Maraba, J., & Da Veiga, A. (2023, October). A Study of Online Privacy Policies of South African Retail Websites. In International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability (pp. 426-440). Cham: Springer Nature Switzerland.
https://link.springer.com/chapter/10.1007/978-3-031-48855-9_32

PRE PRINT VERSION

A Study of Online Privacy Policies of South African Retail Websites

Jean Maraba [0009-0005-7512-6411] and Adéle Da Veiga [0000-0001-9777-8721]

School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
marabajr@gmail.com; dveiga@unisa.ac.za

Abstract. Consumers today are pushing for greater transparency over the potential collection and use of their personal information (PI). It is key for organizations dealing with consumer PI to address privacy concerns and challenges. The use of an online privacy policy is one of the most effective ways of informing consumers about an organization's use of their PI and security measures they have adopted to protect it against possible threats. The purpose of this paper is to firstly, propose a holistic set of online privacy policy guidelines and secondly, to ascertain to what extent online privacy policies, within the South African retail sphere, address the guidelines. This, in turn, also provides an indication as to whether the online privacy policies address conditions of the Protection of Personal Information Act (POPIA). Both qualitative and quantitative analysis methods were used on a sample of 18 retail websites. While it was found that all retail websites had an online privacy policy, some were still failing to meet the proposed guidelines and as such recommendations for improvement are provided relating specifically to access, third-parties, information quality and accountability.

Keywords: Online privacy policy, Personal Information, POPIA

1 Introduction

Online privacy is important in the context of a modern technological society. With the ever-increasing importance of the internet, there is a need to adopt safeguards that protect users from the invasion of their privacy and access to identifying their PI. According to Izogo, 51% of South Africans with internet access were already shopping online in 2018, and the numbers have since been increasing [1]. Mapande and Appiah wrote about how the South African online spending curve reached a high of 53 billion Rand in 2018, with a yearly anticipated growth of 15% all through 2021 [2]. The Covid-19 pandemic fast-tracked this incline, as more and more consumers opted for online shopping as a preferred method of shopping [3]. Parallel to that, more retailers have since invested in an online presence because the convenience and accessibility to large markets which online shopping presents made engaging in it more enticing [3,4].

This increased move and need for online shopping is not one that is met without challenges, one of which is related to consumer privacy. The PI of consumers, such as

physical addresses, cell phone numbers, email address, age, race, gender, and billing information - to mention a few, are collected while shopping online [5] and without adequate measures in place, this PI can easily land in unwarranted hands without consumer consent.

Moraka [6] writes about an increased incline in data breaches by cyber attackers. These result in consumers being scammed, their identities being stolen and, most commonly, receiving unwarranted calls and SMSs from telemarketers [7,8]. The data breaches are not limited to consumer PI, but consumer trends are also recorded and analyzed, as a means of "improving" customer service, experience and for customized marketing. This is called "web tracking" and is unfortunately at the cost of the violation to consumers' privacy [9–11]. Though greatly advantageous, online shopping has, unfortunately, created a profitable business for cyber attackers of all kinds. As a result, laws related to data privacy have gained momentum around the world and most government initiatives seek to protect privacy and reputation through privacy policies [6,12].

The purpose of an online privacy policy is to inform the consumer about the retailers' data practices; what consumer PI is collected; how it is used; if there is further processing with third parties and how the PI is stored while using the website [10]. For the interest of consumers' PI protection, the online privacy policy needs to be in line with legislation, like the Protection of Personal Information Act (POPIA) of South Africa [40].

On the 1st of July 2021, POPIA was made mandatory in South Africa, as an attempt to curb privacy violation and allow for the handling of PI more effectively to safeguard individuals from possible threats [13–15]. POPIA calls for PI to only be processed given that the purpose is adequate, relevant, not excessive, individuals must be notified about the processing of their PI and given the opportunity to consent to it. This method of processing is called the 'notice and choice' model for web privacy, and it ensures that consumers are notified about the data collection and allowed a choice between opting in or out [9]. Notice and Choice serves to grant individuals greater control over how their PI is collected and used. Although conditions and legal requirements are addressed, POPIA does not, however, explicitly specify what should be covered by, or included in, an online privacy policy.

