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

An information privacy culture instrument to measure consumer privacy expectations and confidence

Adéle da Veiga

College of Science, Engineering and Technology, School of Computing, University of South Africa, P.O. Box 392, UNISA 0003, South Africa
dveiga@unisa.ac.za

Abstract

Purpose – This research proposes an information privacy culture index framework (IPCIF) with a validated information privacy culture index instrument (IPCII) to measure information privacy culture across nations. The framework is based on consumers' privacy expectations, their actual experiences when organisations process their personal information, as well as their general privacy concerns.
Design/methodology/approach – A survey method was deployed to collect data in South Africa – the first participating country in the study – to start building a global information privacy culture index and to validate the questionnaire.
Findings – The information privacy culture index revealed that there seems to be a disconnect between what consumers expect in terms of privacy and the way in which organisations are honouring (or failing to honour) those expectations, which results in a breach of trust and the social contract being violated.
Practical implications – Governments, information regulators and organisations can leverage the results of the privacy culture index to implement corrective actions and controls aimed at addressing the gaps identified from a consumer and compliance perspective. The validated IPCII can be used by both academia and industry to measure the information privacy culture of an institution, organisation or country to identify what to improve in order to address consumer privacy expectations and concerns.
Originality/value – The IPCIF and validated IPCII is the first tool that combines the concepts of consumer expectations and their confidence levels in whether organisations are meeting their privacy expectations, which are in line with the Fair Information Practice Principles (FIPPs) and the privacy guidelines of the Organisation for Economic Cooperation and Development (OECD), in order to determine gaps and define improvement plans.

Keywords – culture, data privacy, data protection, information privacy, framework, index, consumer, perceptions, questionnaire, OECD, FIPPs, POPIA

Paper type – Research paper

1. Introduction

Privacy is a fundamental human right with some of the first privacy legislation dating back to the fourteenth century (Swire and Ahmad 2012). Today, privacy is regulated in over a hundred countries with most privacy laws based on international privacy principles (DLA Piper 2018; Greenleaf 2014; Bellman et al. 2004). While privacy is regulated from a common set of principles, people in different countries or from different cultures have different privacy expectations (Moore 2008; Kemp and Moore 2007). Various studies have been conducted into privacy and the concerns that consumers and nations have about the concept (Smith et al. 1995; Bellman et al. 2004; Malhotra et al. 2004; Dell EMC 2015; Symantec 2015; Deloitte & Touche 2017). Privacy expectations as well as privacy concerns vary between nations and within the demographic groups that make up a nation. At the same time, the maturity of privacy or data protection regulations vary between jurisdictions, with certain jurisdictions having a "heavy" stance towards the implementation and regulation thereof, while others are perceived as "moderate" or "low" (DLA Piper 2018).

Additional insight can be obtained by comparing the privacy expectations of consumers or nations to their actual experiences when organisations process their personal information. This would allow for the identification of gaps, which would help improve the safeguarding of personal information and build a trusting relationship. It would also be beneficial if the privacy concepts measured in this way were aligned with best practice principles of privacy, such as those proposed in the Fair Information Practice Principles (FIPPs) (FIPP 2018) and the Guidelines on the Protection of Personal Information and Trans-border Flows of Personal Data of the Organisation for Economic Cooperation and Development (OECD 2013), to allow for comparisons between countries.

This research study aims to develop a global information privacy culture index (IPCI), whereby consumers' or nations' expectations of how organisations should deal with their personal information, can be compared to their actual experiences in this respect. The paper begins by defining the concept of information privacy culture, after which the information privacy culture index framework (IPCIF) and instrument (IPCII) are discussed. This is followed by a discussion of a survey conducted in South Africa – as the first country to participate in the study – followed by the validity and reliability results of the instrument. The discussion of the results is followed by the conclusion, after which the complete IPCII questionnaire is provided.

2. Information privacy culture

The definition of information security culture has been extended to incorporate the concept of privacy, referred to as "information protection culture". This is defined as

> "a culture in which the protection of information and upholding of privacy are part of the way things are done in an organisation. It is a culture in which employees illustrate attitudes, assumptions, beliefs, values and knowledge that contribute to the protection and privacy of information when processing it at any point in time in the information life cycle, resulting in ethical and compliant behaviour" (Da Veiga and Martins 2015: 249)

This definition focuses on the organisational context, which incorporates the perspectives of employees. Similarly, the privacy culture definition of the Information Systems Audit and Control Association (ISACA) also relates to a culture in an organisational context. ISACA (2016) refers to a privacy culture as one that adopts privacy protection behaviours, such as ethical behaviour and proactive privacy commination. The privacy culture may vary in maturity across organisations. There may be no strategic focus or formal documentation, but on the other hand the privacy culture may be mature in guiding employee behaviour when they process personal information. ISACA argues that organisations should extend their privacy focus to "move beyond simply considering legal compliance requirements for privacy by implementing a culture of ethical privacy protection activities" (ISACA 2016:71).

The implication of moving towards a privacy culture entails that employees should ultimately display a pattern of behaviour of upholding the privacy of customer information at all times. The organisation may have a view of how its employees interact with consumer data, while consumers may have a different experience when the organisation processes their personal information. This view is, however, not included in the above privacy culture definitions.

When considering the consumer's view in the perception towards a privacy culture one needs to reflect on a national culture. The *Business Dictionary* (2018) defines a national culture as "[t]he set of norms, behaviors, beliefs and customs that exist within the population of a sovereign nation. International organisations develop management and other practices in accordance with the national culture they are operating in." This relates to the research by Hofstede et al. (2010), which focuses on the influence national culture has on workplace values, where the norms, behaviours, beliefs and customs of a nation affect the practices in an organisation and become part of the organisational culture.

In the context of this study, information privacy culture relates to the perceptions and beliefs a nation (hereafter "consumer") has about the processing of (their) citizens' personal information – what expectations they have and how they believe organisations are meeting those expectations given certain information privacy principles (or requirements). The study therefore encapsulates "how things should be done" and "how things are perceived to be done", in relation to privacy.

3. Data privacy perception instruments

There have been attempts to develop instruments to measure consumers' perceptions as they pertain specifically to privacy. The Concern for Information Privacy (CFIP) instrument, developed by Smith et al. (1995), incorporates one factor that focuses on information collection, unauthorised secondary use, improper access and errors. This instrument has been expanded to incorporate internet user concerns that address three dimensions, namely collection, control and awareness from a social contract perspective (Bellman et al. 2004; Malhotra 2004). A social contract is established between consumers and the organisation when the former provide their personal information to the latter, and they have the option to decide how that information is to be used (Phelps, Nowak and Ferrell 2000). A breach of this social contract occurs when the organisation, for example, shares the consumers' personal information with third parties, without being granted consent.

