Published version can be found here:
Da Veiga, A. (2020). Concern for Information Privacy in South Africa: An Empirical Study Using the OIPCI. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Botha, R. (eds) Information and Cyber Security. ISSA 2020. Communications in Computer and Information Science, vol 1339. Springer, Cham
https://doi.org/10.1007/978-3-030-66039-0_5

Pre-print version included below

Concern for information privacy in South Africa: An empirical study using the OIPCI

Adéle da Veiga

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

Abstract. The information privacy concern of consumers concerning the processing of their personal information by online organizations (websites) is investigated in this study by means of a quantitative approach. An overview of existing concerns about information privacy instruments are presented based on a literature review. The Online Information Privacy Concern Instrument (OIPCI) is used to study consumers' expectations and experience regarding information privacy principles in order to identify their concerns about information privacy. The study was conducted in South Africa with a demographical representative sample of 1000 participants. Gaps were identified where consumers experienced that online organizations were not meeting their privacy expectations. This indicated that the regulatory requirements (in this case, the Protection of Personal Information Act (POPI) are perceived as not being met. The results indicate that while consumers in South Africa have a high expectation for privacy, it is not met in practice. Corrective action and interventions are required from a government and online organization perspective.

Keywords: Information privacy concern, Confidence, Expectations, CFIP, OIPCI, POPI

1 Introduction

Consumers are concerned about the use and protection of their personal information by organizations [1–3], specifically their financial, security and identity information [4]. In recent years, large data breaches have occurred. For example, 540 million Facebook user records were exposed in 2019; First American Financial Corporation had 885 million records exposed, including social security numbers and banking transactions; and in 2019, Microsoft leaked emails and the private contact information of 49 million Instagram users were exposed [5]. These data breaches happen due to various reasons, including internal threats, cyber criminals and exploited applications. While consumers are concerned about the security of their personal information provided to organizations, they are also increasingly concerned about the use of their information by organizations for activities such as advertising, marketing, profiling, location tracking and behavioral tracking [6].

Various researchers have studied consumers' concern for information privacy using different instruments in different contexts [7–12]. Few studies have been conducted in South Africa to understand the privacy expectations and experience of consumers in

line with regulatory requirements. While South Africa has a privacy law, the Protection of Personal Information Act (POPI) [13], it has not yet become effective, although organizations are in the process of implementing compliance requirements [14]. Multinational organizations in South Africa have to comply with the privacy laws of other jurisdictions and therefore implement data protection requirements. At the same time, South African consumers have certain expectations of privacy and concerns about the protection of personal information.

This study aims to identify the concern for information privacy of South Africans consumers in an online context. The instrument used, the Online Information Privacy Concern Instrument (OIPCI) [15], focuses on information privacy in the context of the privacy expectations and experience of consumers about specific internationally accepted privacy principles to determine the concern for information privacy. This instrument extends the context of the initial concern for information privacy instruments to include not only the concern, but also the expectations, experience and legal requirements for privacy. This paper is structured as follows: Section 2 gives an overview of the concern for information privacy followed by section 3 which gives an overview of information privacy concern instruments. The research methodology is discussed in section 4 and the results of the survey and statistical validation of the questionnaire in section 5. This is followed by the conclusion in section 6.

2 Concerns about information privacy

The scope of this paper relates to the personal identifiable information of individuals, referred to as information privacy [16]. Personal information relates to the information of an identifiable, living, natural person; juristic persons are included in the laws of some jurisdictions. Examples of personal information are a person's name and surname, gender, sex, age, religion, disability, health information, identifying numbers and symbols, email addresses, blood type, biometric information, opinions, views or preferences [13]. Personal identifiable information is increasingly processed through digital means. While the processing of such information is necessary to conclude business transactions and deliver services, it raises concern among consumers – which is referred to as the "concern for information privacy (CFIP)" or the "information privacy concern (IPC)".

Concern for information privacy is understood as individuals' concern about information privacy practices [17]. With regard to the privacy concern, Gavison [18:424] states, "I argue only that privacy refers to a unique concern that should be given weight in balancing values." She refers to various concerns about information privacy, such as the way information is acquired and the relationships in which confidentiality and specifically secrecy, anonymity and solitude are referred to as "privacy" in legal terms. She categorizes concern for information privacy in two distinct areas: (i) privacy concern because an individual has insufficient privacy and (ii) unequal distribution of privacy in a societal context, which could lead to "manipulation, deception, and threats to

autonomy and democracy" [18:444]. She argues that the law cannot in all circumstances compensate for privacy losses and that the outcome of court decisions might not "reflect fully or adequately the perceived need for privacy in our lives".

