Botha (Eds.), *Information and Cyber Security. ISSA 2020. Communications in Computer and Information Science*, 1339, (pp. 65–80). Springer, Cham. https://doi.org/10.1007/978-3-030-66039-0_5

Da Veiga, A., Ophoff, J. (2020). Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa. Human Aspects of Information Security and Assurance, *IFIP Advances in Information and Communication Technology*, Springer, pp. 16-29.

Debos, B. T. (2021). How to successfully embed a culture of privacy by design. https://www.ey.com/en_gl/cybersecurity/how-to-successfully-embed-a-culture-of-privacy-by-design

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, 50, 261–272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

Deloitte Touche Tohmatsu (DTTL). (2017). Privacy is paramount, Personal data protection in Africa. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Department of Basic Education. (2010). Guidelines on e-Safety in Schools: Educating towards responsible, accountable and ethical use of ICT in education. https://wcedonline.westerncape.gov.za/documents/eLearning/eLearningCircMins/minutes/del4_18.pdf

DLA Piper. (2022). Data protection laws of the world. https://www.dlapiperdataprotection.com/

Esmaeilzadeh, P. (2019). The effects of public concern for information privacy on the adoption of health information exchanges (HIEs) by healthcare entities. *Health Communication*, 34(10), 1202–1211. https://doi.org/10.1080/10410236.2018.1471336

Fair Information Practice Principles (FIPPs). (n.d.). *IT Law Wikia*. https://itlaw.wikia.org/wiki/Fair_Information_Practice_Principles

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Harper, J. (2021). Privacy and fair information practices – The struggle to protect threatened values, American Enterprise Institute. https://www.aei.org/wp-content/uploads/2021/04/Privacy-and-Fair-Information-Practices.pdf?x91208

Head, M., & Yuan, Y. (2001). Privacy protection in electronic commerce – A theoretical framework. *Human Systems Management*, 20(2), 149–160.

Heales, J., Cockcroft, S., & Trieu, V. H. (2017). The influence of privacy, trust, and national culture on internet transactions. In G. Meiselwitz (Ed.), *Social Computing and Social Media. Human Behavior. SCSM 2017*. Lecture Notes in Computer Science, 10282 (pp. 159–176). Springer, Cham. https://doi.org/10.1007/978-3-319-58559-8_14

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, 168(2021), 539–564. https://doi.org/10.1007/s10551-019-04237-1

ISACA. (2021). Privacy in practice 2021 – Data privacy trends, forecasts and challenges. https://www.isaca.org/go/privacy-in-practice-2021-survey

Information Security Forum (ISF). (2004). Managing privacy – Overview. Information Security Forum Limited, 1–4.

Internet Society and the Commission of the African Union. (2018). Personal Data Protection Guidelines for Africa. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

Jordaan, Y. (2007). Information privacy issues: Implications for direct marketing. *International Retail and Marketing Review*, 3(1), 42–53. http://hdl.handle.net/10500/3073

Jordaan, Y., & Ndhlovu, T. N. (2017). The role of demographics and Facebook activities in users' concerns about online privacy. *Journal of Contemporary Management*, 14(2017), 940–962. https://repository.up.ac.za/bitstream/handle/2263/64007/Jordaan_Role_2017.pdf?sequence=1&isAllowed=y

Kaushik, K., Kumar Jain, N., & Kumar Singh, A. (2018). Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications*, 32(2018), 57–68. https://doi.org/10.1016/j.elerap.2018.11.003

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems*, 119(2019), 46–59. https://doi.org/10.1016/j.dss.2019.02.007

Kosmala, P. B. (2020). Engineering a culture of privacy. *IEEE Consumer Electronics Magazine*, 9(2), 83–88. https://doi.org/10.1109/MCE.2019.2954562

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, 29(2), 16–35. https://doi.org/10.18489/sacj.v29i2.471

Kumaraguru, P., & Cranor, L. F. (2005). Privacy indexes: A survey of Westin's studies. https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

Kuo, K. M., Talley, P. C., & Ma, C. C. (2015). A structural model of information privacy concerns toward hospital websites. *Program: Electronic library and information systems*, 49(3), 305–324. https://doi.org/10.1108/PROG-02-2014-0014

Lee, H., Wong, S. F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly*, 36(2), 294–303. https://doi.org/10.1016/j.giq.2019.01.002

Longerman Research. (2020). Australian Community Attitudes to Privacy Survey 2020. https://www.adma.com.au/sites/default/files/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research*, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mapande, F. V., & Dagada, R. (2017). Users' perceptions of mobile computing system in South Africa: The case for further research. In *Proceedings of the 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2016, pp. 265–269. https://doi.org/10.1109/ICACCE.2016.8073759

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, 137(2), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), 103–125. https://doi.org/10.1057/ejis.2013.17