Consumers' expectations about the way in which organisations use and protect their personal information may differ. The Westin Privacy Segmentation Index segments consumers into three categories (Kumaraguru and Cranor 2005; Miltgen 2009):

- *Privacy fundamentalists*. Members of this group are mainly concerned about sharing and safeguarding their personal information.
- *Privacy pragmatists*. They tend to seek a balance between the advantages and disadvantages of sharing private information, before arriving at a decision.
- *Privacy unconcerned*. These people believe there is greater benefit to be derived from sharing their personal information, and they are thus least protective of their privacy (adapted from Woodruff et al. 2014).

Privacy fundamentalists may be highly concerned if an organisation were to share their personal information with third parties, whereas the privacy unconcerned group may see value in such sharing. These divergent views thus have different effects on the social contract and the trusting relationship the consumer has formed with the organisation. If the social contract is breached, it could result in non-compliance with data protection legislation.

The work of Morton and Sasse (2014) segments consumers (users) into five categories with regard to their privacy concerns and the use of technology: information controllers (seeking to control their personal information collection, use and sharing); security concerned (expecting security of personal information); benefit seekers (valuing the benefits in return for providing personal information); crowd followers (relying on advice from family or friends); and organisational assurance seekers (requiring assurance for processing of information like a privacy policy). The aforementioned research and the Westin Privacy Segmentation Index indicate that consumers have different privacy concerns and expectations from organisations that process their personal information. If they feel that the organisation does not meet their expectations, "they may respond emotionally and reject it, or distrust the motives of the providing organisation" (Morton and Sasse 2014:102).

While consumers may have diverse expectations about the use and protection of their personal information, organisations must comply with the minimum data protection regulations of those jurisdictions that apply to them. If one considers the Western Privacy Index categories, some consumers may have expectations that are in line with data protection regulatory requirements (e.g. privacy fundamentalists), while other groups (e.g. privacy unconcerned) may have lower expectations. By contrast, organisations' compliance with regulatory requirements could vary leading to a range of fines being imposed on them for non-compliance (Australian Government 2018; ICO 2017). While organisations have an obligation to their customers, they must also comply with data protection legislation when processing personal information, irrespective of the consumers' expectations. The FIPPs (FIPP 2018) and the guidelines of the OECD (2013) cover eight fundamental principles for data protection: accountability, processing or use limitation, collection limitation, purpose specification, information quality, openness, security safeguards, data subject participation and access – all of which have been incorporated into most data protection regulations (Bellman et al. 2004).

Industry-related privacy perception instruments are available, such as those developed by Dell EMC (2015), Symantec (2015) and KPMG (2016), which focus on general privacy and online consumer concerns. The Data Protection Eurobarometer (European Commission 2015; European Commission 2016)

is commissioned by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT) and is conducted across the 28 European Member states. These surveys cover aspects such as consumers' perception towards providing personal information and online profiling, concerns about privacy and levels of privacy awareness in an online context. Deloitte and Touche in Australia (2017) conducted a privacy index survey of organisational perspectives about privacy in a work context. The TRUSTe/National Cyber Security Alliance (NCSA 2016) Consumer Privacy Index focuses on consumer concerns, privacy awareness and business impact in the online context. The Dell EMC (2015) Privacy Index is a global survey aimed at measuring consumers' perceptions of the online privacy they enjoy. It includes a ranking across countries, which indicates the willingness of consumers to share private information for the sake of greater convenience. The factors measured are not inclusive of the OECD privacy principles, but survey respondents' views on privacy and awareness in an online context or in respect of organisational privacy measures that have been implemented. These instruments neither incorporate a perspective on consumer expectations, nor do they determine whether organisations are meeting those expectations in line with FIPPs. While Smith's (2014) CFIP measures consumer expectations, it does not gauge perceptions of whether organisations are meeting those expectations; it also does not incorporate all the FIPPs or data protection guidelines outlined by the OECD.

The author therefore proposes that both concepts – consumer expectations and perceptions of whether organisations are meeting those expectations – should be considered in an effort to determine the IPCI of a nation and its diverse demographic groups. Expectations and beliefs regarding compliance should be aligned with the FIPPs and OECD privacy guidelines to ensure that regulatory requirements form the cornerstone of the culture being measured, as that would aid in comparing indices across nations.

4. The information privacy culture index framework (IPCIF)

The information privacy culture index framework (IPCIF) is portrayed in figure 1 as outlined in Da Veiga (2017). The components are as follows:

- *Regulatory factor requirements*. The principles of the FIPPs and OECD privacy guidelines were summarised in eight regulatory factors, each with a number of requirements. Three more regulatory factors were added, namely unsolicited marketing, cross-border transfers and sensitive personal information (PI). These factors are in line with developments in Europe with regard to the General Data Protection Regulation (GDPR) (European Parliament and Council 2016) and other data protection legislation that covers these concepts, such as the Protection of Personal Information Act (POPIA) (Republic of South Africa 2013) of South Africa, the Data Protection Act (DPA) of the United Kingdom (Great Britain 1998) and Australia's Privacy Act (Australia Government 1988). The requirements of these regulatory factors serve as the minimum data protection requirements in the proposed framework and form the cornerstone of the framework. The regulatory requirements of a specific country can be mapped to the regulatory factor requirements in the IPCIF for comparison purposes.

- *Privacy expectations*. This block represents consumers' expectations about each of the regulatory factor requirements. The aim is to establish what consumers' expectations are for each of the requirements of the 11 regulatory factors. Although the regulatory factor requirements serve as a minimum baseline based on the OECD and FIPPS, consumers may have a lower or higher expectation for certain regulatory factor requirements. This could give an indication as to the privacy culture of a country.

- *Compliance/meeting expectations*. The compliance/meeting expectations block depicts the perceptions of consumers as to whether organisations are meeting the requirements of each of the 11 regulatory factors, thus consumers' confidence in whether organisations' behaviour is in line with the regulatory factor requirements. While the regulatory factor requirements entail the minimum requirements for data privacy, one would expect organisations in jurisdictions with enacted data privacy laws to comply with those requirements and that consumers experience it as such. Where consumers believe organisations are not meeting the regulatory factor requirements it could indicate non-compliance with data protection laws. Non-compliance with data protection laws can be measured using internal and external compliance audits and self-assessments. However, the objective of this research is to concentrate on the *perception* of consumers – whether they have confidence that

organisations are meeting the regulatory factor requirements based on their experience when organisations process their personal information.