POPIA defines the eight conditions that must be met when personal information is being processed in South Africa as: "accountability, process limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation" [40]. As such, online privacy policies must address the eight conditions to be aligned with POPIA and South African organizations require guidance for this.

The aim of this paper is to firstly propose guidelines of what should be included in an online privacy policy - this will be done using the scoping literature review and PRISMA method. Secondly, the proposed guidelines will be used to evaluate a sample of South African retail website privacy policies and to propose recommendations for the retail industry to improve the content of online privacy policies in line with the proposed guidelines, which will also aid in better alignment with POPIA's requirements.

2 Research problem

The ongoing expansion of the Internet has led to more and more consumers sharing a lot of their PI and often consumers do this without fully understanding what service providers do with the trail of digital footprints they leave behind [16]. Some websites abuse users' confidence by buying, selling, or analyzing their PI without consent. Without help, people frequently do not comprehend the consequences of privacy issues or take any action to remedy them and, as such, privacy policies are used as a means of addressing this pertinent issue and informing consumers about the different uses of their PI [17].

Case and King [18] recently did a study on several Fortune500 companies' privacy policies to ascertain compliance with Fair Information Practices based on notice, choice, access, and security principles which ensure effective consumer PI protection. These principles are acknowledged by the United State government agencies but could very well be adopted, even in South Africa, as they are aligned with some of the POPIA conditions. Case and King[18] findings revealed that almost all businesses have their policies online and that the majority of those policies contain the four principles and despite the widespread and precise use of data collecting, there seemed to be a gap regarding security measures adopted to protect consumers' personal information [18]. Privacy policies are informed by a country's legislation and in the South African context, POPIA is used. However, as POPIA is founded on principles and doesn't explicitly define the criteria or guidelines of what should be included in a privacy policy, this has opened it to interpretation [19].

3 Background

This section presents an overview of privacy, consumer privacy concerns, POPIA and the purpose of online privacy policies. Studies that investigated privacy policy guidelines are also explored.

3.1 Privacy and consumer concerns

Over time, privacy has proven difficult to conceptualize, define, and it has been suggested that it is highly contextual and cannot be generalized [15, 20, 21]. Lin et al [10] writes about how the idea of privacy is ill-defined and usually contentious in the digital context. Larsen, however, provides a definition for privacy as a state of human life marked by social isolation and public exposure [22]. This condition includes any PI that the person in question has chosen to keep confidential and does not want anyone to know about [22]. In the South African context, the South African Constitution states that "everyone has the right to privacy, which includes the right to not have: their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed" [41].

When appropriate privacy protection measures are not in place, consumer PI can be easily exploited [2, 13]. It has been found in over 15 countries that 87% of people agree

on the need for legislation to prevent the violation of consumer PI [23]. Consumers are less likely to utilize a site if their privacy is abused [23, 24]. Sigmund [24] further describes how the young and educated seem to have more privacy concerns in comparison to the older generation. It can, therefore, be agreed that there is a pressing need for a data protection regime that is precise, and which facilitates the development of legislation, which is in line with technological advancements of the digital age, to protect the privacy of individuals [22]. The use of online privacy policies is precisely for this need and, as such, POPIA is an extension of the constitutional right to privacy and governs how PI is processed and used in South Africa.

