An online information privacy culture

A framework and validated instrument to measure consumer expectations and confidence

Adéle da Veiga

College of Science, Engineering and Technology, School of Computing, University of South Africa, P.O. Box 392, UNISA 0003, South Africa

dveiga@unisa.ac.za

Abstract—Information privacy concerns extend to the online environment with consumers having different expectations towards privacy. While privacy is regulated in many countries the perception of online consumers, the privacy culture, vary as indicated in various global surveys. This research aims to develop a validated instrument that can be used to measure the online information privacy culture of consumers. For this purpose a conceptual Online Information Privacy Culture Index Framework (OIPCIF) is proposed based on the Fair Information Practice Principles (FIPPs) and the OECD privacy guidelines. The Online Information Privacy Culture Index Questionnaire (OIPCIQ) is conceptualized and validated using factor and item analysis. The OIPCO was rolled out in South Africa as the first participating country in the study for which recommendations are made based on the outcomes.

Keywords— privacy; culture; consumer; perceptions; confidence; POPIA; protection of personal information; index; validated instrument; framework; data protection

I. INTRODUCTION

Online companies have to consider the privacy concerns of consumers to establish trust when processing personal information [1], [2]. Privacy concerns of consumers vary between countries and even between demographical groups as evident in global privacy concern studies that have been conducted [3], [4]. While consumers have certain expectations towards the processing of their personal information, which companies should take into account, companies must at the same time comply with data protection legislation. Current privacy concern studies focus mostly on the concerns [5] or expectations of consumers towards privacy [1][3][4]. The existing studies however, does not compare consumers' privacy expectations with their confidence as to whether companies are meeting their privacy expectations in line with general accepted information privacy principles such as that of the Fair Information Practice Principles (FIPPs) [6] and the Guidelines on the Protection of Personal Information and Trans-border Flows of Personal Data [7]. Such an index could aid companies in establishing whether consumer's privacy expectations are higher or lower than regulatory requirements and whether consumer's believe that companies are meeting their expectations. This information can be used to define privacy strategies and policies for companies and to ultimately improve the trusting relationship with consumers through the social contract [8].

II. OBJECTIVES

The main objective of this research is to develop a global Online Information Privacy Culture Index (OIPCI), whereby consumers' expectations of how online companies (websites) should deal with their personal information and their confidence

in whether privacy requirements are met by the online companies.

The specific objectives of the research are to:

- Define a conceptual framework, Online Information Privacy Culture Index Framework (OIPCIF). This framework should be mapped to the FIPPs and the OECD privacy guidelines to enable different jurisdictions to implement the framework and align it to their data protection legislation.
- A second objective is to develop a valid and reliable measurement instrument, Online Information Privacy Culture Index Questionnaire (OIPCIQ), based on the framework that can be used to measure the online information privacy culture of a country.
- The third objective is to conduct a survey in a country to start with the data collection to build the global online information privacy culture index. This also allows the researcher to make recommendations for the participating country to address any developmental areas as well as to validate the measuring instrument.

The paper begins by defining the concept of an online information privacy culture and an overview of some consumer perception studies. There after the OIPCIF is presented. This is followed by a discussion of the research methodology and proposed OIPCIQ, which was deployed in South Africa as part of the empirical study. The results of the study is presented followed by the validity and reliability analysis.

III. INFORMATION PRIVACY CULTURE

An information privacy culture is defined as “the perceptions and beliefs a nation (hereafter ‘consumer’) has regarding the processing of citizens’ personal information – what expectations they have and how they believe companies are meeting those expectations given certain information privacy principles (or requirements).[9]. In defining the online information privacy culture the aforementioned definition needs to be extend to the online environment of cyber space which includes the Internet, telecommunication networks, computer systems and embedded processors and controllers [10]. It therefore includes companies with a website presence that collects and processes personal information of potential or existing customers via the internet.

The online information privacy culture can thus be described as the perception and beliefs of consumers regarding the processing of their personal information in cyberspace - what

expectations they have and how they believe online companies are meeting those expectations given certain information privacy principles (or requirements).