The compliance/meeting expectations block serves a second purpose, namely to establish if consumers' privacy expectations are met by organisations for each of the regulatory factor requirements by comparing the results of the privacy expectations to the results of the compliance/meeting expectations. Hence, the combined name for the block include the concept of compliance and meeting expectations.

- *Gap*. The *privacy expectations* versus *compliance*/*meeting expectations* are compared to establish whether there is a gap. Any discrepancy may indicate whether the expectations of consumers are higher, or in fact lower, than what they believe organisations are currently doing. This could give organisations insight into how to promote a trusting relationship through the social contract they enter into with consumers.

- *Privacy concerns*. The privacy concerns block was added to incorporate the concepts of existing information privacy perception instruments to establish the general privacy concerns of consumers, for instance, how concerned they are about sharing their personal identification numbers, compared to financial or health-related data. Together, the privacy expectations, compliance/meeting expectations and privacy concerns blocks are used as input to define the information privacy culture index (IPCI) of a given country.

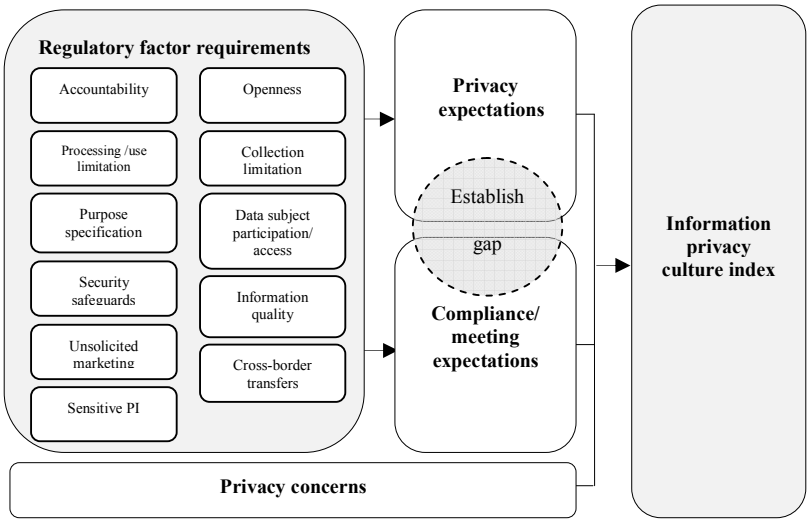


Figure 1: The information privacy culture index framework (IPCIF)

5. The proposed information privacy culture index instrument

The information privacy culture index instrument (IPCII) was developed based on the IPCIF. A number of questions were defined for each regulatory factor in figure 1, and were subsequently mapped to the relevant FIPP and OECD guideline. The questions were defined in pairs – one to measure the privacy expectation and a corresponding question to measure the compliance/meeting expectation about the same regulatory factor requirement. The questions in the privacy expectations section of the questionnaire were phrased starting with: "I expect …". By contrast, questions in the compliance/meeting expectations section were phrased as: "I feel confident that organisations are …". Using a five-point Likert scale for the privacy expectation section, the scale was defined as: I do not expect this; I sometimes expect this; Neutral; I mostly expect this; and I always expect this. For the compliance/meeting expectations questions, the following scale was used: Not at all confident; Somewhat confident; Neutral; Quite confident; and Very confident.

An expert panel, which reviewed the draft IPCII, consisted of an industry consultant who specialises in information privacy, a professor in Industrial Psychology who specialises in survey research methods as

well as opinion and attitude surveys, and three academic lecturers teaching information privacy and POPIA at honours level. The panel was required to judge each question and indicate whether it is "essential" for measuring the regulatory factor requirement and whether the question is "clear" or "unclear". A number of adjustments were made to the draft IPCII to improve the user's understanding of the questions, and to align some questions more clearly with the objective of a specific factor. This improved the content validity of the IPCII questionnaire (Saunders, Lewis and Thornhill 2016). Table 1 gives an extract of two of the questions from the first privacy factor in the regulatory factor requirements block of figure 1, namely Processing/use limitation. The second column includes the mapping to POPIA, as the first data collection exercise was conducted in South Africa. The question pairs for each requirement are listed in columns three and four. Please refer to Appendix A for the complete questionnaire.

Table 1: Extracts of statements from the information privacy culture index instrument (IPCII)

FIPP/OECD	POPIA mapping	Privacy expectations	Compliance/meeting expectations
Processing/ use limitation	Condition 2, section 9, Processing limitation, Lawfulness	b. I expect organisations to use my personal information in a lawful manner	b. I feel confident that organisations are using my personal information in lawful ways
Processing/ use limitation	Condition 2, section 9, Processing limitation, Lawfulness	c. I expect privacy when a company has to processes my personal information for services or products	c. I feel confident that organisations respect my right to privacy when collecting my personal information for services or products

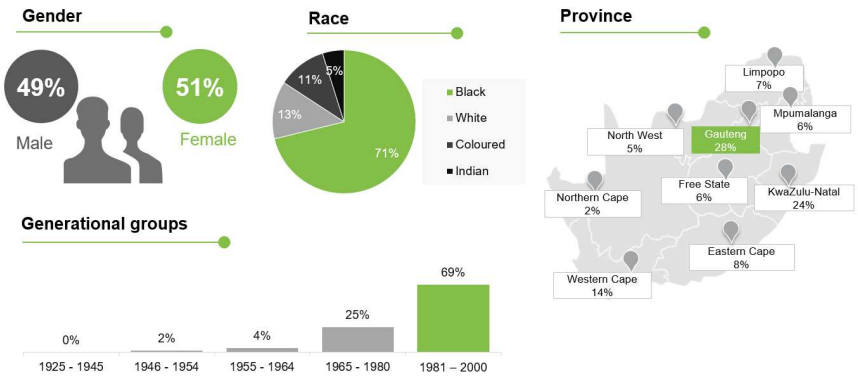
6. Research method

A survey method was employed using the IPCII to gather data from a representative sample of the South African population. This allowed the researcher to obtain numeric data about the attitudes or opinions of the population relating to the information privacy culture components (or constructs) (Creswell 2014). The data were analysed statistically to establish what the expectation and confident perceptions of consumers are. In addition, that data allowed the researcher to assess the internal consistency of the questionnaire applying the Cronbach alpha statistical test (Saunders et al. 2016).

While surveys are a cost-effective means of conducting research, they also have the benefit of including large samples of users or participants, which is necessary when seeking to obtain insight about the privacy culture across a nation (Brewerton and Millward 2002). However, care should be taken to ensure that the sample is representative, and that the measuring instrument produces reliable and valid data (Brewerton and Millward 2002). These aspects were considered as part of the research study.

