Concern for information privacy: a cross-nation study of the United Kingdom and South Africa

Adéle Da Veiga
Jacques Ophoff

This is the Author Accepted Manuscript of a conference paper published in Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings

The final publication is available at Springer via DOI: http://dx.doi.org/10.1007/978-3-030-57404-8_2

Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa

Adéle da Veiga[1][0000-0001-9777-8721] and Jacques Ophoff[2,3][0000-0003-0634-5248]

[1] School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
dveiga@unisa.ac.za
[2] University of Cape Town, Cape Town, South Africa
[3] Division of Cyber Security, School of Design and Informatics, Abertay University, Dundee, Scotland
j.ophoff@abertay.ac.uk

Abstract. Individuals have differing levels of information privacy concern, formed by their expectations and the confidence they have that organisations meet this in practice. Variance in privacy laws and national factors may also play a role. This study analyses individuals' information privacy expectation and confidence across two nations, the United Kingdom and South Africa, through a survey of 1463 respondents. The findings indicate that the expectation for privacy in both countries are very high. However, numerous significant differences exist between expectations and confidence when examining privacy principles. The overall results for both countries show that there is a gap in terms of the privacy expectations of respondents compared to the confidence they have in whether organisations are meeting their expectations. Governments, regulators, and organisations with an online presence need to consider individuals' expectations and ensure that controls that meet regulatory requirements, as well as expectations, are in place.

Keywords: Information Privacy, Concern, Expectation, South Africa, United Kingdom.

1 Introduction

A data subject's (i.e. individual, consumer, citizen) concern for information privacy is an important topic receiving a lot of attention [1–5]. From an organisational perspective, data protection law research examines compliance and issues related to data breaches [6–11]. Consumer expectations, together with whether organisations are indeed meeting such expectations in line with regulatory requirements, is a topic receiving increasing attention. This addresses concern for information privacy [12–14], but also the enhancement of digital trust and organisational compliance [15].

Privacy expectations could vary across groups of citizens based on their demographic profile (such as gender, age, nationality) or varying factors such as culture or

recent data breaches that occurred in a country [16]. Some studies show that privacy expectations are lower in the United States, compared to Europe and the United Kingdom, and that women are more concerned about privacy than men [17]. Surveys also show that individuals in the same data protection jurisdiction could have different perceptions and expectations towards their personal information. For example, citizens from Germany and the United Kingdom are more concerned about their personal information than the French [16]. Consumers indicate that they are becoming more concerned about the manner in which organisations are using personal information and are less likely to trust organisations with it [18]. Various studies have focused on concern for information privacy [4, 19–21], but do not necessarily consider individuals' privacy expectations and confidence in whether organisations are meeting such expectations.

This study aims to holistically measure individuals' concern for information privacy by considering their expectations and, in addition, whether they have experienced that organisations do indeed meet their expectations in practice. It aims to answer the following primary research question: How do individual privacy expectations and confidence in organizational practices align? It also considers whether differences could exist between nations. The study was conducted across two nations, the United Kingdom (UK) and South Africa (SA), providing data for comparative purposes. While there is a concern of consumers toward the use of personal information by government and invasion of their privacy from that perspective [25], it was excluded from the scope of this study.

The remainder of this paper proceeds as follows. Section 2 provides an overview of relevant privacy literature and Section 3 briefly examines privacy legislation in the target countries. Section 4 reviews the research methodology, followed by results and a discussion of the findings in Section 5. Finally, this paper concludes by discussing opportunities for future research.

2 Concern for Information Privacy

Concern for information privacy relates to individuals who have certain concerns about the practices used by responsible parties when processing their personal information [22]. While individuals could have certain privacy expectations there could be risk and potential negative consequences when organisations process their personal information, resulting in concern for their information privacy [4]. Westin developed several surveys to measure concern for information privacy from perspectives such as computer fear, medical, and consumer concerns. He proposed the Concern for Information Privacy (CFIP) Index which is measured using a survey questionnaire. With the growth of the world wide web the Internet Users Information Privacy Concern (IUIPC) survey was developed [23]. The IUIPC or the CFIP of Stewart et al. [24], Smith et al. [22] and Westin [25] were further used in various studies to investigate

concern for information privacy. Examples include the work of Heales et al. [20] who integrated global cultural dimensions and investigated the influence of national culture. Fodor and Brem [26] applied the CFIP and IUIPC to study the privacy concerns of millennials in Germany. Similarly, Tanantuputra et al. [27] applied the CFIP of Smith et al. [22] and tested the influence of demographic factors, self-efficacy, computer anxiety, and internet literacy in Malaysia.