Mlaba, K. (2020, December 23). *1 in 5 South Africans are living in extreme poverty: UN Report*. Global Citizen. https://www.globalcitizen.org/en/content/1-in-5-south-africans-living-extreme-poverty-un/

Mohapi, T. (2020, October 27). *South Africa's notable data breaches and data leaks in the past half-decade*. iAfrikan. https://iafrikan.com/2020/10/27/south-africa-biggest-top-data-breaches-leaks/

Morton, A., & Sasse, M. A. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences. *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 2014, (pp. 102–111). https://ieeexplore.ieee.org/document/6890929

OneTrust DataGuidance. (2020). Comparing privacy laws: GDPR v. POPIA. https://www.dataguidance.com/sites/default/files/onetrustdataguidance_comparingprivacylaws_gdprvpopia.pdf

Organisation for Economic Co-operation and Development (OECD). (2011). Thirty years later – The OECD Privacy Guidelines. https://www.oecd.org/sti/ieconomy/49710223.pdf

Organisation for Economic Co-operation and Development (OECD). (2013). *The OECD Privacy Framework*. OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Chapter 1). https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf https://doi.org/10.1016/0376-5075(81)90068-4

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior*, 49, 324–332. https://doi.org/10.1016/j.chb.2015.02.062

S. Parker, & Van Belle, J.P. (2015). Lifelogging and lifeblogging: Privacy issues and influencing factors in South Africa, In *Proceedings of Second International Conference on Information Security and Cyber Forensics (InfoSec)*, pp. 111-117, doi: 10.1109/InfoSec.2015.7435515.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal–agent perspective. *MIS Quarterly*, 31(1), 105–136. https://doi.org/10.2307/25148783

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27–41. http://www.jstor.org/stable/30000485

Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level – A literature review. *Vilakshan – XIMB Journal of Management*, 18(2), 171–186. https://doi.org/10.1108/xjm-08-2020-0096

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, 26(1–2), 81–99. https://doi.org/10.1080/13511610.2013.747650

Republic of South Africa. (1996). Constitution of the Republic of South Africa Act No. 108 of 1996, Government Gazette No. 17678.

Republic of South Africa. (2000). Promotion of Access to Information Act (PAIA) No. 2 of 2000. Government Gazette No. 20852. https://www.gov.za/documents/promotion-access-information-act#:~:text=The%20Promotion%20of%20Access%20to,provide%20for%20matters%20connected%20theretith

Republic of South Africa. (2002). Electronic Communications and Transactions Act (ECTA) No. 25 of 2002. Government Gazette No. 23708. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

Republic of South Africa. (2013). Protection of Personal Information Act (POPIA) No. 4 of 2013. Government Gazette No. 37067. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Republic of South Africa. (2019). RSA Data Privacy and Security Survey 2019: The growing data disconnect between consumers and businesses. https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf

Rook, L., Sabic, A., & Zanker, M. (2020). Engagement in proactive recommendations: The role of recommendation accuracy, information privacy concerns and personality traits. *Journal of Intelligent Information Systems*, 54(1), 79–100. https://doi.org/10.1007/s10844-018-0529-0

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Pearson: Harlow.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. https://doi.org/10.2307/249477

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459–468. https://doi.org/10.1037/0021-9010.68.3.459

Taplin, K. (2021). South Africa's PNR regime: Privacy and data protection. *Computer Law & Security Review*, 40, 105524.

Teufel, H. (2008). The Fair Information Practice Principles: Framework for Privacy – Policy at the Department of Homeland Security, Privacy Policy Guidance Memorandum. Memorandum No. 2008-01, Homeland Security. https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93, 1–12. https://doi.org/10.1016/j.chb.2018.11.046

Tshiani, V., & Tanner, M. (2018). South Africa's quest for smart cities: Privacy concerns of digital natives of Cape Town, South Africa. *Interdisciplinary Journal of e-Skills and Lifelong Learning*, 14, 55–76. https://doi.org/10.28945/3992

Universities South Africa. (2020). POPIA Industry Code of Conduct: Public Universities. https://www.usaf.ac.za/wp-content/uploads/2020/09/USAf-POPIA-Guideline_Final-version_1-September-2020.pdf

Van der Merwe, M. D., & Van Staden, W. J. (2015). Unsolicited short message service marketing: A preliminary investigation into individual acceptance, perceptions of content, and privacy concerns. In *Proceedings of the Information Security for South Africa (ISSA) Conference*, pp. 1–7. https://doi.org/10.1109/ISSA.2015.7335072

Van Souwe, J., Gates, P., Bishop, B., & Dunning, C. (2017, May 4). *Australian community attitudes to privacy survey 2017*. APO Analysis & Policy Observatory.

Warren, S. D., & Brandeis D. L. (1890). The right to privacy. *Harvard Law Review,* 4(5), 193–220.