6.1 Sample

The final questionnaire was converted to a web-based format. It was sent out to an opt-in database of the South African population, which is managed by a research organisation, Columinate (2018). Data were collected from 1 to 12 June 2017, and in total, 1 007 responses were obtained. The data were deemed to be representative of the demographic profile of the South African population across gender, race, province and generation groups (see figure 2). The responses also ranged across industries and education levels to allow a representative sample across South Africa.



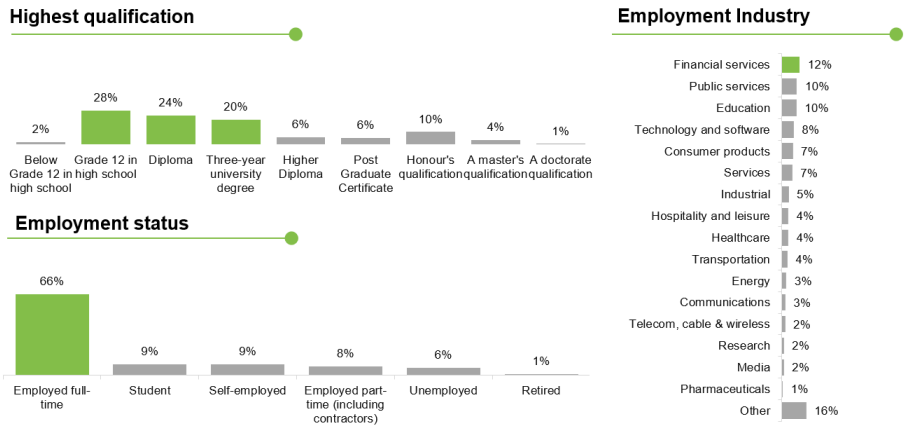


Figure 2: Responses obtained per province and race across South Africa

7. Privacy concern perspective

The data was analysed using the Statistical Package for the Social Sciences (SPSS), version 24. Over 80% of respondents expressed general concerns about the protection of their personal information. They were especially concerned about the safeguarding of their identity (94%), and their financial (92%) and health-related (80%) data. In dealing with organisations, respondents expressed greater concern about sharing their personal information online (79%), than in face-to-face transactions (57%). Most respondents indicated that they currently obtain information about their privacy rights from the internet and from banking institutions, with more than half using their cellphones as the main platform for accessing the internet. While 62% claimed to know their privacy rights when dealing with organisations, 45% indicated that their knowledge on the topic was average. Only 37% indicated that they knew where to lodge complaints if their privacy rights had been violated by organisations.

8. Results

8.1. Privacy expectations

The overall mean for the privacy expectations section was 4.57. Thus, 91.8% of respondents expressed the expectation that the regulatory factor requirements should be honoured when their personal information is processed. This indicates that there is a culture present with a high expectation towards privacy when organisations process consumers' personal information. Table 2 lists the means of each of the regulatory factor requirements. The regulatory factor requirements with the highest expectation, based on the mean, were related to security whereby consumers expect organisations to protect their personal information (4.75) by having the necessary technology and controls in place (4.70) and to safeguard this information when sending it to other countries (4.70). While South Africa's data protection act, POPIA (Republic of South Africa, 2013), has not commenced as yet, it is important for organisations to protect the personal information of their customers to build a relationship of trust by meeting the regulatory factor expectations of South African consumers.

8.2 Compliance/meeting expectations

The overall mean for the compliance/meeting expectations section was 3.02, with a 42.3% confidence on the part of the respondents that organisations are indeed complying with regulatory factor requirements. For all regulatory factor requirement questions in the IPCII, the respondents indicated that they believe organisations are not meeting requirements. It appears that consumers are not confident that South African organisations are meeting the FIPPs and OECD guidelines, and that they are in breach of the regulatory requirements of POPIA, since POPIA maps to each of the regulatory factor requirements. Of concern is the fact that the respondents were not confident that organisations are using their personal information lawfully (3.02), or for the agreed purposes (2.87) and that consent is not always obtained (3.06). Further concerns were raised about the protection of personal information, direct marketing and

cross-border transfers. This raises concerns as to whether the right to privacy, as outlined in section 14 of the Constitution of the Republic of South Africa, 1996, is maintained and what impact it has on the harmonisation with international data protection standards.

8.3 Gap

The means of the regulatory factor requirements measured in the privacy expectation and compliance/meeting expectations sections are depicted in table 2. A consolidated statement is provided for the privacy expectation and compliance/meeting expectations question pair (column one), with the respective means for each in columns two and three. The t value is provided for the paired statements (column four). Column five, gap, outlines the gaps identified between the privacy expectations (column 2) for each of the regulatory factor requirements, and whether respondents were confident the organisation's behaviour was in line with the regulatory factor requirements (compliance/meeting expectations, column 3). A significant difference was identified for all question pairs based on the t-test results. The Sig. (2-tailed) value was 0.000 for all the question pairs (significant if $p < 0.05$) and was supported by the high t values (Howell 1995). While respondents had high expectations for each regulatory factor requirement (see privacy expectation means), organisations seemed to fail to meet those requirements (see compliance/meeting expectations means).

Table 2: Privacy expectations versus compliance/meeting expectations and the related gap

Regulatory factor concepts (combined concept for expectation and compliance section in IPCII)	Privacy expectation mean	Compliance/ meeting expectations mean	t	Gap
a. Notify me before they start collecting my personal information	4.57	3.03	29.426	1.54
b. Use my personal information in a lawful manner	4.68	3.02	31.480	1.66
c. Privacy when a company has to process my personal information for services or products	4.64	3.04	30.894	1.6
d. Not to collect excessive or unnecessary information from me	4.35	3.14	22.152	1.21
e. Only collect my personal information when I have given my consent, or for a legitimate business reason	4.64	3.06	30.167	1.58
f. Only collect my personal information from myself and not from other sources	4.55	3.01	29.785	1.54
g. Explicitly define the purpose for which they want to use my information	4.65	3.05	31.521	1.6
h. Only use my personal information for purposes I agreed to and never for other purposes	4.67	2.87	33.705	1.8
i. Only keep my personal information for as long as required for business purposes or regulatory requirements	4.45	3.32	23.213	1.13
j. Obtain my consent if they want to use my personal information for purposes not agreed to with them	4.62	2.96	31.020	1.66
k. Inform me of the conditions	4.59	2.97	32.410	1.62
l. Keep my personal information updated	4.00	3.03	20.289	0.97
m. Protect my personal information	4.75	3.03	34.703	1.72
n. Organisations to have all the necessary technology and processes in place to protect my personal information	4.70	3.13	31.642	1.57
o. Ensure that third parties have all the necessary technology and processes in place to protect my information	4.64	2.99	32.985	1.68
p. Inform me if records of my personal data were lost, damaged or exposed publicly	4.68	2.73	36.488	1.95
q. Inform me what records or personal information they have about me	4.53	3.00	29.762	1.53
r. Correct or delete my personal information at my request	4.57	3.01	29.787	1.56
s. Do not collect sensitive personal information about me	4.28	3.00	23.580	1.28
t. Honour my choice if I decide not to receive direct marketing	4.66	2.99	31.432	1.67
u. Give me a choice whether I want to receive direct marketing from them	4.67	3.17	30.732	1.5
v. Protect my information when they have to send it to other countries	4.70	2.92	35.243	1.78