The Online Information Privacy Culture Index (OIPCI) [12, 29] was developed to measure consumers' information privacy expectations and whether they experience that online organisations do indeed meet these expectations. This validated instrument was used in this study for data collection and the comparative analysis between SA and the UK.

3 Privacy Regulation

Regulating privacy through laws is a necessity to address information privacy concern of data subjects [2]. Studies show that effective enforcement of privacy laws could decrease concern for information privacy in an online context, but when data subjects perceive that the governance of privacy regulation is weak they have greater privacy concern [2]. Wu et al. [30] argue that while one needs to understand individuals' privacy needs one should also address regulatory requirements. The challenge is that each jurisdiction has its own privacy laws, which are regulated differently. In a global environment online users could be based, and their information processed, across jurisdictions making it a challenge for organisations (website owners) to comply with privacy regulations in each jurisdiction. Wu et al. [30] argues that privacy governance can aid in developing practices and policies meeting higher privacy standards across borders, however organisations could move operations to jurisdictions with no or limited regulations. While this perspective focusses on the implementation of best practices where policies meet higher privacy standards, it cannot be done in isolation of consumer expectations. A consideration is therefore that organisations should understand the privacy expectations of their customers in line with generally accepted privacy principles. They should also map this to legal requirements of the respective jurisdictions they operate in. Where a customer base is in a predominant jurisdiction the generally accepted privacy principles can be mapped to the applicable privacy laws to ensure that legal requirements are complied with whilst meeting customer expectations. From this perspective UK and SA privacy legislation is considered next.

3.1 Privacy Legislation in the UK

Through the Data Protection Act (DPA) 1984 [31] the UK implemented one of world's first measures to protect people's personal information. It was underpinned

by fundamental privacy principles and introduced criminal offences for failure to comply [32]. The DPA has since been revised and in its current format, the Data Protection Act 2018, is closely aligned with the EU General Data Protection Regulation (GDPR). It has modernised data protection laws in the UK to be relevant in an online world.

While the DPA empowers citizens to take control of their data it also provides support to organisations to implement required operational changes. The Act is structured into seven parts and includes 20 schedules. In particular, Part 2 (Chapter 1 and 2) supplements GDPR by completing specific member state interpretations and implementations; this includes reference to lawfulness of processing, special categories of personal data, rights (as well as restrictions of rights) of the data subject, accreditation of certification providers, transfers of personal data to third countries, and specific processing situations. Part 5 confirms the Information Commissioner's Office (ICO) as the UK's supervisory authority. Since 2018 enforcement actions include monetary penalties, enforcement notices, prosecutions, and undertakings [33].

Industry reports indicate that the majority (57%) of UK consumers are concerned about the amount of personal data they have shared online. While consumers are concerned about data sharing many (63%) know little or nothing about their rights or legislation such as GDPR [34]. However, indications are that these are declining numbers and that consumers are becoming 'data pragmatists' who are willing to share personal information for clear rewards [35]. Contradictions between the UK public's perception of online privacy and behaviour is not unusual and this phenomenon has been widely studied in different contexts (e.g. Kokolakis [36]). An examination of the privacy paradox among consumers across four UK cities postulates that insufficient education, apathy, and underestimating risks could still be relevant in this context [37].