Weller, A., & Leach, E. (2020). How to build a 'culture of privacy'. *The Privacy Advisor*, IAPP. https://iapp.org/news/a/how-to-build-a-culture-of-privacy/

Westin, A. F. (2003). Social science perspectives on privacy. *Journal of Social Issues*, 59(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Zenda, B., Vorster, R., & Da Veiga, 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://doi.org/10.18489/sacj.v32i1.712

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries (SAICSIT)*, 2007, pp. 197–204. https://doi.org/10.1145/1292491.1292514

Appendix

Table 5: Race group significant differences

The table displays only the items with significant differences. Grey cells indicate that there was no significant difference for the respective group.

	Questions section	Race groups mean or %	Age groups mean or %	Gender groups mean of %
	Section B: Technology use and privacy concern questions			
1.	Q11. "How concerned are you about the protection of your personal information? "	Black 4.32* White 3.83		
2.	Q12. "How would you rate your knowledge of your privacy rights? "			Male 3.63* Female 3.16
3.	Q15. "Do you know what your privacy rights are to protect your personal information when providing it to a company (what rights you have to privacy and confidentiality of your personal information when providing your information to a company)? "			Male Yes 71%* Female Yes 55%
4.	Q16. "Have you or your immediate family members experienced personal loss, financial loss or harm as a result of my personal information that was misused/lost/shared by a company? (Yes/No) "	Black 37%* White 21%		Male 38%* Female 28%
5.	Q17. "Do you know of someone whose personal information has been misused by another person (conducted fraudulent transactions, exposed confidential information)? "		1955–1964 34% 1965–1980 64%*	
6.	Q22. "How concerned are you about the protection of your health information?"	Black 4.29* White 3.54		
	Section C: Expectations			
1.	Q25b. "I expect companies to use my personal information in a lawful manner (e.g. never to sell my information; publish my confidential information; never use my information for fraudulent transactions). "	Coloured 4.36 White 4.86*		Male 4.51 Female 4.76*
2.	Q25c. "I expect privacy when a company has to process my personal information for services or products (e.g. never share my information with unauthorised personnel or use my information for other purposes. "			Male 4.53 Female 4.73*
3.	Q25d. "I expect companies not to collect excessive or unnecessary information from me (e.g. my children's information, my salary, my health information, my race or religion) than what is needed for them to offer me a service or product. "	Black 4.12 Coloured 3.89 White 4.72*		Male 4.03 Female 4.45*
4.	Q25e. "I expect companies to only collect my personal information when I have given my consent; or if it is necessary for a legitimate business reason. "	Black 4.49 White 4.79*		Male 4.47 Female 4.65*
5.	Q25f. "I expect companies to only collect my personal information from myself and not from other sources (e.g. from other companies, people I know). "	Black 4.40 White 4.74*		Male 4.37 Female 4.60*
6.	Q25g. "I expect companies to explicitly define the purpose for which they want to use my information. "	Coloured 4.41 White 4.81*		Male 4.49 Female 4.71*
7.	Q25h. "I expect companies to only use my personal information for purposes I agreed to and never for other purposes (e.g. telemarketing, targeted advertising) than those agreed by me. "			Male 4.52 Female 4.69*
8.	Q25i. "I expect companies to only keep my personal information for as long as required for business purposes or regulatory requirements. "	Black 4.31 Indian 4.10 White 4.73*		Male 4.23 Female 4.55*
9.	Q25j. "I expect companies to obtain my consent if they want to use my personal information for purposes not agreed to with them. "	Black 4.47 Coloured 4.41 White 4.86 *		Male 4.40 Female 4.70*
10.	Q25k. "I expect companies to inform me of the conditions (e.g. purposes, consequences, recipients of my information, my rights and the way in which they protect confidentiality) for processing my personal information. "			Male 4.44 Female 4.69*
11.	Q25l. "I expect companies to keep my personal information updated. "	Indian 3.20* Black 3.93 Coloured 4.02 White 4.03		
12.	Q25n. "I expect companies to have all the necessary technology and processes in place to protect my personal information. "			Male 4.61 Female 4.77*
13.	Q25o. "I expect companies to ensure that their third parties (processing my personal information) have all the necessary technology and processes in place to protect my personal information. "	Black 4.41 White 4.82*		Male 4.40 Female 4.65*
14.	Q25p. "I expect companies to inform me if records of my personal data were lost, damaged or exposed publicly. "			Male 4.61 Female 4.78*