As individuals, we have our own concern for information privacy, which might be addressed by the law partially or not at all. By using only the law as a measure to implement privacy would mean that individual expectations for privacy is disregarded. It might well be that in some cases the law exceeds privacy expectations and in other cases it does not adequately address it, which could result in concern for information privacy for the individual. Furthermore, individuals could also be concerned about privacy where they experience that organizations do not honor the privacy requirements of the law or perhaps not their inherent expectations of privacy. There are thus two sides which must be considered when attempting to understand concern for information privacy: the one is the individual's expectation for privacy in various matters such as confidentiality, minimality, sharing of data, collection and use of data; the other is that one has to consider whether these expectations are met in reality, since if it is not, it will increase the individual's concern for privacy. Furthermore, if the privacy expectations of individuals are in line with the regulatory requirements for privacy, these must be met in practice – else the data processor is not only in contravention of the law, but also not meeting the individual's privacy expectations. This could increase the concern for information privacy and affect the trust of individuals in data processors processing their personal information [19].

The RSA survey [4] found that the concern for information privacy varied based on demographical factors and nationality, where consumers from different countries had different concerns. This study specifically focuses on understanding the information privacy concern of consumers in South Africa. The next section gives an overview of the various instruments available to measure the concern for information privacy and concludes with the instrument selected for this study.

3 Overview of CFIP instruments

A literature search using Harzing's Publish or Perish software program was conducted to identify the top 10 most cited papers focusing on concern for information privacy. A limitation of this approach is that new research is not included. Therefore, a further search was conducted in Scopus with the date period from 2015 to 2020 to identify the most recent concern for information privacy studies. Twenty-two papers were retrieved using the keywords "information privacy concern", of which 11 were applicable after duplicates were removed. An overview of the prominent concern for information privacy studies from these searches are presented in Table 1. It includes the instruments developed by Westin as well as Smith, Milberg and Burke, who developed some of the

first privacy indexes, which were adapted for various other studies identified in the search.

Table 1. Overview of prominent concern for information privacy studies using instruments.

Instrument	Date	Description
General Privacy Concern Index of Westin	1990	Four questions were used to divide consumers into three categories: high (fundamentalists), moderate (pragmatic) and low privacy concern (unconcerned) [20].
Consumer Privacy Concern Index of Westin	1991	Westin added two more business focus questions for the use of personal information to divide consumers into the three categories [20].
Medical Privacy Concern Index of Westin	1993	Westin added two medical concern questions to the Medical Sensitivity Index. Consumers were grouped in a high, medium or low privacy concern group [20].
Computer Fear Index of Westin	1993	Westin used three computer fear questions to create the index whereby the consumers were divided in three groups, namely high, medium and low computer privacy fear [20].
Distrust Index of Westin	1994	This index used four questions focusing on technology, government and business trust to identify a correlation between distrust and privacy issues. [20].
Privacy Concern Index of Westin	1996	The index used six questions to divide consumers in the privacy fundamentalists, privacy pragmatics and privacy unconcerned groups [20].
Concern for Information Privacy (CFIP)	1996	Develop the CFIP comprising four dimensions of privacy concerns, namely: collection, errors, unauthorized secondary use and improper access comprising 15 questions [1].
Privacy Segmentation Index Core Privacy Orientation Index	1995 - 1999	The privacy segmentation and core privacy orientation survey incorporated three questions focusing on a business context as well as whether existing laws and organizational practice provide privacy protection [20].
Concern for Information Privacy (CFIP)	2002	Stewart and Segars [7] used the CFIP of Smith et al. [17] containing 15 items in four dimensions, namely: collection, unauthorized secondary use, improper access and errors, adding computer anxiety and behavioral intention.
Internet Users' Information Privacy Concern (IUIPC)	2004	Malhotra, Kim and Agarwal used the CFIP of Smith et al. [17] and added the concepts of trust, behavioral intention and risk beliefs to measure the privacy concern of internet users [21].
Personal Internet Interest	2006	The authors used a personal internet interest variable with three questions focusing on privacy concern in the context of obtaining a service of information from the internet [22].
Information Privacy Concern about Peer Disclosure (IPCPD)	2015	Using the context of CFIP in an experiment with scenarios to identify privacy concern in social networking [23].