From an organisational perspective the introduction of GDPR has forced UK organisations to inspect their data processing practices. Research shows that many UK organisations may not be fully aware of the changes in data protection, also at the executive level [38]. This could have significant implications, considering that Section 198 of the DPA includes liability of directors. Another challenge is interpreting the 'regulation's qualitative statements' or accessing external support to do so. This issue can be acute in resource-constrained organisations, such as SMEs [39]. In an effort to support data protection the ICO has published an extensive set of organisational guidelines, specifically aimed at SMEs, that cover the DPA and GDPR as it applies in the UK [40].

3.2 Privacy Legislation in SA

South Africa has lagged in implementing comprehensive privacy legislation. While privacy is addressed to some extent in legal frameworks (e.g. section 14 of the Constitution of the Republic of South Africa (1996) [41] stipulates that all citizens have the right to privacy) the online processing of personal information has been a concerning gap. In this regard legislators have enacted the Protection of Personal Information Act (POPIA) [42] to promote the protection of individuals' data processed by organisa-

tions. POPIA incorporates some of the most effective elements from global privacy laws and parallels can be drawn with the EU's approach in implementing the GDPR [43].

The POPIA regulates the processing of personally identifiable information by public and private bodies, aligning with international standards. While exceptions and special cases to conditions exist (e.g. processing after obtaining consent from a data subject) the POPIA is a comprehensive privacy legislation. With the appointment of an information regulator in December 2016 the Act has moved one step closer to implementation. In line with global trends to establish a data protection authority [6] the information regulator will handle data subject complaints, investigations, and impose penalties.

The POPIA presents a positive step for the protection of personal information and should be welcomed by consumers. Prior research has shown that South African citizens have high privacy expectations regarding organisations processing personal information [44]. However, organisational compliance will take significant effort, unless an organisation is already compliant with similar international laws. A particular concern for organisations is how the law will be interpreted (since it is based on privacy principles) by the information regulator, and how penalties will be imposed. Practical difficulties could include change management, adapting employee culture, and implementing new security technologies [45]. It is also recognised that POPIA will impact data management professionals in particular, with several steps necessary to move towards legislative compliance [46].

4 Research Methodology

A quantitative research approach, using a survey, was followed to measure the concern for information privacy in the UK and SA. Quantitative methods are frequently questionnaire-based, which works well for descriptive research where attitude and opinion data are collected and statistically analysed to draw general conclusions [47, 48]. While qualitative methods could give more in-depth insight it was not included in the scope of this study.

4.1 Instrument and Data Collection

As instrument the Online Information Privacy Culture Index (OIPCI) was used. This questionnaire consists of four sections, starting with questions about biographical data and concern for information privacy. The next sections include expectation and confidence items based on 11 components which map to the FIPPS privacy principles, conditions in the DPA (UK), and the principles in POPIA (SA). All measures use a 5-point scale. The expectation items aim to identify whether the consumer has a high or low expectation of a specific privacy principle. The confidence questions measure whether the consumer perceives that organisations indeed conform in practice to meet the respective privacy principle.

An online research platform, Prolific [49], was used to distribute the survey to a representative sample in the UK. The survey was distributed electronically by InSites Consulting [50], a market research company, to consumers in SA. Ethical clearance was obtained prior to data collection to validate that the survey complied with research principles such as being voluntary, anonymous, and that consent was obtained to use the data for research publications.

4.2 Sample

A total of 456 responses were collected in the UK, and 1007 in SA according to the demographic profile of the country (total responses was 1463). The majority of the UK sample were female (69.96%) whereas the SA sample was relatively balanced (51.9% male). The SA participants represented the demographic profile of SA with two thirds being African (black) and in the UK two thirds of the respondents indicated that they were English, as illustrated in Table 1.

Table 1. Responses per SA and UK demographic profile

South Africa		**United Kingdom**	
Demographic	**Percent**	**Demographic**	**Percent**
African	63.8%	English	63.7%
Coloured	11.3%	Welsh	3.2%
Indian	4.9%	Scottish	6.2%
Asian	0.2%	Northern Irish	1.7%
White	19.9%	British	8.5%
		Other	14.1%
		Missing	2.6%

The majority of the respondents use their mobile phone (58% SA; 59% UK), followed by a laptop (22% SA; 23% UK), desktop (12%) and tablet (8% SA; 7% UK) to access the Internet. Individuals in both countries mostly go online for purposes such as browsing, e-mail, social media, and banking. Respondents indicated that the scenarios in which they provide their personal information to websites are mostly when purchasing a product or for social media purposes.