IV. EXISTING INFORMATION PRIVACY PERCEPTION SURVEYS

Various surveys have been developed and conducted globally to measure consumers' concerns with regards to online privacy on the internet. An extract of these, ranging from industry surveys to academic surveys, are outlined in table 1.

TABLE I. PRIVACY PERCEPTION SURVEYS

Privacy perception surveys	Focus
Concern for Information Privacy (CFIP) [11]	One factor which focuses on information collection, unauthorised secondary use, improper access and errors.
Expanded CFIP [1]	Extended the CFIP with internet user concerns which address three dimensions, namely collection, control and awareness from a social contract perspective.
Internet User's information privacy concerns [12]	Theoretical framework for internet user's privacy concerns, focussing on collection, control and awareness.
The EMC Privacy Index - Global & in-depth country results [3]	Global survey aimed at measuring consumers' perceptions of online privacy and indicates the willingness of consumers to share private information for the sake of greater convenience.
The Data Protection Eurobarometer [4][13]	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 in Europe.
Symantec's State of Privacy Report [14]	Current perceptions on data privacy across Europe.
Deloitte and Touche's Australian Privacy Index [15]	Privacy index survey of organisational perspectives regarding privacy in a work context in Australia.
TRUSTe/National Cyber Security Alliance - Consumer Privacy Infographic [5]	Consumer Privacy Index focusing on consumer concerns, privacy awareness and business impact in the online context.

While most of the surveys in table 1 focus on consumer privacy in an online context, the constructs are not all based on the FIPPs and OECD privacy principles. These studies do not consider both the expectations and concerns of consumers towards privacy in order to determine a gap. The researcher therefore proposes that both concepts – consumer expectations and confidence levels of whether companies are implementing privacy regulatory requirements – should be considered in an effort to determine the online information privacy culture consumers. Expectations and confidence levels regarding the privacy regulatory requirements 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.

V. THE PROPOSED ONLINE INFORMATION PRIVACY CULTURE INDEX FRAMEWORK (OIPCIF)

The Online Information Privacy Culture Index Framework (OIPCIF) is portrayed in Figure 1. The cornerstone of the framework is the FIPPs [6] and the Guidelines on the Protection of Personal Information and Trans-border Flows of Personal Data [7], which are considered in most countries' data privacy laws [1]. From these, nine *regulatory privacy requirements* were defined. The requirements serve as the constructs in the framework as derived from the aforementioned, namely: accountability (AC), openness (OP), processing (use limitation) (PR), collection limitation (CL), purpose specification (PS), data subject participation (access) (DS), security safeguards (SS) and information quality (IQ). Unsolicited marketing (UM), cross border transfers (CB) and sensitive (special) personal information (SP) were also added as regulatory privacy requirements as these aspects are covered in the General Data Protection Regulation of the European Union (GDPR) [16] and in various other data privacy legislation such as the Protection of Personal Information Act (POPIA) of South Africa [17] and the Data Protection Act (DPA) of the United Kingdom[18]. Together the eleven constructs serve as the baseline or minimum data protection requirements of the conceptual framework.

The *privacy expectations* block, in figure 1, relates to the expectations of consumers about each of the eleven regulatory privacy requirements. While the regulatory requirements must be complied with by companies, consumers might have lower of higher expectations than what is required by the law. These expectations could assist to understand the information privacy culture of the various demographical groups in a country. As pointed out in the research by Hofstede [19], national culture plays a role in the perceptions of people towards privacy for example, Europe is seen as a continent that follows a bureaucratic approach to privacy [20] whereas a more permissive approach is followed by North America [21].

The *privacy confidence* block represents consumers' perception as to whether organizations process personal information in line with the regulatory privacy requirements. This could give an indication as to the perceived level of compliance. However, it does not represent actual compliance or non-compliance with data protection laws as this should be determined through external and internal audits of self-assessments by companies. The objective is to determine the perceptions of consumers as it could influence their level of trust towards companies. This can give insight as to whether online companies need to change their awareness and communication strategies about their privacy policy to build a reputation of compliance as to a perception of non-compliance.