Instrument	Date	Description
Social Media Users' Concern for Information Privacy	2015	The constructs of Stewart and Segars [7] and Malhotra et al. [24] were used to develop and validate social media users' concern for information privacy (CFSMIP) [25].
Information Privacy Concern towards Hospital Websites	2015	Three items from Bansal et al. (2010) [26] with items from Wu et al. [27] focusing on online privacy policy, reputation, information privacy concern, and behavioral intention [28].
CFIP, Willingness to Provide Personal Information (WPI)	2016	Adapting statements from Okazaki, Li and Hirose (2009) [29] and Malhotra et al. [24]. The constructs included CFIP, WPI, confidence in privacy protection (CPP), and perceived risk [29] with a total of 24 statements [30].
Internet Users' Information Privacy Concerns (IUIPC) and Personality Traits	2018	Researchers used the internet users' information privacy concerns (IUIPC) scale [24] together with scenarios to establish the relationship between IPC, recommendation accuracy and personality traits [10].
Information Privacy Concern during Social Website Interactions	2018	Twenty-two questions measuring the concern when disclosing personal information on websites. The questions were adapted from the work of Li [31] and Pavlou [32], among others [33].
Users' Information Privacy Concerns (UIPC)	2018	Users' information privacy concerns (UIPC) on privacy protection behavior (PPB) in social networks. The questionnaire included adapted statements from Dinev and Hart [34] [35].
Online Shopping Information Privacy Concern (IPC)	2019	Looking at information privacy concerns of online shopping consumers. One of the constructs was based on the information privacy concern construct of Pavlou [32] [9].
Demographic Characteristics and Information Privacy Concern (IPC)	2019	Researchers used the 16 items of Buchanan, Paine and Reips [36] to design a six-item survey focusing on the concern of sharing personal information over the internet in order to identify demographic differences [37].
CIFP in Health Information Exchange	2019	Using the CIFP of Stewart and Segars [7] and adapting it for health information exchange with opt-in intentions [38].
Mobile Users' Information Privacy Concerns (MUIPC)	2020	Mobile users' information privacy concerns (MUIPC) in the context of the internet of things, adapting survey items from Xu et al. [40], Solove [41] and Smit et al. [17] [42].
Mobile Users' Information Privacy Concerns (MUIPC)	2020	Using the antecedent-privacy-control-outcome model, adding computer anxiety, perceived control and app permission concerns for mobile users and adapting the work of Smith et al. [1], Malthota et al. [21], Stewart and Segars [7], Xu et al. [40] and Dinev, et al. [43] [44].

A number of the concern for information privacy surveys were conducted building on the work of Westin, mostly measuring the privacy concern of the individual perspective (e.g. CFIPT and IUIPC). Smith et al. [16] identified that concern for information privacy studies were conducted either from the individual's concern perspective

(e.g. their personality) or from a privacy experience perspective (what the experience in practice was, such as their information being shared or exposed in the past). It was found that the privacy experience of consumers influences their privacy concern together with other constructs such as gender, awareness of privacy policies, cultural differences [16] and age [37]. While the instruments aim to specifically measure concern for information privacy, they include statements that cover both users' concern and experience when their personal information is processed.

The "General Privacy Concern Index" of Westin is used to divide consumers into categories of concern; however, only one question concentrates on the concept of concern (namely, whether they are concerned about threats to their personal privacy) [21]. The other three questions focus on whether consumers agree on aspects relating to what business or government does in relation to privacy concepts based on their experience. The Consumer Privacy Concern Index included a question about the protection of privacy rights and if consumers agreed or disagreed with the statement, not necessarily measuring a concern. The questions used by Smith et al. [17:170] included concern questions such as "I'm concerned that companies are collecting too much personal information about me"; whereas other questions are phrased from an expectations perspective, such as "Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information" [17:170]. Malhotra et al. [21] included questions from various authors with a concern, expectation or confidence perspective. A consumer concern question used is, for example, "I am concerned about threats to my personal privacy today" [21:352]. They also included questions from an expectations perspective, such as "Online companies should never sell the personal information in their computer datasets to other companies" [21:352]. Some questions are phrased from a confidence perspective, thus establishing if companies indeed exhibit certain values or behavior, for example: "Online companies are always honest with customers when it comes to using (the information) that I would provide" [21:352].