3.2 Protection of Personal Information Act (POPIA)

On the 1st of July 2021, the Protection of Personal Information Act, No. 4 of 2013 came into effect. The aim of POPIA is to ensure that PI is processed lawfully. POPIA defines the different roles involved in the collection, use, transfer, storage, and application of PI in South Africa as the 'Responsible Party'- which is the retail website owner in this case. The 'Operator' – a third party contracted by the responsible party to process personal information on their behalf; 'Information Officer'- a designated individual within an institution responsible for ensuring compliance with POPIA; and the 'Data Subject'- which is the person whose PI is being processed. Furthermore, Section 3(a) of the act defines the eight conditions that need to be met for the lawful processing of PI in the country as; **Accountability:** the responsible party must ensure they are POPIA compliant. They accept responsibility for any violation and are responsible for the collection and processing of data subjects' PI and how it is shared with third parties; **Process limitation:** PI must be processed without the violation of data subjects; **Purpose specification:** PI can only be collected for a specific, documented and lawful purpose, related to the activity or function of the party collecting it and data subjects should be aware of the purpose; **Further processing limitation**: this must be consistent with the purposes for which the PI was collected; **Information quality:** the responsible party must ensure that PI is complete, accurate, not misleading, updated if needed, and consistent with the purposes for which it was collected; **Openness:** the responsible party must ensure that data subjects are aware of PI being collected, its purpose, source, name, and address of the responsible party and whether collection is voluntary or mandatory; **Security safeguards**: PI must be kept safe and secure, which necessitates the use of security measures; **Data subject participation**: data subjects have the right to access and amend their personal information, as well as have the opportunity to delete it if necessary.

3.3 Purpose of online privacy policies

The online privacy policy is a legally enforceable agreement between the website owner and user, and it is produced in accordance with the laws and regulations of a country [10, 25]. On it, the responsible party unilaterally and proactively declare the principles and measures for the safeguarding of consumer PI being collected, what PI is being collected and its intended use. The privacy policy describes the way organiza-

tions gather, utilize, share, and transfer consumer information and how information security is ensured [10, 26]. Online privacy policies are important and need to be clearly visible to consumers when they visit the retailer's website.

A study by Dias et al [27], defined Information collection, Use and Disclosure, Disclosure purpose, Opt-Out, User Access, Security, Use of cookies and Child privacy as suitable conditions for privacy policy guidelines. Isaak and Hanna [28], only highlighted Public transparency, Disclosure for users, Control: "Do no track" and notification. All the afore mentioned can be applied in a South African context. Limited studies have been done defining a comprehensive set of guidelines for online privacy policies in a South African Retail context. The aim of the next section is to review existing literature and to propose a holistic set of guidelines for online privacy policy content.

4 Literature review

A scoping literature review, using the PRISMA method, was followed to identify existing criteria and guidelines for online privacy policy content [42, 43]. The objective of this literature review is to gain insights and perspective from related studies and propose guidelines that South African Retailer website owners can follow to implement and improve their online privacy policies.

IEEE, Scopus, and ACM databases were used to collect literature dated between the years 2016 and 2022. Boolean operations were used in conjunction with the key words, for example, "POPIA AND Websites"; "online privacy policies AND South Africa"; "privacy policies AND websites"; "POPIA AND Compliance", "Websites AND privacy" and only English written journals and articles relating to online privacy policies and guidelines were selected. The titles and abstracts were screened, full text of potentially relevant articles were retrieved and reviewed for eligibility into the final inclusion. Some articles were found through the references, which were also downloaded and verified for inclusion. According to the inclusion criteria, there was a total of 64 articles. The number of relevant articles was then significantly reduced to 15 after excluding papers that did not meet the inclusion criteria as seen in Table 1 below.

Table 1. Reporting items for the systematic review – adapted PRISMA

Database	**Scopus**	**IEEE**	**ACM**	**Total**
No. of records identified from database	28	17	19	**64**
Records removed before screening	8	5	12	**25**
Records screened	20	12	7	**39**
Records excluded	4	0	1	**5**
Reports retrieved	16	12	6	**34**
Records not retrieved	6	1	1	**8**
Records assessed for eligibility	10	11	5	**26**
Records excluded	2	6	3	**11**

Records in review	8	5	2	**15**

4.1 Summary of website criteria

In total, ten consolidated guidelines were derived from the reviewed studies which are consolidated in Table 2 below. The table shows that some studies covered all these guidelines, whereas others only focused on a few. Notice (15), choice (15), security (15) and purpose specification (9) were the privacy principles that were included in most studies for online privacy policy content.