9. Validating the information privacy culture index instrument (IPCII)

The IPCII was subjected to an exploratory factor analysis (EFA) using the principle component analysis with the varimax rotation. The EFA was conducted on the items in the expectation and confidence

constructs. The data collected were subject to Bartlett's test of sphericity and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy, to test the aptness of the sample for the EFA (O'Rourke and Hatcher 2013). Bartlett's test of sphericity should be significant ($p < 0.05$), to indicate sampling adequacy (Howell 1995). In this research study, Bartlett's test was significant at $p < 0.00$ for the expectations and compliance / meeting expectations (confidence) constructs adding further evidence to sampling validity.

The KMO should be 0.60 or higher in order to proceed with factor analysis (O'Rourke and Hatcher 2013). In the expectations construct, three components (factors), see table 3, were identified with a KMO value of 0.950 and an eigenvalue larger than one. Kaiser (1960) recommends retaining all factors with eigenvalues greater than 1. All item loadings in the expectations construct were above 0.4, which is considered the minimum criterion to retain items in a factor (Field 2009).

Table 3: Privacy expectations table

Privacy expectation construct statements	IPCI requirements and mapping to POPIA	Component		
		1	2	3
Q24k. I expect companies to inform me of the conditions for processing my personal information	Openness (Condition 6, section 18)	0.557		
Q24m. I expect companies to protect my personal information	Security (Condition 7, section 19)	0.673		
Q24n. I expect companies to have all the necessary technology and processes in place to protect my personal information	Security (Condition 7, section 19)	0.687		
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	Security (Condition 7, section 20 & 21)	0.623		
Q24p. I expect companies to inform me if records of my personal data were lost, damaged or exposed publicly	Security (Condition 7, section 22)	0.587		
Q24q. I expect companies to tell me what records of personal information they have about me when I enquire about it	Data subject participation (Condition 8, section 23)	0.550		
Q24r. I expect companies to correct or delete my personal information at my request	Data subject participation (Condition 8, section 24)	0.638		
Q24t. I expect companies to honour my choice if I decide not to receive direct marketing	Unsolicited marketing (Section 69)	0.704		
Q24u. I expect companies to give me a choice if I want to receive direct marketing from them	Unsolicited marketing (Section 69)	0.679		
Q24v. I expect companies to protect my information when they have to send it to other countries	Cross-border transfers (Section 72)	0.694		
Q24a. I expect companies to notify me before they start collecting my personal information	Openness (Condition 6, section 18)		0.533	
Q24b. I expect companies to use my personal information in a lawful manner	Processing / Use Limitation (Condition 2, section 9)		0.766	
Q24c. I expect privacy when a company has to processes my personal information for services or products	Processing / Use Limitation (Condition 2, section 9)		0.737	
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	Processing / Use Limitation (Condition 2, section 11)		0.689	
Q24f. I expect companies to only collect my personal information from myself and not from other sources	Processing / Use Limitation (Condition 2, section 12)		0.634	
Q24g. I expect companies to explicitly define the purpose for which they want to use my information	Purpose specification (Condition 3, section 13)		0.636	
Q24h. I expect companies to only use my personal information for purposes I agreed to and never for other purposes	Purpose specification (Condition 3, section 13)		0.678	
Q24j. I expect companies to obtain my consent if they want to use my personal information for purposes not agreed to with them	Further processing (Condition 4, section 15)		0.434	
Q24d. I expect companies not to collect excessive or unnecessary information from me than what is needed for them to offer me a service or product	Processing / Use Limitation (Condition 2, section 10)			0.473
Q24i. I expect companies to only keep my personal information for as long as required for business purposes or regulatory requirements	Purpose specification (Condition 3, section 14)			0.575
Q24l. I expect companies to keep my personal information updated	Quality (Condition 6, section 16)			0.724
Q24s. 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)	Sensitive PI (section 26)			0.653

In the compliance/meeting expectations construct, one component (factor) was identified with a KMO value of 0.984. All item loadings in the compliance/meeting expectations construct were above 0.4 (see table 4).

Table 4: Compliance/meeting expectations table

Compliance/meeting expectations statement constructs	IPCI requirements and mapping POPIA	Component
		1
Q25a. I feel confident that companies are notifying me before collecting my personal information	Openness (Condition 6, section 18)	0.804
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)	Processing / Use Limitation (Condition 2, section 9)	0.854
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)	Processing / Use Limitation (Condition 2, section 9)	0.871
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)	Processing / Use Limitation (Condition 2, section 10)	0.814
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)	Processing / Use Limitation (Condition 2, section 11)	0.846
Q25f. I feel confident that companies are collecting my personal information from legitimate sources	Processing / Use Limitation (Condition 2, section 12)	0.790
Q25g. I feel confident that companies are explicitly defining the purpose they want to use my information for	Purpose specification (Condition 3, section 13)	0.849
Q25h. 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)	Purpose specification (Condition 3, section 13)	0.859
Q25i. I believe that companies are keeping my personal information indefinitely	Purpose specification (Condition 3, section 14)	0.572
Q25j. I feel confident that companies are obtaining my consent to use my personal information for purposes other than those agreed to with me	Further processing (Condition 4, section 15)	0.771
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	Openness (Condition 6, section 18)	0.855
Q25l. I feel confident that companies keep my personal information up to date	Quality (Condition 6, section 16)	0.793
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)	Security (Condition 7, section 19)	0.887
Q25n. I feel confident that companies have all the necessary technology and processes in place to protect my personal information	Security (Condition 7, section 19)	0.857
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	Security (Condition 7, section 20 & 21)	0.851
Q25p. I feel confident that companies inform me if records of my personal data were lost, damaged or exposed publicly	Security (Condition 7, section 22)	0.845
Q25q. I feel confident that companies can tell me what records or personal information they have about me	Data subject participation (Condition 8, section 23)	0.833
Q25r. I feel confident that companies will correct or delete my personal information at my request	Data subject participation (Condition 8, section 24)	0.840
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.	Sensitive PI (section 26)	0.716
Q25t. I feel confident that companies honour my choice if I do not want to receive direct marketing	Unsolicited marketing (Section 69)	0.813
Q25u. Companies always give me a choice to indicate if I want to receive direct marketing from them	Unsolicited marketing (Section 69)	0.729
Q25v. I feel confident that companies protect my information if they have to send it to other countries	Cross-border transfers (Section 72)	0.825
Q25w. I feel confident that if I submit a complaint it will be dealt with appropriately by the relevant authorities	Procedure for dealing with complaints (Section 63) (No corresponding question in the expectations construct)	0.808
Q25x. I believe that organisations take their responsibility seriously to protect my personal information	Accountability (Condition 1) (No corresponding question in the expectations construct)	0.860