The CIFP or IUIPC were used in various studies to design new instruments to measure concern for information privacy in the context of each study, such as social networking [25, 35], online shopping [9] or mobile phones [44]. Others designed new instruments focusing on social networking and trust [45,] and consumers' concerns in providing personal information for marketing purposes [46]. Researchers like Miyazaki and Fernandez [47] studied concern for information privacy from a risk perspective in terms of online shopping, finding that the more internet experience users have, the less privacy risk they perceive in terms of online shopping and security. Of importance to note is that Norberg et al. [48] studied the concept of the "privacy paradox" (a discrepancy between privacy attitude and privacy behavior as well as between privacy behavior and privacy intention). In their study, they found that the privacy paradox exists, whereby individuals disclose significantly more information than what they intent to disclose and behavior intent is not a predictor of actual behavior in a privacy context. Kokolakis [49] analyzed studies on the privacy paradox, supporting and challenging it.

Each of these studies used a survey or experiment method to identify the dichotomy between privacy concern and behavior.

The studies discussed used various instruments for the concern of information privacy. These instruments include items that concentrate on the consumer's information privacy concern and/or expectations and/or experience in practice within a certain context. However, there is no balance of these items in that for each information privacy concern item, there is a corresponding expectation or experience statement to measure both perspectives. The instruments are also not aligned with best practice data privacy principles, such as the Fair Information Practice Principles (FIPPS) to measure information privacy concern and expectations in line with legal requirements with which organizations must comply.

The Online Information Privacy Culture Index (OIPCI) [50], used in this study, and the Information Privacy Culture Index (IPCI) [51] consider both perspectives and expand on the concept of information privacy concern to also incorporate the privacy expectations and experience of data subjects as well as the concept of compliance with legal requirements. These questionnaires were developed in previous studies and measure for each FIPPs the expectation of the consumer together with their experience in practice as to whether it is met (thus their confidence that organizations are meeting that principle in practice). A number of specific concerns for information privacy statements are also included, making it comprehensive in terms of understanding the gap between information privacy expectations and experience, which outlines the concern for information privacy. The questions in the OIPCI and IPCI (as with the CIFP, UIPC, IUIPC and MUIPC) focus on concern for information privacy with statements from an expectation and experience perspective. The IPCI and OIPCI also measure the information privacy concern and gives an indication of the culture of privacy. In the context of this study, the instrument [50] is referred to as the Online Information Privacy Concern Instrument (OIPCI).

4 Methodology

This research employs a quantitative research design using a survey method. Surveys are useful to measure concern for information privacy; however, as a limitation it was found to be unreliable in terms of self-reporting of privacy behavior [49]. Privacy behavior is not measured in this study, only perceptions and attitudes.

4.1 Measuring instrument

The OIPCI comprises 11 privacy principles, namely: accountability (AC), openness (OP), processing (use limitation) (PR), collection limitation (CL), purpose specification (PS), data subject participation (access) (DS), security safeguards (SS) and information

quality (IQ), unsolicited marketing (UM), cross-border transfers (CB) and sensitive (special) personal information (SP). These were mapped to the POPI [15]. For each privacy principle, a question pair is used to measure the privacy expectation and experience (or confidence) of that principle being honored or implemented in practice by organizations. Information privacy concern can be identified where the expectation and experience about a specific principle do not match, thus where a gap is identified. The privacy principles map to the regulatory requirements of the POPI; therefore, if consumers experience that any of the requirements are not met in practice, it will also indicate a perception of non-compliance for organizations.

4.2 Sample

A thousand responses were collected in 2018 in South Africa, according to the demographic profile of the country. The sample included 52% males and 48% females. The sample mostly included Millennials/Generation Y (63%), followed by Generation X (16%) and Generation Z (12%). The majority of the sample were employed (79%), with some participants unemployed (10%), students (8%) or retired (2.9%). Thirty percent of the participants had a school certificate and 3% had not completed school, 24% a diploma, 23% a university degree or diploma and 20% a postgraduate qualification. As stated, the participants represented the demographic profile of the country: 64% black, 20% white, 11% colored and 5% Indian. As such, the majority of the home languages spoken by the respondents were African languages. The questionnaire was sent electronically by a market research company [52]. Ethical clearance was obtained from the university, ensuring that the survey met the ethical requirements such as being voluntary, anonymous and that consent was obtained to use the survey data for research publications.

5 Results

The respondents indicated that they obtained privacy information from the internet/websites (71%), banks (40%) and organizations to whom they provided their information (29%). The preferred methods to obtain privacy information, in order of preference, were: internet/websites, bank, government, organization to whom they provided their personal information and organizations they worked for. Sixty-three percent said that they knew of someone whose personal information had been misused (e.g. confidential information exposed), indicating that South Africans are experiencing data breaches. Ninety percent said that they were indeed concerned when providing their personal information on websites. They were mostly concerned about their identification (91%), financial (88%) and health (66%) information. Respondents were specifically concerned when websites built an online profile of them without consent (90%) or tracked their movements on the internet (82.8%).