Table 2. Summary of privacy policy guidelines

Study Objective	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
This study presents the first extensive audit of disclosure of third-party data gathering in website privacy policies, with the goal of evaluating the effectiveness of "notice and choice" to find out if consumers are informed of the names of the organizations that gather their data. Over 200,000 websites' privacy policies are reviewed and data flows on a million websites are monitored. [9]	X	X				X					**3**
This study explores the extent to which supervised binary classification may be utilized to differentiate between dubious and valid privacy rules that are placed on websites. A data set containing 67 policies from malicious websites and 100 policies from reputable websites (from the top corporations on the Fortune Global 500 list) is used. When all policy information is manually analyzed, it is possible to see statistically significant differences in terms of length and conformity to the seven general privacy principles. [29]	X	X	X	X	X	X		X			**7**
To provide countermeasures for the growth of the PI protection legal framework in China, this study proposes measuring research of well-known websites in China that combines strategy analysis and web verification. [10]	X	X	X			X					**4**
This paper defines privacy governance and explores what successful governance looks like in an online setting. It seeks to better understand how New Zealand (NZ) organizations use their websites to inform users about their privacy practices and whether those practices follow the privacy laws established by the NZ government by using a content analysis questionnaire. [21]	X	X	X	X	X	X	X				**7**
This study adds to the corpus of knowledge by evaluating the need for, adoption of, and advertising of privacy policies on the websites of Portuguese local authorities, as well as by gathering evidence of those authorities' compliance with privacy standards.[27]	X	X	X	X	X	X					**6**
This study was carried out to look at the practices of the Fortune 500, the largest organizations, to see if the concepts of notice, choice, access, and security are supported by the Fair Information Practices. [18]	X	X				X					**3**
This study suggests that user friendly privacy policies that use fair information practices based on OECD guidelines will provide a competitive advantage by establishing trust between website owners and users. [30]	X	X	X			X					**4**
Through concentrating on the comparative study of privacy policies—the main means by which service providers advise customers about the collection and use of their data—this study helps readers better comprehend websites. It examined 1,562 websites and their privacy policies in comparison to premium websites to better	X	X		X	X	X		X			**6**

Study Objective	1	2	3	4	5	6	7	8	9	10	Total
understand the data usage dangers connected with such services. [31]											
This study reports on the compliance evaluation of privacy protection in e-Government systems in the countries of Anglophone West Africa, specifically in Ghana, Nigeria, Liberia, Sierra Leone, and Gambia, to partially fill the gap of literature lacking on investigations on the current status of information security and privacy protection of e-Government services in Africa. [32]	X	X	X	X	X	X		X	X		**8**
This study aims to measure the improvements in privacy laws worldwide brought about by the (General Data Protection Regulation) GDPR. It makes use of the data mining application Privacy Check to compare three corpora (totaling 550) of privacy policies automatically between before and after the GDPR. Additionally, it manually examined the policies in two corpora to assess the present state of GDPR compliance throughout the world. [33]	X	X	X			X	X		X		**6**
In this research, online privacy policies from ten industries in the three biggest economies in South Asia—India, Pakistan, and Bangladesh—are evaluated. The policies are evaluated based on accessibility, readability, and conformity with 8 privacy principles using a manual qualitative study on a dataset of 284 well-known websites. [34]	X	X	X	X	X	X		X		X	**8**
The study's objective was to examine policies from public websites in the United States Association of Research Libraries compliance with American Library Association privacy policy guidelines.[35]	X	X	X	X	X	X				X	**7**
This study assessed the Middle Eastern region's main banks' and mobile money providers' adherence to privacy laws and privacy notices' readability.[36]	X	X	X	X		X				X	**6**
This study demonstrates an automated analysis of the GDPR and Pakistan Data Protection Act compliance of privacy policies on Pakistani websites. [44]	X	X	X	X	X	X			X		**7**
This study compared the privacy policies of 30 Nigerian internet retailers with those of the Fair Information Practices (FIP) principles. [37]	X	X	X		X	X		X	X		**7**

