An Information Privacy Culture Index Framework and Instrument to Measure Privacy Perceptions across Nations: Results of an Empirical Study

A. da Veiga

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

Abstract

This research proposes an Information Privacy Culture Index Framework (IPCIF) with a related Information Privacy Culture Index Instrument (IPCII) to measure privacy perceptions across nations. The proposed framework is based on three concepts, namely that an information privacy culture encompasses consumers' privacy expectations, their actual experiences when organisations process their personal information, as well as their general privacy concerns. The underlying foundation of the framework is based on the Fair Information Practice Principles and OECD privacy guidelines, to allow for comparison of consumers' expectations across data protection jurisdictions. A survey method was deployed to collect data in South Africa – the first participating country in the study – to build a global information privacy culture index. The index revealed that South Africans have a very high expectation of privacy, but that they feel organisations are failing to meet both those expectations and the regulatory requirements of this county's data protection laws. 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 has resulted in a breach of trust and of the social contract. The government, the Information Regulator and organisations can leverage the results of the index in order to implement controls aimed at addressing the gaps identified from a consumer and compliance perspective.

Keywords

Culture, data privacy, index, information privacy, framework, consumer, perceptions, questionnaire

1. Introduction

Various studies have been conducted into privacy and the concerns which consumers and nations have regarding the concept (Smith et al. 1995; Bellman et al. 2004; Malhotra 2004; Dell EMC 2015; Symantec 2015; Deloitte & Touche 2017). Privacy concerns and expectations vary between nations and also within the demographic groups which make up a nation. At the same time, 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 2017). Additional insight can be obtained if the privacy expectations of consumers or nations are compared to their actual experiences when organisations process their personal information. That will allow

for the identification of gaps, which will help improve the safeguarding of personal information and to 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 2017) 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. The discussion of the results is followed by the conclusion.

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).

The definition of an information protection culture focuses on the organisational context, which incorporates the perspectives of employees, rather than the level of a national culture, to determine how privacy is perceived from a consumer perspective. The *Business Dictionary* (2017) 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 regarding the processing of 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 which focuses on information collection, unauthorised secondary use, improper access and errors. This instrument has been expanded to incorporate internet user concerns which 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 the consumer and the organisation, when the former provides his/her personal information to the latter, and s/he has 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 consumer's personal information with third parties, without being granted consent.

Consumers' expectations regarding the way in which organisations use and protect their personal information, might 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 are people who 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 might be highly concerned if their personal information were shared with third parties, whereas the privacy unconcerned group might 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) in five categories with regards to their privacy concerns and the use of technology: information controllers (seeking to control their personal information collection, use and sharing), security concerned (expects security of personal information), benefit seekers (value the benefits in return for providing personal information), crowd followers (rely on advice from family or friends) and organisational assurance seekers (require 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, pp.102). 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.

Globally, more than 100 countries have enacted data protection legislation (or referred to as privacy legislation) (Greenleaf 2014; DLA Piper 2017). The FIPPs (FIPP 2017) 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).

While consumers might have diverse expectations regarding 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 might have expectations that are in line with data protection regulatory requirements (e.g. privacy fundamentalists), while other groups (e.g., privacy unconcerned) might 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 2017; ICO 2017).

Other 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 regarding 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 which have been implemented. These instruments do not 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, nor 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 will aid in comparing indices across nations.

4. The proposed Information Privacy Culture Index Framework (IPCIF)

The Information Privacy Culture Index Framework (IPCIF) is portrayed in Figure 1. The components are as following:

- *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), 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 which 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 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 might 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' behavior 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 as to whether they have confidence that organisations are meeting the regulatory factor requirements which is formed 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 including 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 could 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.

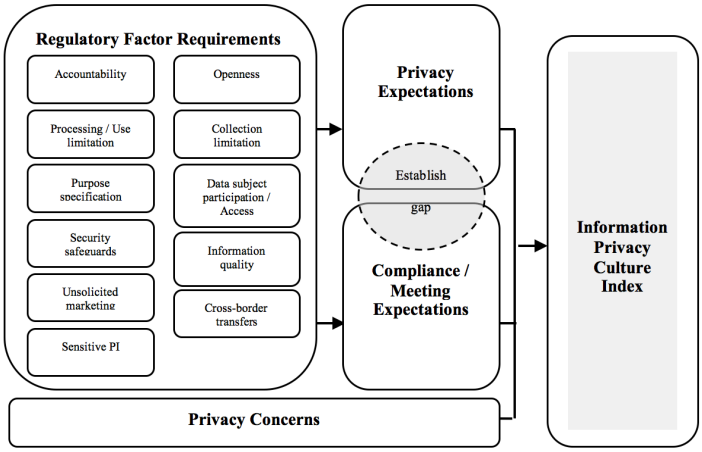

Figure 1: The Information Privacy Culture Index Framework (IPCIF)

5. 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 et al. 2009). 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.

