An information privacy culture instrument to measure consumer privacy expectations and confidence
Adéle Da Veiga,

Article information:

To cite this document:
Permanent link to this document:
https://doi.org/10.1108/ICS-03-2018-0036

Downloaded on: 19 June 2019, At: 06:27 (PT)
References: this document contains references to 42 other documents.
To copy this document: permissions@emeraldinsight.com
The fulltext of this document has been downloaded 448 times since 2018*

Users who downloaded this article also downloaded:


Access to this document was granted through an Emerald subscription provided by All users group

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.
An information privacy culture instrument to measure consumer privacy expectations and confidence

Adéle Da Veiga
School of Computing, University of South Africa (Unisa) Johannesburg, South Africa

Abstract
Purpose – This paper aims to propose 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 and 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 (IPCI) and to validate the questionnaire.

Findings – The IPCI 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 to address consumer privacy expectations and concerns.

Originality/value – The IPCIF and validated IPCII are the first tools that combine 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 and the privacy guidelines of the Organisation for Economic Cooperation and Development, to determine gaps and define improvement plans.

Keywords Culture, Consumer protection, Information privacy, Data protection, Data privacy, Protection of personal information act (POPIA), General Data Protection Regulation (GDPR), Fair information practice principles (FIPPS), Organisation of Economic Coordination and Development (OECD)

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 100 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

This work is based on research supported wholly by the National Research Foundation of South Africa (grant number: 105735).
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., 1996; Bellman et al., 2004; Malhotra et al., 2004; Dell EMC, 2015; Symantec, 2015; Deloitte and Touche, 2017). Privacy expectations and 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 IPCI 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, p. 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. Information Systems Audit and Control Association (ISACA) (2016) refers to a privacy culture as one that adopts privacy protection behaviours, such as ethical behaviour and proactive privacy communication. 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, p. 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. (1996)*, 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 et al., 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 et al., 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 as follows (*Kumaraguru and Cranor, 2005; Miltgen, 2009*):

1. **Privacy fundamentalists.** Members of this group are mainly concerned about
sharing and safeguarding their personal information.

2. **Privacy pragmatists.** They tend to seek a balance between the advantages and
disadvantages of sharing private information, before arriving at a decision.

3. **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, p. 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; Information Commission Office (ICO) of the United Kingdom, 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 and 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 focus on respondents’ views on privacy and awareness in an online context or on 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 (1996) 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 the 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
The IPCIF is portrayed in Figure 1 as outlined in Da Veiga (2017). The components are as follows.

4.1 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. These factors are in line with developments in Europe with regard to the General Data Protection Regulation (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 UK (Great Britain, 1998) and Australia’s Privacy Act (Australian 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.

Figure 1.
The IPCIF
4.2 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.

4.3 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.

4.4 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.

4.5 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 IPCI of a given country.

5. The proposed information privacy culture index instrument
The 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 et al., 2016). Table I 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 the Appendix for the complete questionnaire.

### 6. Research method

A survey method was utilised 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’s 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).

<table>
<thead>
<tr>
<th>FIPP/OECD</th>
<th>POPIA mapping</th>
<th>Privacy expectations</th>
<th>Compliance/meeting expectations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing/use limitation</td>
<td>Condition 2, Section 9, Processing limitation, Lawfulness</td>
<td>I expect organisations to use my personal information in a lawful manner</td>
<td>I feel confident that organisations are using my personal information in lawful ways</td>
</tr>
<tr>
<td>Processing/use limitation</td>
<td>Condition 2, Section 9, Processing limitation, Lawfulness</td>
<td>I expect privacy when a company has to processes my personal information for services or products</td>
<td>I feel confident that organisations respect my right to privacy when collecting my personal information for services or products</td>
</tr>
</tbody>
</table>

**Table I.** Extracts of statements from the IPCII
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 (Figure 2). The responses also ranged across industries and education levels to allow a representative sample across South Africa.