The new factors were named, as displayed in table 5, with the aim of summarising the key concepts included in each factor. The Cronbach alpha for the identified factors were all above 0.8, indicating a good reliability, except for factor C. Saunders et al. (2016) recommend a minimum cut-off of 0.70. However, Cronbach alpha loadings of 0.60–0.70 can be accepted (HR Statistics 2017). If more statements are added to factor C, it should increase the Cronbach alpha coefficient. As such, additional items will be added to factor C in future research with the aim of improving the Cronbach alpha value.

Table 5: New factors and Cronbach alpha values

Factors	Number of items	Cronbach alpha
Factor A: Information protection expectations	10	0.895
Factor B: Information usage expectations	8	0.873
Factor C: Information collection expectation	4	0.642
Factor D: Confidence in meeting privacy expectations and compliance requirements	24	0.978

10. Discussion

The IPCII indicates that South Africans have high expectations regarding privacy. They are concerned about sharing their personal, financial and health-related data – especially in an online context. While indications are that privacy rights are not always protected in an online context in South Africa (Da Veiga and Swartz 2017), the index reveals that consumers are not confident that organisations in general are processing their information in line with FIPPs, or with POPIA regulatory requirements. In addition, they are unsure which recourse to take if their rights are violated. There seems to be a disconnect between what consumers expect in terms of privacy, and how consumers believe organisations are honouring those expectations, resulting in a breach of trust and the social contract being violated. As South Africans do not have a clear understanding of what their privacy rights entail, there is a need for awareness-raising and education initiatives on the part of government, the Information Regulator, as well as organisations. Organisations should engage in internal gap and compliance assessments to establish which of the regulatory factors they are contravening. That would enable them to implement measures and controls that comply with POPIA requirements.

The validated IPCI consist of four factors that can be used across countries to establish what the privacy expectations and confidence levels of consumers are. The full questionnaire is included in Appendix A. Further research will incorporate data collection in other countries, with a view to building a national information privacy culture index for comparison purposes, using a dashboard.

11. Conclusion

An information privacy culture index framework and validated information privacy culture index instrument are proposed in this paper. The objective is to measure privacy perceptions across nations by focusing on consumers' privacy expectations, their actual experiences when organisations process their personal information and general privacy concerns against the backdrop of FIPPs and OECD privacy guidelines. Data from the information privacy culture index instrument, which has been rolled out in South Africa, proved valuable in identifying gaps between consumers' information privacy expectations and what they believe is happening in reality – a scenario which has resulted in a breach of trust and the social contract being violated. In addition, it indicated that consumers have a low level of confidence that organisations are behaving in line with the FIPPs and OECD privacy guidelines as mapped to POPIA. The government, Information Regulator and organisations can leverage the results of the proposed index in order to implement controls aimed at addressing any gaps identified from a consumer and compliance perspective. The index can also be monitored over time to identify where changes are needed. Future research will focus on the inclusion of other countries, and comparisons between demographic groups.

12. Acknowledgement

This work is based on research supported wholly by the National Research Foundation of South Africa (grant number: 105735).

13. References

Australian Government (1988), *Privacy Act*, Act 119 of 1988, available at: https://www.legislation.gov.au/Series/C2004A03712 (accessed 16 February 2018).

Australian Government (2018), "Office of the Australian Information Commissioner, Statements", available at: https://www.oaic.gov.au/media-and-speeches/statements/ (accessed 16 February 2018).

Bellman, S., Johnson, E.J., Kobrin, S.K. and Lohse, G.L. (2004), "International differences in information privacy concerns: a global survey of consumers", *The Information Society*, Vol. 20, pp. 313–324.

Business Dictionary (2018), "National-culture", available at: http://www.businessdictionary.com/definition/national-culture.html (accessed 16 February 2018).

Brewerton, P. and Millward, L. (2002), *Organizational research methods*, Sage, London.

Columinate (2018), available at: https://www.columinate.com (accessed 16 February 2018).

Creswell, J.W. (2014), *Research design, qualitative, quantitative, and mixed method approaches*, Sage, Los Angeles, CA.

Da Veiga, A. and Martins N. (2015), "Information security culture and information protection culture: a validated assessment instrument", *Computer Law and Security Review*, Vol. 31 No. 2015, pp. 243–256.

Da Veiga, A. (2017), "An Information Privacy Culture Index Framework and Instrument to Measure Privacy Perceptions across Nations: Results of an Empirical Study", In Furnell, S. and Clarke N. (eds.), Proceedings of the *Eleventh International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2017), Australia, Adelaide, pp. 196-205, ISBN: 978-1-84102-428-8.

Da Veiga, A. and Swartz, P. (2017), "Personal information and regulatory requirements for direct marketing: a South African insurance industry experiment", *Research Journal of the South African Institute of Electrical Engineering (SAIEE)*, Vol. 108 No. 2, pp. 56–70.

Dell EMC (2015), "The EMC Privacy Index, global & in-depth country results", available at: https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf (accessed 16 February 2018).

Deloitte & Touche (2017), "Australian Privacy Index", available at: https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index-2017.html (accessed 16 February 2018).

DLA Piper (2018), "Data protection laws of the world", available at: https://www.dlapiperdataprotection.com/index.html (accessed 16 February 2018).

European Commission (2015), "Special Eurobarometer 431, data protection report", available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf (accessed 19 October 2017).

European Commission (2016), "Flash Eurobarometer 443, e-Privacy Report", available at: https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy (accessed 16 February 2018).

European Parliament and Council (2016), General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, *Official Journal of the European Parliament*, available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 16 February 2018).

Fair Information Practice Principles (FIPP) (2018), IT Law Wikia, available at: http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (accessed 16 February 2018).

Field, A. (2009), *Discovering statistics using SPSS*, 3rd edition, Sage Publications, London.

Great Britain (1998), *Data Protection Act*, London, Stationery Office, available at: http://www.legislation.gov.uk/ukpga/1998/29/contents (accessed 16 February 2018).