Fig. 1. Online Information Privacy Culture Index Framework (OIPCIF)

A *gap* can be determined if the privacy expectations about each regulatory factor requirement is compared with the perception of consumers' confidence as to whether companies are meeting each regulatory factor requirement. Consumers' expectations might be higher or lower than what they believe companies are currently doing. The identified discrepancies can be used by companies to understand the expectations of their consumers and to address areas where they fail to meet it in order to promote a trusting relationship.

The *privacy concerns* block relates to general concerns of consumers when sharing their information online. These could relate to concerns when sharing different types of personal information and to establish the awareness levels of consumers towards their privacy rights. This information can be used by Regulators to define privacy guidelines for online companies as well as serve as input to awareness campaigns and codes of conduct which Regulators often provide. Online companies can also use this information for their strategies when designing websites used for the collection of personal information of consumers.

The privacy expectations, privacy confidence, gap and privacy concerns together gives an indication of the online information privacy culture and together serve as the *index*. As the regulatory privacy requirements are based on general accepted privacy principles the data protection regulatory requirements of a country can be mapped to the requirements of the proposed framework to allow for comparison of the index between countries.

VI. RESEARCH METHODOLOGY

A. Research method and design

A quantitative research design with a survey research method was utilized in this research [22]. Questionnaires are often used in research where attitudes and opinions of respondents are measured about specific concepts using for example a Likert scale [22], [23]. The targeted population was internet users of South Africa and as such only people who use the internet and websites with access to email were included, hence the selection of a web format for the survey.

B. Research instrument: Online Information Privacy Culture Index Questionnaire (OIPCIQ)

The OIPCIF was used to design the questionnaire statements of the Online Information Privacy Culture Index Questionnaire (OIPCIQ). A panel of five experts provided input to the questionnaire design where after some questions were adapted. Herewith addressing content validity to ensure that the questions adequately cover the subject and are based on literature [23].

The questionnaire was developed with four sections. Section one related to biographical questions such as generation groups, gender, income, language, province, industry, qualification levels and employment status. In section two questions regarding privacy concerns and awareness were asked.

Section three comprised of 22 privacy expectation questions and section four of 22 privacy confidence questions. The privacy expectations section and the privacy confidence sections' questions were paired. Each privacy expectation question were phrased to establish the expectation of consumers about a specific privacy regulatory requirement. The related privacy confidence (paired) question was phrased to establish the level of confidence that consumers have that companies are implementing that specific privacy regulatory requirement. A Likert-style rating scale was used. The privacy expectations question scale was: I do expect this; I sometimes expect this; Neutral; I mostly expect this; I always expect this. The scale used for the privacy confidence questions was: Very confident; Somewhat confident; Neutral; Quite confident and Very confident.

C. Sample

The survey was conducted in South Africa as the first participating country in the study. The questionnaire was sent out electronically to an opt-in database of consumers, which is managed by a research organisation, iFeedback [24]. A total of 512 responses were obtained during 2017. After the data was cleansed and uncompleted questionnaires were removed a total of 356 responses were used in the final data analysis. Two hundred and twenty responses were required to conduct the validity and reliability test of the questionnaire (5-point scale times the number of questions) [25]. SPSS was used for the analysis.

The majority of the respondents were male (61%). Ninety seven percent were employed, with the majority having posts graduate qualifications. Responses were received across 16 industries, mostly in technology and software (15.61%), financial services (13.23%) and industrial (10.85%). Respondents mostly used their laptops to access the internet (50.48%), followed by cellphones (22.84%), desktops (21.88%) and tablets (4.81%). The sample therefore represented mostly employed South Africans with post graduate qualifications. The findings and recommendations are therefore limited to this group. Future research will focus on obtaining a wider, representative sample of the South African population. The data obtained in this research enabled the researcher to validate the questionnaire and to obtain an indication of the privacy culture of the participating sample of online South African consumers.