7. Privacy concern perspective
The data were analysed using the Statistical Package for the Social Sciences (SPSS), version 24. Over 80 per cent of respondents expressed general concerns about the protection of their personal information. They were especially concerned about the safeguarding of their

---

**Figure 2.**
Responses obtained per province and race across South Africa
identity (94 per cent), and their financial (92 per cent) and health-related (80 per cent) data. In dealing with organisations, respondents expressed greater concern about sharing their personal information online (79 per cent), than in face-to-face transactions (57 per cent). 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 cell phones as the main platform for accessing the internet. While 62 per cent claimed to know their privacy rights when dealing with organisations, 45 per cent indicated that their knowledge on the topic was average. Only 37 per cent 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 per cent 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 II 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, namely (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 per cent 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, as 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 II. A consolidated statement is provided for the privacy expectation and compliance/meeting expectations question pair (Column 1), with the respective means for each in columns two and three. The t-values are provided for the paired statements (Column 4). Column 5, 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
<table>
<thead>
<tr>
<th>Regulatory factor concepts (combined concept for expectation and compliance section in IPCII)</th>
<th>Privacy expectation mean</th>
<th>Compliance/meeting expectations mean</th>
<th>t</th>
<th>Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Notify me before they start collecting my personal information</td>
<td>4.57</td>
<td>3.03</td>
<td>29.426</td>
<td>1.54</td>
</tr>
<tr>
<td>b. Use my personal information in a lawful manner</td>
<td>4.68</td>
<td>3.02</td>
<td>31.480</td>
<td>1.66</td>
</tr>
<tr>
<td>c. Privacy when a company has to process my personal information for services or products</td>
<td>4.64</td>
<td>3.04</td>
<td>30.884</td>
<td>1.6</td>
</tr>
<tr>
<td>d. Not to collect excessive or unnecessary information from me</td>
<td>4.35</td>
<td>3.14</td>
<td>22.152</td>
<td>1.21</td>
</tr>
<tr>
<td>e. Only collect my personal information when I have given my consent, or for a legitimate business reason</td>
<td>4.64</td>
<td>3.06</td>
<td>30.167</td>
<td>1.58</td>
</tr>
<tr>
<td>f. Only collect my personal information from myself and not from other sources</td>
<td>4.55</td>
<td>3.01</td>
<td>29.785</td>
<td>1.54</td>
</tr>
<tr>
<td>g. Explicitly define the purpose for which they want to use my information</td>
<td>4.65</td>
<td>3.05</td>
<td>31.521</td>
<td>1.6</td>
</tr>
<tr>
<td>h. Only use my personal information for purposes I agreed to and never for other purposes</td>
<td>4.67</td>
<td>2.87</td>
<td>33.705</td>
<td>1.8</td>
</tr>
<tr>
<td>i. Only keep my personal information for as long as required for business purposes or regulatory requirements</td>
<td>4.45</td>
<td>3.32</td>
<td>23.213</td>
<td>1.13</td>
</tr>
<tr>
<td>j. Obtain my consent if they want to use my personal information for purposes not agreed to with them</td>
<td>4.62</td>
<td>2.96</td>
<td>31.020</td>
<td>1.66</td>
</tr>
<tr>
<td>k. Inform me of the conditions</td>
<td>4.59</td>
<td>2.97</td>
<td>32.410</td>
<td>1.62</td>
</tr>
<tr>
<td>l. Keep my personal information updated</td>
<td>4.00</td>
<td>3.03</td>
<td>20.289</td>
<td>0.97</td>
</tr>
<tr>
<td>m. Protect my personal information</td>
<td>4.75</td>
<td>3.03</td>
<td>34.703</td>
<td>1.72</td>
</tr>
<tr>
<td>n. Organisations to have all the necessary technology and processes in place to protect my personal information</td>
<td>4.70</td>
<td>3.13</td>
<td>31.642</td>
<td>1.57</td>
</tr>
<tr>
<td>o. Ensure that third parties have all the necessary technology and processes in place to protect my personal information</td>
<td>4.64</td>
<td>2.99</td>
<td>32.985</td>
<td>1.68</td>
</tr>
<tr>
<td>p. Inform me if records of my personal data were lost, damaged or exposed publicly</td>
<td>4.68</td>
<td>2.73</td>
<td>36.488</td>
<td>1.95</td>
</tr>
<tr>
<td>q. Inform me what records or personal information they have about me</td>
<td>4.53</td>
<td>3.00</td>
<td>29.762</td>
<td>1.53</td>
</tr>
<tr>
<td>r. Correct or delete my personal information at my request</td>
<td>4.57</td>
<td>3.01</td>
<td>29.787</td>
<td>1.56</td>
</tr>
<tr>
<td>s. Do not collect sensitive personal information about me</td>
<td>4.28</td>
<td>3.00</td>
<td>23.580</td>
<td>1.28</td>
</tr>
<tr>
<td>t. Honour my choice if I decide not to receive direct marketing</td>
<td>4.66</td>
<td>2.99</td>
<td>31.432</td>
<td>1.67</td>
</tr>
<tr>
<td>u. Give me a choice whether I want to receive direct marketing from them</td>
<td>4.67</td>
<td>3.17</td>
<td>30.732</td>
<td>1.5</td>
</tr>
<tr>
<td>v. Protect my information when they have to send it to other countries</td>
<td>4.70</td>
<td>2.92</td>
<td>35.243</td>
<td>1.78</td>
</tr>
</tbody>
</table>
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. (two-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).