5 Results

The SA respondents indicated that they obtain privacy information from the Internet/websites (71%), banks (40%), and organisations to whom they provide their information (29%). Similarly, the UK respondents indicated that they obtain privacy information from the Internet/websites (26.3%), the organisation where they work (10.2%), the government (9.6%), organisations to whom they provide their infor-

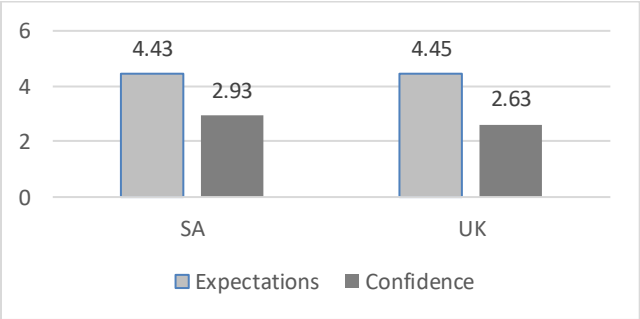
mation (9.6%), and banks (9.4%). Respondents indicated that the preferred places to obtain privacy information were the Internet/websites, banks, government, organisation to whom they provide their personal information, and organisation they work for.

5.1 Expectation versus Confidence Means

The expectation for privacy in both countries was very high, with the UK being slightly higher (mean of 4.45) than SA (4.43). This shows that consumers expect privacy when sharing their personal information on websites. This could be expected in the UK where data protection laws have been in place for a long time. However, while POPIA has not yet commenced, online users in SA still have a high expectation of privacy.

The difference in expectation versus confidence is illustrated in Fig. 1. The results for both countries show that there is a gap in terms of respondents' privacy expectation compared to the confidence they have in whether organisations are meeting this. The UK respondents were more negative (2.63) compared to the SA respondents (2.93) in terms of their confidence in whether online companies are indeed meeting the regulatory requirements and their expectation for privacy. Correspondingly, the gap between the means for expectation versus confidence questions is higher for the UK (1.82) than SA (1.5).

Fig. 1. Expectation and Confidence Means: SA and UK



While the DPA has been in place since 1995, UK respondents were less confident that online companies are preserving their privacy. If consumers feel that organisations are not meeting their privacy expectations it indicates that organisations might not meet regulatory requirements as the expectations are in line with the POPIA and DPA requirements.

5.2 Expectations and Confidence regarding Privacy Principles

The majority of expectation response means for both the UK and SA were above 4.00. Only two statements with the lower means were recorded. The first was the expectation to keep personal information updated, which was higher for SA (3.67 mean, 61% expected this) than the UK (3.32 mean, 42.9% expected this). The second related to whether respondents know where to submit a complaint if they believed an online company did not protect their personal data. More people in SA (3.29, 47.5% agreed) believed they know where to submit a complaint compared to the UK (2.66 mean, 27.8% agreed).

The statement with the highest mean for SA respondents related to the expectation that online companies should only use personal information for the purposes agreed with the data subject and never for other purposes (4.64 mean, 92.2% expected this). Secondly, to use personal information in a lawful manner (4.62 mean, 91.4% expected this). Thirdly, the expectation that online companies should have all the necessary technology and processes in place to protect personal information (4.61 mean, 91% expected this) as well as to protect it when sending it to other countries (4.61 mean, 92.7% expected this). In the UK the expectation statement that had the highest mean was to correct or delete personal information upon request (4.73 mean, 91% expected this). Secondly, to honour the choice if one decides not to receive direct marketing (4.72 mean, 90.4% expected this). Thirdly, to inform the data subject if personal information was lost, damaged, or exposed publicly (4.7 mean, 89.1% expected this).