Table note: (1) Notice, (2) Choice, (3) Purpose specification, (4) Third-Party, (5) Access, (6) Security, (7) Storage (8) Information quality, (9) Data collection limitation, (10) Minor data protection

4.2 Proposed online privacy policy guidelines

The ten guidelines derived from the scoping literature review were revised to seven guidelines. Notice, choice, and minor consent were combined because all three address consent. Storage was incorporated in Transparency and Purpose Specification as it pertains to how long the retailer intends on storing the consumer PI. Table 3 describes the proposed guidelines and includes a mapping to the conditions in POPIA.

Table 3. Proposed online privacy policy guidelines

Proposed Criteria	Mapping to POPIA guidelines
Notice & Choice: Online privacy policy content should inform the consumer about their PI collection practices, the types of PI they collect and allow consumers to consent to their PI collection practices or decline by using opt-in/out method. Considerations for minors under the age of eighteen should also be made.	Processing limitation (section 9 -12) & Openness (Section 17-18),

Proposed Criteria	Mapping to POPIA guidelines
Transparency and Purpose Specification: The online privacy policy content should clearly inform the consumer about the purpose for which they collect their PI, what type of PI is collected, how they collect it and how long they retain it.	Purpose Specification (section 13-14), Openness (section 17 & 18)
Third-Party: In the event the collected PI is shared with third parties within or outside the country's borders, the online privacy policy content should clearly specify that. The retailer should also take accountability in ensuring that the third parties comply with privacy guidelines and only use the PI for its initial intended use.	Further processing limitation (section 15)
Security: The online privacy policy content should inform the consumer about the security mechanisms they have in place to secure their PI and that in the event of a data breach, the website owner will inform the affected parties as well as the Information Regulator.	Security Safeguards (section 19–2)
Information Quality: The retailer should ensure that the collected consumer PI is accurate and up to date. This can also be achieved by allowing consumer access to their collected PI as per the proposed guideline 6. This should be clearly articulated in the online privacy policy content.	Information quality (section16)
Access: The online privacy policy content should have a paragraph informing the consumer about how they can access PI collected about them and allow them to update or delete their PI.	Data subject participation (section 23-25)
Accountability: The retailer should ensure that their privacy policy aligns with POPIA conditions and regulatory requirements for the processing of consumer PI. This should be articulated in the online privacy policy content.	Accountability (section 8)

5 Research methodology

5.1 Research paradigm

The interpretivism philosophical paradigm was adopted as the relative ontology that interpretivists use as it allows for several interpretations of the same occurrence [38]. This paradigm is applied by analyzing literature from authors in various countries. This is largely because privacy is context based, and privacy policy guidelines are informed by the laws governing a specific country.

5.2 Research design and methodology

A case study research methodology is applied. Yin [39] defines a case study as an empirical method that "investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident".

This study implores a single case study research method with embedded multiple units of analysis by reviewing online privacy policies within the South African Retail Industry, from eighteen different companies against the proposed online privacy guidelines as indicated in Table 3. The retail industry is the main unit of analysis, and the eighteen retailers constitute the analysis sub-units. A research ethics clearance was obtained for this project through the university's relevant research ethics bodies and, as such, organizational confidentiality and privacy is protected.

5.3 Data collection and analysis

A non-probability, purpose sampling method was used in the collection of the online privacy policies. In non-probability sampling, there is no way of knowing the probability of a subject being selected, and, purpose sampling permits the researcher to choose the sampled data at their convenience [45]. The range of selected retailers varied from food, clothing, and household items.