Greenleaf, G. (2014), "Sheherezade and the 101 data privacy laws: origins, significance and global trajectories", *Journal of Law, Information & Science*, Vol. 23 No. 1, pp. 1–48.

Hofstede, G., Hofstede, G.J. and Minkov, M. (2010), *Cultures and organizations: software of the mind*, 3rd ed, McGraw-Hill, New York, NY.

Howell, D.C. (1995), *Fundamental statistics for the behavioural sciences*, third edition, International Thomson Publishing, California.

HR Statistics (2017), *Quantitative research design*, HR Statistics Pty, South Africa.

Information Commission Office (ICO) of the United Kingdom (2017), "Actions we've taken", available at: https://ico.org.uk/action-weve-taken/ (accessed 16 February 2018).

Information Systems Audit and Control Association (ISACA) (2016), ISACA privacy principles and program management guide, ISACA, Rolling Meadows, IL.

Kaiser, H.F. (1960), "The application of electronic computers to factor analysis", *Educational and Psychological Measurement*, Vol. 20 No. 1, pp. 141–151.

Kemp, R., and Moore, A. D. (2007). "Privacy", *Library Hi Tech*, Vol. 25 No. 1, pp. 58–78.

KPMG (2016), "Survey reveals consumers' data privacy concerns", available at: https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html (accessed 16 February 2018).

Kumaraguru, P. and Cranor, L.F. (2005), "Privacy indexes: a survey of Westin's studies", Carnegie Mellon Univ. CMU-ISRI-5-138.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336–355.

Miltgen, C. (2009), "Online consumer privacy concerns and willingness to provide personal data on the internet", *International Journal of Networking and Virtual Organisations*, Vol. 6 No. 6, pp. 574–603.

Moore, A. (2008), "Defining privacy", *Journal of Social Philosophy*, Vol. 39 No. 3, pp. 411–428.

Morton, A. and Sasse, A.M. (2014), "Desperately seeking assurances: segmenting users by their information-seeking preferences." In the *Twelfth Annual International Conference on Privacy, Security and Trust*, Toronto, Canada: IEEE, pp. 102–111.

NCSA (2016), TRUSTe/NCSA Consumer Privacy Infographic – US Edition, available at: https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/ (accessed 16 February 2018).

O'Rourke, N. and Hatcher, A. (2013). *A step-by-step approach to using SAS for factor analysis and structural equation modelling*, SAS Institute, Cary, NC.

Phelps, J., Nowak, G. and Ferrell, E. (2000), "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy and Marketing*, Vol. 19 No. 1, pp. 27–41.

Republic of South Africa (2013), *The Protection of Personal Information Act*, Act 4 of 2013. Pretoria, Government Printer, available at: http://www.justice.gov.za/legislation/acts/2013-004.pdf (accessed 5 September 2017).

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

Smith, H.J., Milberg, S.J. and Burke, S.J. (1995), "Information privacy: measuring individual's concerns about organisational practice", *MIS Quarterly*, June, pp. 167–195.

Swire, P.P. and Ahmad, K. (2012), *Foundations of information privacy and data protection, a survey of global concepts, laws and practices,* International Association of Privacy Professionals, Portsmouth, NH.

Symantec (2015), "State of privacy report", available at: https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf (accessed 16 February 2018).

Woodruff, A., Pihus, V. and Consolvo, S. (2014), "Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin Categories, Behavioral Intentions, and Consequences", In: *Tenth Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association, Menlo Park, CA, pp. 1–18.

Appendix A - Information Privacy Culture Index Instrument (IPCII) Questionnaire

Section A: Basic demographics

The following questions are aimed at getting to know you better:

1. In which province do you reside?

Gauteng	
KwaZulu-Natal	
Limpopo	
North West	
Mpumalanga	
Free State	
Western Cape	
Eastern Cape	
Northern Cape	

2. Please indicate your race:

Black	
Coloured	
Indian	
Asian	
White	

3. When were you born?

1925 - 1945	
1946 - 1954	
1955 - 1964	
1965 - 1980	
1981 – 2000	

4. Are you…

Male	
Female	

5. What is your highest qualification?

Below Grade 12 in high school	
Grade 12 in high school	
Diploma	
Three-year university degree	
Higher Diploma	
Post Graduate Certificate	
Honour's qualification	
Master's qualification	
Doctorate qualification	
None	

6. What is your employment status?

Employed full-time	
Employed part-time (including contractors)	
Self-employed	
Unemployed	
Retired	
Student	

7. Please indicate which of the following best describes the industry you work in:

Communications	
Consumer products	
Education	
Energy	
Financial services	
Healthcare	
Hospitality and leisure	
Industrial	
Media	
Pharmaceuticals	
Public services	
Research	
Services	
Technology and software	
Telecom, cable & wireless	
Transportation	
Other (To specify in open ended)	

8. What is your total monthly personal income before tax?

I do not receive an income	
Less than R6 000	
R6 000 – R7 999	
R8 000 – R9 999	
R10 000 – R14 999	
R15 000 – R19 999	
R20 000 – R24 999	
R25 000 – R29 999	
R30 000 – R39 999	
R40 000 – R49 999	
R50 000 – R59 999	
R60 000 – R79 999	
R80 000 – R99 999	
R100 000 – R149 999	
R150 000 – R199 999	
R200 000 +	

Section B: Use of technology and privacy rights knowledge

In the following section, we would like to know more about your internet use and knowledge of your privacy rights.

9. What device do you mostly use to access the internet?

Cellphone	
Laptop	
Tablet	
Desktop	

10. Please indicate for what purposes you use your devices when connected to the internet:

Browsing the internet	
Internet banking	
Social media, such as Facebook, Twitter and so forth	
Playing games	
Maps and navigation	
Instant messages, for example, SMS or WhatsApp, chat programmes	
Downloading videos, music or books	
Sending and receiving e-mails	
Using online applications (GPS, health, financial etc.)	
Saving information in the cloud: photos in Dropbox	
Making phone calls	
Selling products/services	
Buying products/services	
Other (To specify in open ended)	

10b. Please specify for what purposes you use your devices when connected to the internet.

11. How concerned are you about the protection of your personal information?

Not concerned	
Somewhat concerned	
Neutral	
Concerned	
Extremely concerned	

12. How would you rate your knowledge of your privacy rights?

Very poor	
Poor	
Average	
Good	
Very good	

13. How concerned are you to share your personal information with companies on the internet?

Not concerned	
Somewhat concerned	
Neutral	
Concerned	
Extremely concerned	

14. How concerned are you to share your personal information with companies in everyday business transactions that do not involve the internet? (ie face to face transactions)

Not concerned	
Somewhat concerned	
Neutral	
Concerned	
Extremely concerned	

15. 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)?