UK respondents were more negative in terms of whether online companies are meeting privacy requirements and expectations in practice (four statements with a mean below 2.5). They were most negative about whether online companies are only using their personal information for purposes they agreed (2.27 mean, 17.5% were confident). Secondly, they indicated that they are not confident that online companies are ensuring that third-party's have all the necessary technology and processes in place to protect their personal information (2.37 mean, 22.4% were confident). Thirdly, they were not confident that online companies were using their personal information in lawful ways (2.48 means, 23.7% were confident), nor collecting it with their consent (2.49 mean, 25% were confident). The lowest means in the SA data related to the confidence that online companies are informing one if personal information was lost, damaged, or exposed publicly (2.75 mean, 35% expected this). Secondly, respondents were less confident that online companies protect their information when sending it to other countries (2.81 mean, 34% were confident). Thirdly, that personal information is only used for purposes data subjects agreed to (2.84 mean, 36% were confident).

5.3 Significant Country Differences

Table 2 in Appendix A portrays the means of the items for the SA and UK data. The last column indicates the difference in means, in descending order of difference. A positive number indicates that the SA mean was higher. A negative number indicates

the UK mean was higher. There were 30 items with a significant difference (indicated with "*") based on Levine's test of significance. The Sig. (2-tailed) value was 0.000 for all the question pairs (significant if $p<0.05$) and was supported by the t-values.

The SA respondents were significantly more positive than the UK respondents for 22 of the confidence statements. This indicates that, compared to the UK, SA respondents are more confident that online companies are implementing data privacy requirements and thereby meeting their privacy expectations. A reason could be that UK respondents are more aware of the regulatory requirements, having had data privacy law in place for a long time as well as an active regulator issuing fines. In SA POPIA has not yet commenced which could result in less awareness amongst consumers regarding compliance with the law. However, it could also relate to a difference in national culture or compliance of organisations. This aspect requires further investigation for influencing factors and additional data collection once POPIA has commenced.

Respondents from both countries were negative in terms of whether online companies (websites) take their responsibility to protect individuals' personal information seriously, with the UK (2.77 mean, 31.85 were confident) respondents being significantly more negative compared to the SA respondents (2.98 mean, 39% were confident). It should be noted that in the case of both countries none of the confidence-expectation item pair means correspond, indicating a gap in terms of what online users expect and how they experience their information being used in practice. Of importance is that there are statistically significant (based on the t-tests conducted) differences for all paired items in the SA and UK data. Thus, respondents from both countries have a high expectation for privacy, but are significantly less confident that online companies meet this in practice. This emphasises the concern for privacy from an expectation and compliance perspective for both countries.

6 Conclusion

This study aimed to measure individuals' concern for information privacy by considering their expectations and perceptions whether organisations do indeed meet expectations in practice. The study was conducted in two countries, the UK and SA, providing data for comparative purposes. The expectation for privacy in both countries are very high. The overall results for both countries show that there is a gap in terms of the privacy expectations of respondents compared to the confidence they have in whether organisations are meeting their expectations. The UK respondents are more concerned that online companies are not meeting expectations, which also indicates that regulatory requirements might not be met. Governments, regulators, and organisations with an online presence need to consider the expectations of individuals and ensure that controls for privacy expectations and regulatory requirements for data privacy are in place.

The results highlight the transdisciplinary nature of information privacy and that it is important to consider synergies between individual and organisational research [51].

As POPIA is not yet implemented in SA the study can be repeated in future to identify whether concern for information privacy changes once legislation is in place. Further work should also focus on the concern for information privacy between biographical groups and to expand the data collection to qualitative methods.