The overall results showed that there was a gap in terms of the privacy expectations (4.43 mean) of respondents compared to the confidence (2.93 for mean) they had in whether organizations were meeting their expectations. Table 2 shows the means for each of the expectation and experience statements. All the expectation statements were significantly more positive compared with the corresponding experience statement based on the Sig. (two-tailed) test, which means that there was a significantly higher expectation for privacy than what consumers experienced in practice, thus their privacy expectations were not met. The three question pairs with the biggest discrepancy between expectation and experience were for the expectation that online companies would inform consumers if their personal data was lost, to only use their personal data for the agreed purposes and to protect their data when sending it to other countries. There was thus a significant gap in terms of the privacy expectations of consumers and what they experienced in practice, thus highlighting the concern for information privacy. If consumers feel that organizations are not meeting their privacy expectations, it also indicates that organizations might not be meeting regulatory requirements as the expectations statements are in line with the requirements of the POPI.

Table 2. Means for privacy expectation and experience statements. (Items from [50])

Privacy expectation	Mean	Privacy experience (confidence)	Mean	Gap
"I expect online companies (websites) to inform me if records of my personal data were lost damaged or exposed publically."	4.59	"I feel confident that online companies (websites) inform me if records of my personal data were lost damaged or exposed publically."	2.76	1.83
"I expect online companies (websites) to only use my personal information for purposes I agreed to and never for other purposes than those agreed by me."	4.64	"I believe that online companies (websites) are only using my personal information for purposes I agreed to and never for other purposes."	2.84	1.8
"I expect online companies (websites) to protect my information when they have to send it to other countries."	4.61	"I feel confident that online companies (websites) protect my information if they have to send it to other countries."	2.82	1.79
"I expect online companies (websites) to use my personal information in a lawful manner."	4.62	"I feel confident that online companies (websites) are using my personal information in lawful ways."	2.84	1.78
"I expect privacy when an online company (website) has to process my personal information for services or products."	4.59	"I feel confident that online companies (websites) respect my right to privacy when collecting my personal information for services or products."	2.87	1.72
"I expect online companies (websites) to obtain my consent if they want to use my personal information for purposes not agreed to with them."	4.59	"I feel confident that online companies (websites) are obtaining my consent to use my personal information for purposes other than those agreed to with me."	2.88	1.71
"I expect online companies (websites) to protect my personal information."	4.56	"I feel confident that online companies (websites) are protecting my personal information."	2.86	1.70
"I expect online companies (websites) to explicitly define the purpose for which they want to use my information."	4.59	"I feel confident that online companies (websites) are explicitly defining the purpose they want to use my information for."	2.92	1.67
"I expect online companies (websites) to only collect my personal information when I have given my consent; or if it is	4.58	"I feel confident that online companies (websites) are collecting my personal information only with my	2.92	1.66

Privacy expectation	Mean	Privacy experience (confidence)	Mean	Gap
necessary for a legitimate business reason."		consent or for a legitimate business reason."		
"I expect online companies (websites) to inform me of the conditions for processing my personal information."	4.56	"I feel confident that online companies (websites) adequately inform me of the conditions."	2.91	1.65
"I expect online companies (websites) to honor my choice if I decide not to receive direct marketing."	4.58	"I feel confident that online companies (websites) honor my choice if I do not want to receive direct marketing."	2.94	1.64
"I expect online companies (websites) to ensure that their third parties (processing my personal information) have all the necessary technology and processes in place to protect my personal information."	4.51	"I feel confident that online companies (websites) ensure that their third parties have all the necessary technology and processes in place to protect my personal information."	2.90	1.61
"I expect online companies (websites) to have all the necessary technology and processes in place to protect my personal information."	4.60	"I feel confident that online companies (websites) have all the necessary technology and processes in place to protect my personal information."	3.00	1.60
"I expect online companies (websites) to only collect my personal information from myself and not from other sources."	4.49	"I feel confident that online companies (websites) are collecting my personal information from legitimate sources."	2.91	1.58
"I expect online companies (websites) to correct or delete my personal information at my request."	4.56	"I feel confident that online companies (websites) will correct or delete my personal information at my request."	2.98	1.58
"I expect online companies (websites) to notify me before they start collecting my personal information."	4.48	"I feel confident that online companies (websites) are notifying me before collecting my personal information."	2.92	1.56
"I expect online companies (websites) to tell me what records of personal information they have about me when I enquire about it."	4.41	"I feel confident that online companies (websites) can tell me what records or personal information they have about me."	2.99	1.42
"I expect online companies (websites) not to collect sensitive personal information about me."	4.31	"I feel confident that online companies (websites) only collect sensitive personal information about me with my explicit consent.	2.93	1.38
"I expect online companies (websites) to give me a choice if I want to receive direct marketing from them."	4.51	Online companies (websites) always give me a choice to indicate if I want to receive direct marketing from them."	3.14	1.37
"I expect online companies (websites) not to collect excessive or unnecessary information from me than what is needed for them to offer me a service or product."	4.35	"I feel confident that online companies (websites) are requesting only relevant and not information other than what is needed for them to offer me a service or product."	3.04	1.31
"I expect online companies (websites) to only keep my personal information for as long as required for business purposes or regulatory requirements."	4.26	"I believe that online companies (websites) are keeping my personal information indefinitely."	3.26	1.00
"I expect online companies (websites) to keep my personal information updated."	3.67	"I feel confident that online companies (websites) keep my personal information up to date."	2.95	0.72