I. RESULTS

A. Online concerns results

There seems to be more concern about the sharing of personal information over the internet as 81% of consumers were concerned about depositing their personal information on websites in contrast with 65% being concerned about sharing their personal information with companies in everyday business transactions that does not involve the internet. Most consumers (4.59 mean) are concerned about depositing their financial information on websites and personal identification numbers (4.51 mean). Consumers are also concerned about the protection of their personal information when depositing their personal information in websites (4.41. mean). They are especially concerned when websites build online profiles without their consent (4.45 mean) or when their personal information might be sold without their consent (4.31 mean).

Seventy five per cent of the consumers indicated that they know of someone who's personal information has been misused by another person via the internet with 34% who were directly affected. While consumers are concerned about depositing their personal information on websites most indicated that their knowledge of their privacy rights are average (42.3%) or poor (25%).

B. Online privacy expectation results

The highest expectation related to honoring of respondents; choice if they decide not to received direct marketing (4.88). This was followed by the expectation that online companies should protect their personal information when it is sent to other countries (4.85). The third highest expectation related to online companies having the necessary technology and processes in place to protect consumer's personal information. For all the privacy regulatory requirements the mean was above 4.00, except the expectation that websites should keep personal information of consumers' up to date (3.19). This indicates that the participating sample of South Africans have a high expectation for privacy and the protection of their information when they deposit their personal information on websites.

Although POPIA has not commenced as yet, these consumers still have a high expectation of privacy and it is important for online companies to implement measures to process personal information lawfully and to protect it. This will aid in building a trusting relationship with consumers as well as meeting regulatory requirements.

C. Online privacy confidence results

The means for the confidence questions were all below 3.00 with 12 below 2.00, except for the question relating to confidence that online companies are keeping personal information indefinitely (3.05). The aspects in which the consumers have the lowest confidence for online companies are: informing consumers if their personal data were lost, damaged, exposed (1.69), using personal information only for agreed purposes (1.88), notifying consumers before the personal information is collected (1.90), that complaints will be dealt with appropriately (1.92) and that online companies are using personal information in lawful ways. The low means for the confidence of the privacy requirements indicate that this sample of South African consumers have a low confidence level that their privacy rights are honored. This raises the question as to whether online companies (websites) are compliant with the conditions of POPIA and whether privacy rights of consumers are upheld.

D. Gap results

Table 1 outlines the gap for the question pairs in the privacy expectation and privacy confidence constructs of the questionnaire. 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 [26]. This indicates that the consumers have a higher expectation of privacy than what they believe is happening in practice. They have limited confidence that online companies are meeting the privacy regulatory requirements which does not only mean that consumer expectations are not met, but that regulatory requirements might also not be met.

II. VALIDATION OF INSTRUMENT (OIPCIQ)

The OIPCIQ was validated using an exploratory factor analysis (EFA) which was conducted on the items in the expectation and confidence constructs [27]. The data collected was subject to the Bartlett's Test for Sphericity and the Kaiser-Meyer Olkin (KMO) Measure of Sampling Adequacy, to test the aptness of the sample for the EFA [28]. Bartlett's test of sphericity should be significant ($p < 0.05$), to indicate sampling adequacy [29]. In this research study, the Bartlett's test was significant at $p < 0.00$ adding further evidence to sampling validity.

TABLE II. PRIVACY EXPECTATIONS VERSUS PRIVACY CONFIDENCE (MEANS)