Acknowledgements

Women in Research Grant of UNISA and NRF Incentive Funding for Rated Researchers grant number: 103965

References

1. Degirmenci K (2020) Mobile users' information privacy concerns and the role of app permission requests. Int J Inf Manage 50:261–272. doi:10.1016/j.ijinfomgt.2019.05.010
2. Anic ID, Škare V, Kursan Milaković I (2019) The determinants and effects of online privacy concerns in the context of e-commerce. Electron Commer Res Appl 36:. doi:10.1016/j.elerap.2019.100868
3. Wang Y, Herrando C (2019) Does privacy assurance on social commerce sites matter to millennials? Int J Inf Manage 44:164–177. doi:10.1016/j.ijinfomgt.2018.10.016
4. Yun H, Lee G, Kim DJ (2019) A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. Inf Manag 56:570–601. doi:10.1016/j.im.2018.10.001
5. Kaushik K, Kumar Jain N, Kumar Singh A (2018) Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. Electron Commer Res Appl 32:57–68. doi:10.1016/j.elerap.2018.11.003
6. Greenleaf G, Systems I (2019) Global data privacy laws 2019: 132 national laws & many bills
7. Custers B, Dechesne F, Sears AM, et al (2018) A comparison of data protection legislation and policies across the EU. Comput Law Secur Rev 34:234–243. doi:10.1016/j.clsr.2017.09.001
8. Chua HN, Herbland A, Wong SF, Chang Y (2017) Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telemat Informatics 34:157–170. doi:10.1016/j.tele.2017.01.008
9. Politou E, Michota A, Alepis E, et al (2018) Backups and the right to be forgotten in the GDPR : An uneasy relationship. Comput Law Secur Rev 34:1247–1257. doi:10.1016/j.clsr.2018.08.006
10. Tosoni L (2018) Rethinking Privacy in the Council of Europe ' s Convention on Cybercrime. Comput Law Secur Rev 34:1197–1214. doi:10.1016/j.clsr.2018.08.004
11. Liginlal D, Sim I, Khansa L, Fearn P (2011) HIPAA Privacy Rule compliance : An interpretive study using Norman ' s action theory 5. Comput Secur 31:206–220. doi:10.1016/j.cose.2011.12.002
12. Da Veiga A (2018) An information privacy culture instrument to measure

consumer privacy expectations and confidence. Inf Comput Secur 26:338–364. doi:10.1108/ICS-03-2018-0036
13. Da Veiga A (2017) An Information Privacy Culture Index Framework and Instrument to measure privacy perceptions across nations: Results of an empirical study. In: Furnell S, Clark N (eds) Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA). Plymouth University, Adelaide
14. Da Veiga A (2018) An online information privacy culture. In: Conference on Information Communications Technology and Society (ICTAS). IEEE, Durban, South Africa, pp 1–6
15. Abraham C, Sims RR, Daultrey S, Buff A (2019) How Digital Trust Drives Culture Change
16. RSA (2019) RSA DATA PRIVACY & SECURITY SURVEY 2019 :
17. Baruh L, Secinti E, Cemalcilar Z (2017) Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. J Commun. doi:10.1111/jcom.12276
18. Sherman E (2019) People are concerned about their privacy in theory, not practice, says new study. Fortune
19. Bellman S, Johnson EJ, Kobrin SJ, Lohse GL (2004) International Differences in Information Privacy Concerns: A Global Survey of Consumers. Inf Soc 20:313–324. doi:10.1080/01972240490507956
20. Heales J, Cockcroft S, Trieu VH (2017) The influence of privacy, trust, and national culture on internet transactions. In: Meiselwitz G (ed) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer International Publishing, pp 159–176
21. J.H Smith, Milberg S., Burke S. (1995) Information Privacy: Measuring Individual's Concerns about Organisational Practice. MIS Q June:167–195
22. Smith HJ, Milberg SJ, Burke SJ (1996) Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Q 20:167. doi:10.2307/249477
23. Malhotra NK, Kim SS, Agarwal J (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scal. Inf Syst Res 15:336–355
24. Stewart KA, Segars AH (2002) Examination empirical for information privacy of the concern instrument. Inf Syst Res 13:36–49
25. Kumaraguru P, Cranor LF (2005) Privacy indexes: A survey of Westin's studies. Carnegie Mellon Univ CMU-ISRI-5:
26. Fodor M, Brem A (2015) Computers in Human Behavior Do privacy concerns matter for Millennials ? Results from an empirical analysis of Location-Based Services adoption in Germany. Comput Human Behav 53:344–353. doi:10.1016/j.chb.2015.06.048
27. Tanantaputra J, Chong CW, Rahman MS (2017) Influence of individual factors on concern for information privacy (CFIP), a perspective from Malaysian higher educational students. Libr Rev 66:182–200. doi:10.1108/LR-05-2016-0043
28. Esmaeilzadeh P (2019) The Effects of Public Concern for Information Privacy on the Adoption of Health Information Exchanges (HIEs) by Healthcare Entities. Health Commun 34:1202–1211. doi:10.1080/10410236.2018.1471336
29. Da Veiga A (2017) An Information Privacy Culture Index Framework and