9. Validating the information privacy culture index instrument

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 to proceed with factor analysis (O’Rourke and Hatcher, 2013). In the expectations construct, three components (factors) (Table III) 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).

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 (Table IV).

The new factors were named, as displayed in Table V, with the aim of summarising the key concepts included in each factor. The Cronbach’s 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’s 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’s alpha coefficient. As such, additional items will be added to factor C in future research with the aim of improving the Cronbach’s alpha value.

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 and 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.
<table>
<thead>
<tr>
<th>Privacy expectation construct statements</th>
<th>IPCI requirements and mapping to POPIA</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q24k. I expect companies to inform me of the conditions for processing my personal information</td>
<td>Openness (Condition 6, Section 18)</td>
<td>0.557</td>
</tr>
<tr>
<td>Q24m. I expect companies to protect my personal information</td>
<td>Security (Condition 7, Section 19)</td>
<td>0.673</td>
</tr>
<tr>
<td>Q24n. I expect companies to have all the necessary technology and processes in place to protect my personal information</td>
<td>Security (Condition 7, Section 19)</td>
<td>0.687</td>
</tr>
<tr>
<td>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</td>
<td>Security (Condition 7, Section 20 and 21)</td>
<td>0.623</td>
</tr>
<tr>
<td>Q24p. I expect companies to inform me if records of my personal data were lost, damaged or exposed publicly</td>
<td>Security (Condition 7, Section 22)</td>
<td>0.587</td>
</tr>
<tr>
<td>Q24q. I expect companies to tell me what records of personal information they have about me when I enquire about it</td>
<td>Data subject participation (Condition 8, Section 23)</td>
<td>0.550</td>
</tr>
<tr>
<td>Q24r. I expect companies to correct or delete my personal information at my request</td>
<td>Data subject participation (Condition 8, Section 24)</td>
<td>0.638</td>
</tr>
<tr>
<td>Q24t. I expect companies to honour my choice if I decide not to receive direct marketing</td>
<td>Unsolicited marketing (Section 69)</td>
<td>0.704</td>
</tr>
<tr>
<td>Q24u. I expect companies to give me a choice if I want to receive direct marketing from them</td>
<td>Unsolicited marketing (Section 69)</td>
<td>0.679</td>
</tr>
<tr>
<td>Q24v. I expect companies to protect my information when they have to send it to other countries</td>
<td>Cross-border transfers (Section 72)</td>
<td>0.694</td>
</tr>
<tr>
<td>Q24a. I expect companies to notify me before they start collecting my personal information</td>
<td>Openness (Condition 6, Section 18)</td>
<td>0.533</td>
</tr>
<tr>
<td>Q24b. I expect companies to use my personal information in a lawful manner</td>
<td>Processing/Use Limitation (Condition 2, Section 9)</td>
<td>0.766</td>
</tr>
<tr>
<td>Q24c. I expect privacy when a company has to processes my personal information for services or products</td>
<td>Processing/Use Limitation (Condition 2, Section 9)</td>
<td>0.737</td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Privacy expectation construct statements</th>
<th>IPCI requirements and mapping to POPIA</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>Processing/Use Limitation (Condition 2, Section 11)</td>
<td>0.689</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q24f. I expect companies to only collect my personal information from myself and not from other sources</td>
<td>Processing/Use Limitation (Condition 2, Section 12)</td>
<td>0.634</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q24g. I expect companies to explicitly define the purpose for which they want to use my information</td>
<td>Purpose specification (Condition 3, Section 13)</td>
<td>0.636</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q24h. I expect companies to only use my personal information for purposes I agreed to and never for other purposes</td>
<td>Purpose specification (Condition 3, Section 13)</td>
<td>0.678</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q24i. I expect companies to obtain my consent if they want to use my personal information for purposes not agreed to with them</td>
<td>Further processing (Condition 4, Section 15)</td>
<td>0.434</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>Processing/Use Limitation (Condition 2, Section 10)</td>
<td>0.473</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q24j. I expect companies to only keep my personal information for as long as required for business purposes or regulatory requirements</td>
<td>Purpose specification (Condition 3, Section 14)</td>
<td>0.575</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q24k. I expect companies to keep my personal information updated</td>
<td>Quality (Condition 6, Section 16)</td>
<td>0.724</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Sensitive PI (Section 26)</td>
<td>0.653</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance/meeting expectations statement constructs</td>
<td>IPCI requirements and mapping</td>
<td>Component 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25a. I feel confident that companies are notifying me before collecting my personal information</td>
<td>Openness (Condition 6, Section 18)</td>
<td>0.804</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Processing/Use Limitation (Condition 2, Section 9)</td>
<td>0.854</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Processing/Use Limitation (Condition 2, Section 9)</td>
<td>0.871</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Processing/Use Limitation (Condition 2, Section 10)</td>
<td>0.814</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Processing/Use Limitation (Condition 2, Section 11)</td>
<td>0.846</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25f. I feel confident that companies are collecting my personal information from legitimate sources</td>
<td>Purpose specification (Condition 3, Section 12)</td>
<td>0.790</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25g. I feel confident that companies are explicitly defining the purpose they want to use my information for</td>
<td>Purpose specification (Condition 3, Section 13)</td>
<td>0.849</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Purpose specification (Condition 3, Section 13)</td>
<td>0.859</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25i. I believe that companies are keeping my personal information indefinitely</td>
<td>Purpose specification (Condition 3, Section 14)</td>
<td>0.572</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25j. I feel confident that companies are obtaining my consent to use my personal information for purposes other than those agreed to with me</td>
<td>Further processing (Condition 4, Section 15)</td>
<td>0.771</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>Openness (Condition 6, Section 18)</td>
<td>0.855</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25l. I feel confident that companies keep my personal information up to date</td>
<td>Quality (Condition 6, Section 16)</td>
<td>0.793</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Security (Condition 7, Section 19)</td>
<td>0.887</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q25n. I feel confident that companies have all the necessary technology and processes in place to protect my personal information</td>
<td>Security (Condition 7, Section 19)</td>
<td>0.857</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table IV. Compliance/meeting expectations (continued)
The validated IPCI consists 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 the Appendix. Further research will incorporate data collection in other countries, with a view to building a national IPCI for comparison purposes, using a dashboard.