Privacy expectation	Mean	Privacy confidence	Mean	Gap
31. I expect online companies (websites) to notify me before they start collecting my personal information.	4.	54. I feel confident that online companies (websites) are notifying me before collecting my personal information.	1.90	2.1
32. I expect online companies (websites) to use my personal information in a lawful manner.	4.82	55. I feel confident that online companies (websites) are using my personal information in lawful ways.	1.94	2.88
33. I expect privacy when an online company (website) has to process my personal information for services or products	4.80	56. I feel confident that online companies (websites) respect my right to privacy when collecting my personal information for services or products	2.02	2.78
34. I expect online companies (websites) not to collect excessive or unnecessary information from me than what is needed for them to offer me a service or product.	4.73	57. I feel confident that online companies (websites) are requesting only relevant and not information other than what is needed for them to offer me a service or product.	2.13	2.6
35. I expect online companies (websites) to only collect my personal information when I have given my consent; or if it is necessary for a legitimate business reason.	4.82	58. I feel confident that online companies (websites) are collecting my personal information only with my consent or for a legitimate business reason.	1.97	2.85
31-42 - 36. I expect online companies (websites) to only collect my personal information from myself and not from other sources.	4.73	59. I feel confident that online companies (websites) are collecting my personal information from legitimate sources.	1.95	2.78
37. I expect online companies (websites) to explicitly define the purpose for which they want to use my information.	4.76	60. I feel confident that online companies (websites) are explicitly defining the purpose they want to use my information for.	1.97	2.79
38. I expect online companies (websites) to only use my personal information for purposes I agreed to and never for other purposes than those agreed by me.	4.81	61. I believe that online companies (websites) are only using my personal information for purposes I agreed to and never for other purposes.	1.88	2.93
39. I expect online companies (websites) to only keep my personal information for as long as required for business purposes or regulatory requirements.	4.65	62. I believe that online companies (websites) are keeping my personal information indefinitely.	3.05	1.6
40. I expect online companies (websites) to obtain my consent if they want to use my personal information for purposes not agreed to with them.	4.84	63. I feel confident that online companies (websites) are obtaining my consent to use my personal information for purposes other than those agreed to with me.	2.07	2.77
41. I expect online companies (websites) to inform me of the conditions for processing my personal information.	4.75	64. I feel confident that online companies (websites) adequately inform me of the conditions.	1.96	2.79
42. I expect online companies (websites) to keep my personal information updated.	3.19	65. I feel confident that online companies (websites) keep my personal information up to date.	2.10	1.09
43. I expect online companies (websites) to protect my personal information.	4.83	66. I feel confident that online companies (websites) are protecting my personal information.	1.94	2.89
44. I expect online companies (websites) to have all the necessary technology and processes in place to protect my personal information.	4.84	67. I feel confident that online companies (websites) have all the necessary technology and processes in place to protect my personal information.	2.13	2.71
45. I expect online companies (websites) to ensure that their third parties (processing my personal information) have all the necessary technology and processes in place to protect my personal information.	4.83	68. I feel confident that online companies (websites) ensure that their third parties have all the necessary technology and processes in place to protect my personal information.	1.96	2.87
46. I expect online companies (websites) to inform me if records of my personal data were lost damaged or exposed publicly.	4.73	69. I feel confident that online companies (websites) inform me if records of my personal data were lost damaged or exposed publicly.	1.69	3.04
47. I expect online companies (websites) to tell me what records of personal information they have about me when I enquire about it.	4.74	70. I feel confident that online companies (websites) can tell me what records or personal information they have about me.	2.10	2.64
48. I expect online companies (websites) to correct or delete my personal information at my request.	4.79	71. I feel confident that online companies (websites) will correct or delete my personal information at my request.	2.08	2.71
49. I expect online companies (websites) not to collect sensitive personal information about me.	4.70	72. I feel confident that online companies (websites) only collect sensitive personal information about me with my explicit consent.	2.03	2.67
50. I expect online companies (websites) to honour my choice if I decide not to receive direct marketing.	4.94	73. I feel confident that online companies (websites) honour my choice if I do not want to receive direct marketing.	2.04	2.9
51. I expect online companies (websites) to give me a choice if I want to receive direct marketing from them.	4.82	74. Online companies (websites) always give me a choice to indicate if I want to receive direct marketing from them.	2.36	2.46
52. I expect online companies (websites) to protect my information when they have to send it to other countries.	4.85	75. I feel confident that online companies (websites) protect my information if they have to send it to other countries.	1.94	2.91