Instrument to Measure Privacy Perceptions across Nations: Results of an Empirical Study. In: Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA). Plymouth University, Adelaide, Australia, pp 196–209
30. Wu PF, Vitak J, Zimmer MT (2019) A contextual approach to information privacy research. J Assoc Inf Sci Technol 00:1–6. doi:10.1002/asi.24232
31. Data Protection Act 2018. United Kingdowm
32. Carey P (2018) Data Protection: A Practical Guide to UK and EU law, 5th ed. Oxford University Press, United Kingdom
33. Information Commissioner Office (ICO) Information Commissioner Office. In: Inf. Comm. Off. https://ico.org.uk/action-weve-taken/enforcement/
34. Ashford W (2018) Most Britons concerned about personal data sharing. https://www.computerweekly.com/news/252436267/Most-Britons-concerned-about-personal-data-sharing
35. Association D& M Data & Marketing Association. In: Data Priv. What Consum. really thinks. https://dma.org.uk/research/data-privacy-what-the-consumer-really-thinks-1
36. Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput Secur 64:122–134. doi:10.1016/j.cose.2015.07.002
37. Williams M, Nurse JRC (2016) Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective. In: Tryfonas T (ed) Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, pp 186–197
38. Addis M, Kutar M (2018) The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. In: Implementation and Readiness. UK Academy for Information Systems Conference Proceedings
39. Sirur S, Nurse JR., Webb H (2018) Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In: Proceedings of the 2nd International Workshop on Multimedia Privacy and Secu-rity. pp 88–95
40. Guide to data protection. https://ico.org.uk/for-organisations/guide-to-data-protection/)
41. South African Government (1996) Constitution of the Republic of South Africa
42. The Parliament of the Republic of South Africa (2013) Protection of Personal Information Act (PoPIA) 4 of 2013. Cape Town
43. De Bruyn M (2014) The Protection Of Personal Information (POPI) Act - Impact on South Africa. Int Bus Econ Res J 13:1315–1340
44. Da Veiga A (2018) An information privacy culture instrument to measure consumer privacy expectations and confidence. Inf Comput Secur 26:339–364
45. Pelteret, M., Ophoff, J.: Organizational Information Privacy Strategy and the Impact of the PoPI Act. In: 2017 Information Security for South Africa (ISSA). pp. 56–65 (2017). https://doi.org/10.1109/ISSA.2017.8251775.
46. Kandeh AT, Botha RA, Futcher LA (2018) Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. South African J Inf Manag 20:1–9. doi:10.4102/sajim.v20i1.917
47. Cresswell JW (2014) Research design - Qualitative, quantitative, and mixed

methods approaches, Fourth edi. SAGE Publications, Los Angeles
48. Saunders M, Lewis P, Thornhill A (2016) Research methods for business students, seventh ed. Pearson Education Limited, England
49. Prolific. https://www.prolific.co/
50. InSites Consulting South Africa. In: InSites Consult. https://insites-consulting.com/. Accessed 5 May 2020
51. Pelteret, M., Ophoff, J.: A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science: The International Journal of an Emerging Transdiscipline. 19, 277–301 (2016).