11. Conclusion
An IPCIF and a validated IPCI 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 IPCI 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 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.

References


Appendix. 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

(continued)
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 +

(continued)
### 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

(continued)
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.

(continued)
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.

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

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?**

<table>
<thead>
<tr>
<th>Concern level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not concerned</td>
<td></td>
</tr>
<tr>
<td>Somewhat concerned</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Concerned</td>
<td></td>
</tr>
<tr>
<td>Extremely concerned</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Concern level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not concerned</td>
<td></td>
</tr>
<tr>
<td>Somewhat concerned</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Concerned</td>
<td></td>
</tr>
<tr>
<td>Extremely concerned</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Concern level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not concerned</td>
<td></td>
</tr>
<tr>
<td>Somewhat concerned</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Concerned</td>
<td></td>
</tr>
<tr>
<td>Extremely concerned</td>
<td></td>
</tr>
</tbody>
</table>

*(continued)*
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."

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
</table>

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:

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 process 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.

(continued)
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>24i. I expect companies to only keep my personal information for as long as required for business purposes or regulatory requirements.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24j. I expect companies to obtain my consent if they want to use my personal information for purposes not agreed to with them.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24l. I expect companies to keep my personal information updated.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24m. I expect companies to protect my personal information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24n. I expect companies to have all the necessary technology and processes in place to protect my personal information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24p. I expect companies to inform me if records of my personal data were lost, damaged or exposed publicly.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24q. I expect companies to tell me what records of personal information they have about me when I enquire about it.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24r. I expect companies to correct or delete my personal information at my request.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24t. I expect companies to honour my choice if I decide not to receive direct marketing.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24u. I expect companies to give me a choice if I want to receive direct marketing from them.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24v. I expect companies to protect my information when they have to send it to other countries.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(continued)
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:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>25a. I feel confident that companies are notifying me before collecting my personal information.</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>25f. I feel confident that companies are collecting my personal information from legitimate sources.</td>
<td></td>
</tr>
<tr>
<td>25g. I feel confident that companies are explicitly defining the purpose they want to use my information for.</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>25i. I believe that companies are keeping my personal information indefinitely.</td>
<td></td>
</tr>
<tr>
<td>25j. I feel confident that companies are obtaining my consent to use my personal information for purposes other than those agreed to with me.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

(continued)
25. 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.

26. 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.

Corresponding author
Adèle Da Veiga can be contacted at: dveiga@unisa.ac.za

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com