	Questions section	Race groups mean or %	Age groups mean or %	Gender groups mean of %
15.	Q25q. "I expect companies to tell me what records of personal information they have about me when I enquire about it. "	Black 4.45 Coloured 4.39 White 4.81*		Male 4.45 Female 4.64*
16.	Q25r. "I expect companies to correct or delete my personal information at my request. "	Black 4.48 Coloured 4.32 White 4.79*		
17.	Q25s. "I expect companies not to collect sensitive personal information about me (e.g. information on my children, religious beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal record or biometric information). "	Black 4.19 White 4.58*		Male 4.13 Female 4.40*
18.	Q25t. "I expect companies to honour my choice if I decide not to receive direct marketing. "	Black 4.51 Coloured 4.34 White 4.82 *		Male 4.43 Female 4.71*
19.	Q25u. "I expect companies to give me a choice if I want to receive direct marketing from them. "	Black 4.46 Coloured 4.27 White 4.76*		Male 4.38 Female 4.67*
20.	Q25v. "I expect companies to protect my information when they have to send it to other countries. "			Male 4.50 Female 4.77*
	Section D:Confidence			
1.	Q26a. "I feel confident that companies are notifying me before collecting my personal information. "	Black 3.24 Coloured 3.39 Indian 3.20 White 2.10*	1955–1964 2.24 1965–1980 2.67 1981–2000 3.30 *	Male 3.41* Female 2.63
2.	Q26b. "I feel confident that companies are using my personal information in lawful ways (e.g. never sell my information, publish my confidential information, or use my information for fraudulent transactions). "	Black 3.15 Coloured 3.30 White 2.18*	1955–1964 2.24 1965–1980 2.68 1981–2000 3.19*	Male 3.23* Female 2.69
3.	Q26c. "I feel confident that companies respect my right to privacy when collecting my personal information for services or products (e.g. never to share my information with unauthorised personnel or use my information for other purposes). "	Black 3.22 Coloured 3.45 White 2.12*	1955–1964 2.34 1981–2000 3.22*	Male 3.32* Female 2.69
4.	Q26d. "I feel confident that companies are requesting only relevant and not information other than what is needed for them to offer me a service or product. (e.g. information on my children, my salary, my health, my race or religion). "	Black 3.29 Coloured 3.20 White 2.41*	1955–1964 2.34 1981–2000 3.21*	Male 3.33* Female 2.80
5.	Q26e. "I feel confident that companies are collecting my personal information only with my consent, or for a legitimate business reason (e.g. not collecting my information without my consent while I browse the internet, or buying my information from other companies). "	Black 3.28 Coloured 3.41 White 2.27*	1955–1964 2.31 1981–2000 3.29*	Male 3.41* Female 2.71
6.	Q26f. "I feel confident that companies are collecting my personal information from legitimate sources. "	Black 3.13 Coloured 3.09 White 2.33*	1946–1954 2.64 1955–1964 2.10 1981–2000 3.17*	Male 3.25* Female 2.66
7.	Q26g. "I feel confident that companies are explicitly defining the purpose they want to use my information. "	Black 3.23 Coloured 3.23 White 2.17*	1955–1964 2.07 1965–1980 2.71 1981–2000 3.26*	Male 3.24* Female 2.76
8.	Q26h. I believe that companies are only using my personal information for purposes I agreed to and never for other purposes (e.g. telemarketing, targeted advertising. "	Black 3.14 Coloured 3.23 White 2.03*	1965–1980 2.53 1981–2000 3.15*	Male 3.24* Female 2.56
9.	Q26j. "I feel confident that companies are obtaining my consent to use my personal information for purposes other than those agreed to with me. "	Black 2.98 Coloured 3.09 Indian 3.20 White 2.24*	1965-1980 2.47 1981-2000 3.05*	Male 3.13* Female 2.56
10.	Q26k. "I feel confident that companies adequately inform me of the conditions (e.g. purposes, consequences, recipients of my information, my rights and the way in which they protect confidentiality) for processing my personal information. "	Black 3.08 Coloured 3.23 Indian 3.15 White 2.18*	1981–2000 3.15* 1965–1980 2.59 1955–1964 2.21	Male 3.20* Female 2.63
11.	Q26l. "I feel confident that companies keep my personal information up to date"	Black 3.16 Coloured 3.18 White 2.32*	1981–2000 3.19* 1965–1980 2.66 1955–1964 2.28	Male 3.30* Female 2.64
12.	Q26m. "I feel confident that companies are protecting my personal information (e.g. keep my data confidential and protect it from being accessed by unauthorised parties). "	Black 3.22 Coloured 3.39 White 2.15*	1981–2000 3.29* 1965–1980 2.57 1955–1964 2.24	Male 3.39* Female 2.60
13.	Q26n. "I feel confident that companies have all the necessary technology and processes in place to protect my personal information."	Black 3.25 Coloured 3.48 White 2.42*	1981–2000 3.32* 1965–1980 2.77 1955–1964 2.48	Male 3.44* Female 2.74

* Significantly at 0.5; Questionnaire items from (Da Veiga 2018a)