Two factors (A and B), see table 3, were identified for the *expectations construct*. According to Kaiser [28], the KMO should be 0.60 or higher and the cumulative percentage explained by the factors should be higher than 60% in order to proceed with factor analysis. The KMO for factor A and B was 0.924. A total of four Eigenvalues were larger than 1, thus suggesting that three factors may be extracted [30]. Horne's [31] parallel analysis, on the other hand, suggested that two factors may be appropriate. A two, three, and four factor solution was explored. It was found that almost no items loaded on a third and a fourth factor, and therefore a two factor solution was adopted although the cumulative percentage was 51% for

the two factors. All item loadings in the expectations construct were above 0.4, except items 47 and 49, which were marginally lower. Based on the theoretical model and the small change in the Cronbach alpha, should the items be deleted, the items, were retained. The loading of item 42 was much lower and was therefore not included. Most of the loadings of the items in factor A and B were between 0.60 and 0.80.

Two factors (C and D) were also identified in the *confidence construct* with KMO value of .969 and a total cumulative percentage of 65.89% for the two factors. A total of three Eigenvalues were larger than 1, thus suggesting that three

factors may be extracted [28]. Horne's parallel analysis, suggested that two factors may be appropriate. Both a two- and three factor solution was explored. It was found that almost no items loaded on a third factor, and therefore a two factor solution was adopted. The loading of the individual items were all above 0.60. The Cronbach alpha for the identified factors were all above 0.8, indicating a good reliability.

TABLE III. ONLINE INFORMATION PRIVACY CULTURE INDEX QUESTIONNAIRE – NEW FACTORS

Factors	Questions	Cronbach alpha
Factor A: Expectations for respect of personal information/privacy	31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 47, 49, 52	0.931
Factor B: Expectations for use and protection of personal information	43, 44, 45, 46, 48, 50, 51	0.846
Factor C: Confidence in respect for personal information/privacy	54, 55, 56, 57, 58, 59, 60, 61, 63, 64, 65	0.956
Factor D: Confidence in use and protection of personal information	66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77	0.955

III. CONCLUSION

This research proposes an Online Information Privacy Culture Index Framework (OIPCIF) and related instrument. The Online Information Privacy Culture Index Questionnaire (OIPCIQ) was developed based on the international privacy guidelines to measure the online privacy expectations of consumers, their confidence in whether online companies are meeting regulatory requirements and to identify a gap between the expectations and beliefs of what companies are doing in practice. The questionnaire was deployed in South Africa and the data used to validate the instrument. The validated OIPCIQ, with the four new factors, can be used in other countries to build a global index of privacy culture that can serve as input to define organisational, government and regulator strategies and policies for privacy. Future research will focus on extending the South African sample that participated, comparing biographical groups and to validate the conceptual framework with Structural Equation Modelling (SEM).

ACKNOWLEDGMENT

This research is wholly supported by the Women in Research (WiR) Grant from UNISA.