Strategies can be implemented for meeting consumer expectations in order to address information privacy concern. Online organizations should understand their

consumer base and if there are unique privacy concerns or expectations that they need to take cognizance of when designing websites, selling services or products online, conducting marketing and processing personal information. These could comprise an intervention for each of the IOPC item pairs with a gap to ensure that regulatory, process and technology controls are indeed in place. Furthermore, the privacy terms and conditions should be included clearly on online websites with additional communication and awareness. It is recommended that online organizations conduct privacy compliance assessments to identify with which conditions of privacy legislation they do not comply in order to alleviate information privacy concern from that perspective.

5.1 Questionnaire validation

Exploratory factor analysis was applied to the data using Principal Component Analysis as the extraction method. This was conducted separately for the expectations and experience factors. Varimax with Kaiser normalization was used as the rotation method, with three rotations. Two factors were identified for expectations and two for experience. Bartlett's test for sphericity and the Kaiser-Meyer Olkin (KMO) measure of sampling adequacy was found to be significant at $p < 0.00$, indicating validity of the sample where $p < 0.05$ [53]. Table 3 outlines the four factors with the corresponding items. Only item 23 was excluded, as it was an additional item which was added and can rather be interpreted as a yes/no question.

Table 3. Factors and Cronbach alpha.

Factor name	Items	Cronbach alpha	Total items
Factor A: Expectations	1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 22	0.917	11
Factor B: Expectations	9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21	0.871	11
Factor C: Confidence	24, 25, 26, 27, 28, 29 ,30 31	0.958	8
Factor D: Confidence	32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47	0.966	16
Excluded in analysis	23	N/A	1

The KMO values were more than the minimum required 0.60 [54], namely 0.971 for expectations and 0.984 for confidence. Fifty-three percent of the variance was accounted for by the two expectations factors and 70% for the two experience factors, all with an Eigenvalue above one [55]. All the item values were above 0.4, which was the minimum for inclusion. The identified factors in this study closely resembles the factors of the first validation of the OIPCIQ study with 356 participants, where four factors were also identified [51].

A limitation of the this study is that a comparative analysis could not be conducted for the data collected in this study compared to the data collected in the first study [50]. The demographic profile of the first study was not representative of the South African

population whereas this study was. The samples could therefore not be compared. Future research will aim to conduct a comparative study to monitor if there is a change in concern for information privacy over a period of time.

6 Conclusion

This paper outlines the concern for information privacy study which was conducted in South Africa. An overview of existing instruments was provided with a discussion of the OIPC instrument used in this study. The results indicated that while consumers have a high expectation for privacy, it is not met in practice by online organizations (websites). There is a large gap between what consumers expect in terms of privacy and how consumers perceive that online organizations are processing their personal information. While online organizations are not meeting consumer privacy expectations, they are also not meeting the minimum requirements of the POPI as perceived by consumers. The concern for information privacy is thus high in South Africa and corrective action is required from a government and online organization perspective. Further research should be aimed at extending the study to other jurisdictions for comparative results between countries for information privacy concern and to conduct a comparative study in South Africa to monitor the concern for information privacy over a period of time.