7 Appendix A

Table 2. Means and Significant Differences (items from [14])

Items - Experience	SA	UK	Diff.
I know where to submit a complaint if I believe an online company (website) did not protect my personal information.*	3.29	2.66	0.63
I expect online companies (websites): …to keep my personal information updated.*	3.67	3.32	0.35
…to explicitly define the purpose for which they want to use my information.	4.59	4.51	0.08
…to inform me of the conditions for processing my personal information.	4.56	4.49	0.07
…to notify me before they start collecting my personal information.*	4.48	4.43	0.05
…to only use my personal information for purposes I agreed to and never for other purposes.	4.64	4.61	0.03
…not to collect sensitive personal information about me.	4.31	4.3	0.01
…to obtain my consent if they want to use my personal information for purposes not agreed to with them.	4.59	4.62	-0.03
…I expect privacy when an online company (website) has to processes my personal information for services or products.	4.59	4.63	-0.04
…to only collect my personal information when I have given my consent; or if it is necessary for a legitimate business reason.	4.58	4.62	-0.04
…to only collect my personal information from myself and not from other sources.	4.49	4.53	-0.04
…to use my personal information in a lawful manner.	4.62	4.67	-0.05
…to have all the necessary technology and processes in place to protect my personal information.	4.61	4.66	-0.05
…to ensure that their third parties (processing my personal information) have all the necessary technology and processes in place to protect my personal information.	4.51	4.56	-0.05
…to protect my information when they have to send it to other countries.	4.61	4.67	-0.06
…to protect my personal information.*	4.56	4.65	-0.09
…to inform me if records of my personal data were lost, damaged or	4.59	4.7	-0.11

exposed publicly.			
…to give me a choice if I want to receive direct marketing from them.*	4.51	4.63	-0.12
…to honour my choice if I decide not to receive direct marketing.*	4.58	4.72	-0.14
…to correct or delete my personal information at my request.*	4.56	4.73	-0.17
…to only keep my personal information for as long as required for business purposes or regulatory requirements.*	4.26	4.44	-0.18
…not to collect excessive or unnecessary information from me.*	4.35	4.55	-0.2
…to tell me what records of personal information they have about me when I enquire about it.*	4.41	4.68	-0.27
Items - Confidence			
I believe that online companies (websites) are only using my personal information for purposes I agreed to and never for other purposes.*	2.84	2.27	0.57
I feel confident that online companies (websites):			
…ensure that their third parties have all the necessary technology and processes in place to protect my personal information.*	2.89	2.37	0.52
…are requesting only relevant and not information other than what is needed for them to offer me a service or product.*	3.04	2.54	0.5
…are collecting my personal information only with my consent, or for a legitimate business reason.*	2.92	2.49	0.43
…keep my personal information up to date.*	2.95	2.53	0.42
…are explicitly defining the purpose they want to use my information for.*	2.92	2.5	0.42
…are notifying me before collecting my personal information.*	2.92	2.51	0.41
…have all the necessary technology and processes in place to protect my personal information.*	3	2.62	0.38
…respect my right to privacy when collecting my personal information for services or products.*	2.87	2.5	0.37
…are using my personal information in lawful ways.*	2.84	2.48	0.36
…adequately inform me of the conditions.*	2.9	2.57	0.33
…are collecting my personal information from legitimate sources. *	2.91	2.62	0.29
…protect my information if they have to send it to other countries.*	2.81	2.53	0.28
…are protecting my personal information.*	2.86	2.59	0.27
…only collect sensitive personal information.*	2.92	2.65	0.27
…are obtaining my consent to use my personal information for purposes other than those agreed to with me.*	2.88	2.62	0.26
…inform me if records of my personal data were lost, damaged or exposed publically.*	2.75	2.52	0.23
I believe that online companies (websites) take their responsibility seriously to protect my personal information.*	2.98	2.77	0.21
I feel confident that if I submit a complaint, believing that an online company (website) did not protect my personal information, that it will be dealt with appropriately by the relevant authorities.*	2.92	2.74	0.18

…will correct or delete my personal information at my request.*	2.98	2.82	0.16
can tell me what records or personal information they have about me.	2.99	2.86	0.13
I believe that online companies (websites) are keeping my personal information indefinitely.	3.26	3.14	0.12
Online companies (websites) always give me a choice to indicate if I want to receive direct marketing from them.	3.14	3.06	0.08
…honour my choice if I do not want to receive direct marketing.	2.93	2.87	0.06

* significant difference between SA and UK mean