FIPP / OECD	POPIA mapping	Privacy expectations	Meeting expectations/ compliance
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

Table 1: Extracts of statements from the Information Privacy Culture Index Instrument (IPCII)

6. Research method

A survey method was employed using the IPCII to gather data from a sample of the South African population, which was analysed through statistical analysis. 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). Care should, however, 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 (2017). Data were collected from 1–12 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 racial groups, provinces and gender (see Figure 2).

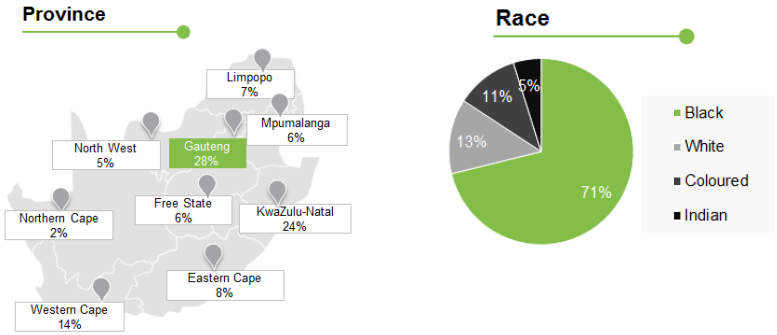

Figure 2: Responses obtained per province and race across South Africa

7. Privacy concern perspective

The data was analysed using the Statistical Package for the Social Sciences (SPSS), version 24. Over 80 per cent 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 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 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 also 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 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 20 regulatory factor requirement questions in the IPCII, the respondents indicated that they believe organisations are not meeting it. It appears as though consumers are not confident that South African organisations are meeting the FIPPS and OECD guidelines as well as to be in breach of the regulatory requirements of POPIA, since POPIA maps to the 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 with regard to 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 the impact which 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 regarding each regulatory factor requirement (see privacy expectation means), organisations seemed to fail to meet those requirements (see compliance / meeting expectations means).

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 processes 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 to 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

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

9. 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 of the social contract. 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 will enable them to implement measures and controls which comply with POPIA requirements.

This research is part of a larger project in which the questionnaire will be validated (using factor and item analysis), as will the framework (using structural equation modelling). Further research will also incorporate data collection in other countries, with a view to building a national information privacy culture index for comparison purposes, using a dashboard.

10. Conclusion

An Information Privacy Culture Index Framework, with the related 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 the Fair Information Practice Principles and OECD privacy guidelines. Data from the Information Privacy Culture Index Instrument, which was 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 there is a low level of confidence in consumers that organisations are behaving in line with the Fair Information Practice Principles 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 include the validation of the framework and the instrument, the inclusion of other countries, and comparisons between demographic groups.

11. Acknowledgement

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

12. References

Australian Government (1988), Privacy Act, Act 119 of 1988, https://www.legislation.gov.au/Series/C2004A03712 (Accessed 15 August 2017).

Australian Government (2017), "Office of the Australian Information Commissioner, Statements", https://www.oaic.gov.au/media-and-speeches/statements/ (Accessed 30 August 2017).

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 (2017), "National-culture", http://www.businessdictionary.com/definition/national-culture.html (Accessed 30 August 2017).

Brewerton P. and Millward L. (2002), Organizational Research Methods, Sage, London.

Columinate (2017), https://www.columinate.com (Accessed 30 August 2017).

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. 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", https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf (Accessed 30 August 2017).

Deloitte & Touche (2017), "Australian Privacy Index", https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index-2017.html (Accessed 30 August 2017).

DLA Piper (2017), "Data Protection Laws of the World", https://www.dlapiperdataprotection.com/index.html (Accessed 15 August 2017).

European Commission. (2015), "Special Eurobarometer 431, Data Protection Report", 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", https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy (Accessed 22 October 2017).

European Parliament and Council (2016), General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Official Journal of the European Parliament,

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (Accessed 15 August 2017).

Fair Information Practice Principles (FIPP) (2017), IT Law Wikia, http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (Accessed 15 August 2017).

Great Britain (1998), Data Protection Act, London, Stationery Office, http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 15 August 2017).

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.

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

Information Commission Office (ICO) of the United Kingdom (2017), "Actions We've Taken", https://ico.org.uk/action-weve-taken/ (Accessed 30 August 2017).

KPMG (2016), "Survey Reveals Consumers' Data Privacy Concerns", https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-se)e-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html (Accessed 30 August 2017).

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.

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, https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/ (Accessed 30 August 2017).

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, http://www.justice.gov.za/legislation/acts/2013-004.pdf, (Accessed 5 September 2017).

Saunders, M., Lewis, P., and Thornhill, A. (2009), Research Methods for Business Students, 5th ed., Pearson Education, Essex.

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.

Symantec (2015), "State of Privacy Report", https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf (Accessed 30 August 2017).

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.