Acknowledgements

Women in Research Grant of UNISA.

References

1. Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. MIS Q 20:167. doi:10.2307/249477
2. Malhotra NK, Kim SS, Agarwal J, et al (2014) Internet users' information privacy concerns (IUIPC): The construct, the scale and a casual model. Inf Sys Res 15:336–355. doi:10.1287/isre.l040.0032
3. Degirmenci K (2020) Mobile users' information privacy concerns and the role of app permission requests. Int J Inf Manage 50:261–272. doi:10.1016/j.ijinfomgt.2019.05.010
4. RSA (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
5. Varonis (2020) 7 Must-know data breach statistics for 2020. https://www.varonis.com/blog/data-breach-statistics/
6. Palos-Sanchez P, Saura JR, Martin-Velicia F (2019) A study of the effects of programmatic advertising on users' concerns about privacy overtime. J Bus Res 96:61–72. doi:10.1016/j.jbusres.2018.10.0597

   Stewart KA, Segars AH (2002) Examination empirical for information privacy of

the concern instrument. Inf Syst Res 13:36–49
8. Xu Z (2019) An empirical study of patients' privacy concerns for health informatics as a service. Technol Forecast Soc Change 143:297–306. doi:10.1016/j.techfore.2019.01.018
9. Li Y, Liu H, Lee M, Huang Q (2019) Information privacy concern and deception in online retailing: The moderating effect of online–offline information integration. Internet Res 30:511–537. doi:10.1108/INTR-02-2018-0066
10. Rook L, Sabic A, Zanker M (2018) Engagement in proactive recommendations: The role of recommendation accuracy, information privacy concerns and personality traits. J Intell Inf Syst 54:79–100. doi:10.1007/s10844-018-0529-0
11. Pentina I, Zhang L, Bata H, Chen Y (2016) Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. Comput Human Behav 65:409–419. doi:10.1016/j.chb.2016.09.005
12. Da Veiga A (2015) The influence of information security policies on information security culture: Illustrated through a case study. In: Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015). Lesvos, Greece, pp 22–33
13. Parliament of the Republic of South Africa (2013) Protection of Personal Information Act (POPI) 4 of 2013. Cape Town
14. Botha J, Eloff M, Swart I (2015) The effects of the POPI on small and medium enterprises in South Africa. In: Proceedings of the International Information Security South Africa (ISSA) Conference. Johannesburg, South Africa, pp 1–8
15. Da Veiga A (2018) An online information privacy culture. In: Proceedings of the Conference on Information Communications Technology and Society (ICTAS). Durban, South Africa, pp 1–6
16. Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. MIS Q 35:989–1015
17. Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. MIS Q Manag Inf Syst 20:167–195. doi:10.2307/249477
18. Gavison R (1980) Privacy and the limits of law. Yale Law J 89:421. doi:10.2307/795891
19. Chellappa RK, Sin RG (2005) Personalization versus privacy: An empirical examination of the online consumer's dilemma. Inf Technol Manag 6:181–202. doi:10.3138/cras.42.1.7
20. Kumaraguru P, Cranor LF (2005) Privacy indexes: A survey of Westin's studies, CMU-ISRI-5-138, Institute for Software Research International School of Computer Science, Carnegie Mellon University, pp 1–22
21. Malhotra NK, Kim SS, Agarwal J, et al (2014) Internet users' information privacy concerns (IUIPC): The construct, the scale and a casual model. Inf Sys Res 15:336–355. doi:10.1287/isre.l040.0032
22. Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. Inf Syst Res 17:61–80
23. Chen J, Ping JW, Xu YC, Tan BCY (2015) Information privacy concern about peer disclosure in online social networks. IEEE Trans Eng Manag 62:311–324.