Yes	
No	

16. 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	

17. Do you know of someone whose personal information has been misused by another person (conducted fraudulent transactions, exposed confidential information)?

Yes	
No	

18. Where have you obtained information on your privacy rights in the past?

Internet/websites	
The government	
The organisation where I work	
Organisations to whom I provide my personal information	
At a bank (my personal bank and others)	
At a school, college or university	
My family or friends	
A book	
In a newspaper or magazine	
Television or radio	
Individual discussions with experts	
Workshops by experts	
Pamphlets	
SMS (from government or companies)	
Nowhere	
Other (To specify in open ended)	

18b. Please specify where have you obtained information on your privacy rights in the past.

19. Which method(s) would you prefer to receive more information on your privacy rights? Please rank your top 5 methods from the options below in order of preference, where 1 = most preferred' and 5 = least preferred.

Internet/websites	
The government	
The organisation where I work	
Organisations to whom I provide my personal information	
The bank	
At a school, college or university	
My family or friends	
A book	
In a newspaper or magazine	
Television or radio	
Individual discussions with experts	
Workshops by experts	
Pamphlets	
SMS	
Nowhere	
Other (To specify in open ended)	

19b. Please specify which other method(s) would you prefer to receive more information on your privacy rights?

20. How concerned are you about the protection of your financial information?

Not concerned	
Somewhat concerned	
Neutral	
Concerned	
Extremely concerned	

21. How concerned are you about the protection of your health information?

Not concerned	
Somewhat concerned	
Neutral	
Concerned	
Extremely concerned	

22. How concerned are you about the protection of your identification information online (eg name, ID number etc)?

Not concerned	
Somewhat concerned	
Neutral	
Concerned	
Extremely concerned	

23. Please indicate the extent to which you agree or disagree with the following statement:

"I know where to submit a complaint if I believe a company did not protect my personal information."

Strongly disagree	
Disagree	
Neutral	
Agree	
Strongly agree	

Section C: Privacy expectations

In the following section, we would like to know more about your expectations from companies regarding their treatment of your personal information.

24. Please rate the extent to which you expect companies to handle your personal information in the various scenarios below:

	I always expect this	I mostly expect this	Neutral	I sometimes expect this	I do not expect this
24a. I expect companies to notify me before they start collecting my personal information.	○	○	○	○	○
24b. 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).	○	○	○	○	○
24c. I expect privacy when a company has to processes my personal information for services or products (e.g. never share my information with unauthorised personnel or use my information for other purposes).	○	○	○	○	○
24d.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.	○	○	○	○	○

24e.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.	○	○	○	○	○
24f. I expect companies to only collect my personal information from myself and not from other sources (e.g. from other companies, people I know).	○	○	○	○	○
24g. I expect companies to explicitly define the purpose for which they want to use my information.	○	○	○	○	○
24h. I expect companies to only use my personal information for purposes I agreed to and never for other purposes (e.g. tele marketing, targeted advertising) than those agreed by me.	○	○	○	○	○
24i. I expect companies to only keep my personal information for as long as required for business purposes or regulatory requirements.	○	○	○	○	○
24j. I expect companies to obtain my consent if they want to use my personal information for purposes not agreed to with them.	○	○	○	○	○
24k. 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.	○	○	○	○	○
24l. I expect companies to keep my personal information updated.	○	○	○	○	○
24m. I expect companies to protect my personal information.	○	○	○	○	○
24n. I expect companies to have all the necessary technology and processes in place to protect my personal information.	○	○	○	○	○
24o. 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.	○	○	○	○	○
24p. I expect companies to inform me if records of my personal data were lost, damaged or exposed publicly.	○	○	○	○	○
24q. I expect companies to tell me what records of personal information they have about me when I enquire about it.	○	○	○	○	○
24r. I expect companies to correct or delete my personal information at my request.	○	○	○	○	○
24s. 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)	○	○	○	○	○
24t. I expect companies to honour my choice if I decide not to receive direct marketing.	○	○	○	○	○
24u. I expect companies to give me a choice if I want to receive direct marketing from them.	○	○	○	○	○
24v.I expect companies to protect my information when they have to send it to other countries.	○	○	○	○	○

Section D: Perceptions of compliance/meeting privacy expectations

In the following section, we would like to know more about your confidence in companies regarding their treatment of your personal information.

25. Please rate the extent to which you are confident of companies' compliance with the law, when dealing with your personal information in various scenarios below:

	Very confident	Quite confident	Neutral	Somewhat confident	Not at all confident
25a .I feel confident that companies are notifying me before collecting my personal information.	○	○	○	○	○
25b. 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).	○	○	○	○	○
25c. 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).	○	○	○	○	○
25d. 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)	○	○	○	○	○
25e. 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).	○	○	○	○	○
25f.I feel confident that companies are collecting my personal information from legitimate sources.	○	○	○	○	○
25g. I feel confident that companies are explicitly defining the purpose they want to use my information for.	○	○	○	○	○
25h. I believe that companies are only using my personal information for purposes I agreed to and never for other purposes (e.g. tele marketing, targeted advertising).	○	○	○	○	○
25i. I believe that companies are keeping my personal information indefinitely.	○	○	○	○	○
25j. I feel confident that companies are obtaining my consent to use my personal information for purposes other than those agreed to with me.	○	○	○	○	○
25k.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.	○	○	○	○	○

25l. I feel confident that companies keep my personal information up to date.	○	○	○	○	○
25m. 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).	○	○	○	○	○
25n. I feel confident that companies have all the necessary technology and processes in place to protect my personal information.	○	○	○	○	○
25o. I feel confident that companies ensure that their third parties have all the necessary technology and processes in place to protect my personal information.	○	○	○	○	○
25p. I feel confident that companies inform me if records of my personal data were lost, damaged or exposed publicly.	○	○	○	○	○
25q. I feel confident that companies can tell me what records or personal information they have about me.	○	○	○	○	○
25r. I feel confident that companies will correct or delete my personal information at my request.	○	○	○	○	○
26s. 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.	○	○	○	○	○
25t. I feel confident that companies honour my choice if I do not want to receive direct marketing.	○	○	○	○	○
25u. Companies always give me a choice to indicate if I want to receive direct marketing from them.	○	○	○	○	○
25v. I feel confident that companies protect my information if they have to send it to other countries.	○	○	○	○	○
25w. I feel confident that if I submit a complaint it will be dealt with appropriately by the relevant authorities.	○	○	○	○	○
25x. I believe that organisations take their responsibility seriously to protect my personal information.	○	○	○	○	○

Thank you for your participation.