REFERENCES

- [1] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *Inf. Soc.*, vol. 20, no. 5, pp. 313–324, 2004.
- [2] P. Kumaraguru and L. F. Cranor, "Privacy Indexes : A Survey of Westin's Studies," no. December, pp. 1–22, 2005.
- [3] EMC Corporation, "The EMC Privacy Index - Global & in-depth country results," 2014. [Online]. Available: <https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf>. [Accessed: 17-Nov-2017].
- [4] European Commission, "Flash Eurobarometer 443: Report e-Privacy," 2016. [Online]. Available: <http://bookshop.europa.eu/en/the-euro-area-pbKC0215874/?CatalogCategoryID=iEKep21x3hEAAAEud3kBgSLq>. [Accessed: 17-Nov-2017].
- [5] Trust. N.C.S. Alliance, "TRUSTe/NCSA Consumer Privacy Infographic – US Edition," 2016. [Online]. Available: <https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/>.
- [6] "Fair Information Practice Principles (FIPPS)," *IT Law Wikia*, 2017.
- [7] OECD, "OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data," *The OECD Privacy Framework*, 2013. [Online]. Available: <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. [Accessed: 17-Nov-2017].
- [8] J. Phelps, G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information," *J. Public Policy Mark.*, no. 19, p. 1, 2000.
- [9] A. Da Veiga, "An Information Privacy Culture Index Framework and Instrument to measure privacy perceptions across nations: Results of an empirical study," in *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 2017.
- [10] "Joint Staff US Army, Cyberspace Operations. The Defense Technical Information Center," 2013. [Online]. Available: www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. [Accessed: 17-Nov-2017].
- [11] J.H Smith, S. . Milberg, and S. . Burke, "Information Privacy: Measuring Individual's Concerns about Organisational Practice," *MIS Q.*, vol. June, pp. 167–195, 1995.
- [12] N. K. Malhotra, S. S. Kim, J. Agarwal, G. Tech, W. Peachtree, and S. S. Kim, "Internet Users Information Privacy Concerns (UIPC): The construct, the scale and a casual model," vol. 15, no. 4, pp. 336–355, 2014.
- [13] European Union, "Special Eurobarometer 431 - Data protection," *Data protection*, 2015. [Online]. Available: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf. [Accessed: 17-Nov-2017].
- [14] Symantec, "State of privacy report 2015," 2015. [Online]. Available: <https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>.
- [15] Deloitte and Touche Australia, "Deloitte Australian Privacy Index 2017," 2017. [Online]. Available: <file:///C:/Users/dveiga/Downloads/deloitte-au-risk-deloitte-australian-privacy-index-2017-300517.pdf>.
- [16] The European Parliament and the Council of the European Union, "General Data Protection Regulation," *Off. J. Eur. Union*, pp. 1–88, 2016.
- [17] The Parliament of the Republic of South Africa, *Protection of Personal Information Act (PoPIA) 4 of 2013*, no. 32495. Cape Town, 2013, pp. 1–50.
- [18] National Archives, "Data Protection Act 1998," pp. 1–92, 1998.
- [19] G. Hofstede, G. J. Hofstede, and M. Minkov, *Cultures and Organizations: Software of the mind*, Third. US: The McGraw-Hill Companies, 2010.
- [20] G. Greenleaf, "Sheherezade and the 101 data privacy laws: Origins , significance and global trajectories," *UNSW Law Res. Pap. No. 2013*, vol. 40, no. September, p. 29, 2013.
- [21] L. Bygrave, "Privacy and data protection in an international perspective," *Scand. Stud. Law*, 2010.
- [22] J. W. Cresswell, *Research design - Qualitative, quantitative, and mixed methods approaches*, Fourth ed. Los Angeles: SAGE Publications, 2014.
- [23] M. Saunders, P. Lewis, and A. Thornhill, *Research methods for business students*, Seventh ed. England: Pearson Education Limited, 2016.
- [24] "iFeedback." [Online]. Available: <http://ifedback.co.za/>. [Accessed: 11-Nov-2017].
- [25] N. O'Rourke and L. Hatcher, *A step-by-step approach to using SAS for factor analysis and structural equation modeling*. 2013.
- [26] D. C. Howell, *Fundamental statistics for the behavioural sciences*, Third. California: International Thomson Publishing, 1995.
- [27] J. W. Osborne and A. B. Costello, "Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis," *Pan-Pacific Manag. Rev.*, vol. 12, no. 2, pp. 131–146, 2009.
- [28] H. F. Kaiser and J. Rice, "Little jiffy, mark IV," *Educ. Psychol. Meas.*, vol. 34, no. 1, pp. 111–117, 1974.
- [29] J. E. Bartlett, W. J. Kotrlik, and C. C. Higgins, "Organizational research: Determining appropriate sample size in survey research," *Inf. Technol. Learn. Perform. J.*, vol. 19, no. 1, p. 43.
- [30] J. F. Hair, R. E. Anderson, B. J. Babin, and W. C. Black, *Multivariate data analysis: A global perspective (Vol. 7)*. Upper Saddle River, NJ: Pearson, 2010.
- [31] J. L. Horne, "A rationale and test for the number of factors in factor analysis," *Psychometrika*, vol. 30, 1965.