doi:10.1109/TEM.2015.2432117
24. Malhotra NK, Kim SS, Agarwal J, et al (2014) Internet users' information privacy concerns (IUIPC): The construct, the scale and a casual model. Inf Sys Res 15:336–355. doi:10.1287/isre.l040.0032
25. 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. Comput Human Behav 49:324–332. doi:10.1016/j.chb.2015.02.062
26. Bansal G, Zahedi FM, Gefen D (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst 49:138–150
27. Wu KW, Huang SY, Yen DC, Popova I (2012) The effect of online privacy policy on consumer privacy concern and trust. Comput Human Behav 28:889–897
28. Kuo KM, Talley PC, Ma CC (2015) A structural model of information privacy concerns toward hospital websites. Program 49:305–324. doi:10.1108/PROG-02-2014-0014
29. Okazaki S, Li H, Hirose M (2009) Consumer privacy concerns and preference for degree of regulatory control. J Advert 38:63–77
30. Anic ID, Budak J, Rajh E (2016) New information economy in post-transition countries: An economic approach to privacy concern. Transform Bus Econ 15:165–178
31. Li Y (2014) The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decis Support Syst 57:343–354
32. Pavlou PA, Liang H, Xue Y (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal–agent perspective. MIS Q 31:105–136
33. Kaushik K, Kumar JN, Kumar SA (2018) Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. Electron Commer Res Appl 32:57–68. doi:10.1016/j.elerap.2018.11.003
34. Dinev T, Hart P (2004) Internet privacy concerns and their antecedents: Measurement validity and a regression model. Behav Inf Technol 23:413–422. doi:10.1080/01449290410001715723
35. Adhikari K, Panda RK (2018) Users' information privacy concerns and privacy protection behaviors in social networks. J Glob Mark 31:96–110. doi:10.1080/08911762.2017.1412552
36. Buchanan T, Paine C, Joinson AN, Reips UD (2007) Development of measures of online privacy concern and protection for use on the internet. J Am Soc Inf Sci Technol. doi:10.1002/asi.20459
37. Lee H, Wong SF, Oh J, Chang Y (2019) Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. Gov Inf Q 36:294–303. doi:10.1016/j.giq.2019.01.002
38. Esmaeilzadeh P (2019) The effects of public concern for information privacy on the adoption of health information exchanges (HIEs) by healthcare entities. Health Commun 34:1202–1211. doi:10.1080/10410236.2018.1471336
39. Xu H, Teo H, Tan BC, Argarwal R (2012) Privacy concerns: A study of location-based services effects of individual self-protection, industry self-regulation, and

government regulation on privacy concerns: A study of location-based services. Inf Syst Res 23:1342–1363. doi://doi.org/10.1287/isre.1120.0416
40. Xu H, Teo H, Tan BCY, Agarwal R (2012) Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. Inf Syst Res 23:1342–1363. doi://doi.org/10.1287/isre.1120.0416
41. Solove DJ (2006) A taxonomy of privacy. Univ PA Law Rev 154:477–564. doi:10.2307/40041279
42. Foltz CB, Foltz L (2020) Mobile users' information privacy concerns instrument and IoT. Inf Comput Secur. Ahead of print. doi:10.1108/ICS-07-2019-0090
43. Dinev T, Xu H, Smith JH, Hart P (2013) Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. Eur J Inf Syst 22:295–316. doi:10.1057/ejis.2012.23
44. Degirmenci K (2020) Mobile users' information privacy concerns and the role of app permission requests. Int J Inf Manage 50:261–272. doi:10.1016/j.ijinfomgt.2019.05.010
45. Dwyer C, Hiltz S, Passerini K (2007) Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In: Proceedings of the Thirteenth Americas Conference on Information Systems. Colorado, USA, pp 1–13
46. Phelps J, Nowak G, Ferrell E (2000) Privacy concerns and consumer willingness to provide personal information. J Public Policy Mark 19:27–41
47. Miyazaki AD, Fernandez A (2001) Consumer perceptions of privacy and security risks for online shopping. J Consum Aff 35:27–44. doi:10.1111/j.1745-6606.2001.tb00101.x
48. Norberg PA, Horne DR, Horne DA (2007) The privacy paradox: Personal information disclosure intentions versus behaviors. J Consum Aff 41:100–126. doi:10.1111/j.1745-6606.2006.00070.x
49. Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput Secur 64:122–134. doi:10.1016/j.cose.2015.07.002
50. Da Veiga A (2017) An information privacy culture index framework and instrument to measure privacy perceptions across nations: Results of an empirical study. In: Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA). Adelaide, Australia, pp 196–209
51. Da Veiga A (2018) An information privacy culture instrument to measure consumer privacy expectations and confidence. Inf Comput Secur 26:339–364
52. InSites Consulting South Africa. https://insites-consulting.com/
53. Bartlett JE, Kotrlik WJ, Higgins CC (2001) Organizational research: Determining appropriate sample size in survey research. Inf Tech Learn Perform J 19:43–50
54. Kaiser HF, J. Rice (1974) Little jiffy, mark IV. Educ Psychol Meas 34:111–117
55. Hair JF, Anderson RE, Babin BJ, Black W (2010) Multivariate data analysis: A global perspective, 7th ed. Pearson, Upper Saddle River, NJ