A combination of both qualitative and quantitative data analysis methods was used. First, the online privacy policies were uploaded to Atlas.ti and a content analysis method was used by searching for words such as "consent", "opt in", "security", "data breach", "amend", "delete", "third-party" and "collected" to identify data practices within the privacy policies and group them into codes of relevant themes. An excel spreadsheet was also used to track if each one of the retailers had a privacy policy pop up when the site was visited and if they had a hyperlink at the bottom of their webpage.

6 Results

Only seven of the eighteen retailers had a privacy policy notification pop-up on the landing page of their website. All eighteen retailer websites had a hyperlink at the bottom of their page directing consumers to their online privacy policy page.

Table 4. Online Privacy Policy pop-up

	Frequency	Percentage
Retailers with privacy policy pop-up	7	38%
Retailers with online privacy policy hyperlink	18	100%

All the sampled retailers addressed Notice and Choice; Security; Transparency and Purpose specification guidelines. This is great effort towards safer consumer PI processing. Only 94% addressed Access, 61% explicitly informed consumers about third party processing and 39% obliged with Information quality. These findings indicate that although all retailers had an online privacy policy on their websites, there is still a lack of consistency with some of the guidelines this study suggests.

The least addressed guideline, at a 22% is Accountability and this indicates the retailer's attempts to recuse their responsibility towards POPIA and their neglect to fostering good consumer relationship and trust. Figure 1 illustrates an aggregated view of how the eighteen online privacy policies addressed the proposed guidelines.

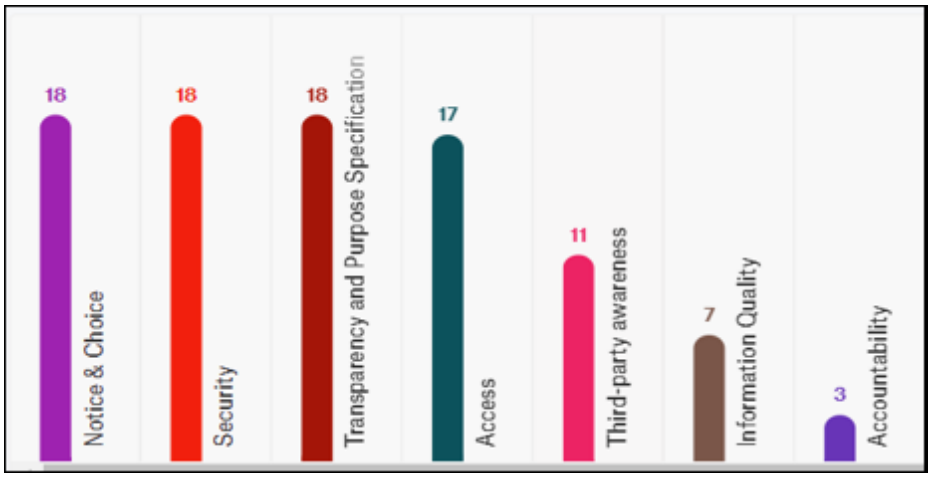

Fig. 1. Aggregated view of retailer online privacy policy.

7 Discussion and recommendations

The study revealed that the content of the reviewed South African retailer's privacy policies 100% addressed Notice and Choice, Transparency and Purpose Specification, and Security. Ninety-four percent addressed Access. Consumers should be granted access to their PI collected. This is closely tied to consent, as consumers have the right to opt out of any agreement, at any given time. Not only that but granting consumer access to collected PI allows for better quality of the PI, as they can update/amend their PI when necessary. As the collector of the PI, retailers should take sole responsibility for the cost of processing and retaining consumer PI. This should be addressed in the content of the online privacy policy. Sixty-one percent addressed Third-party, the content of an online privacy policy should clearly inform the consumer of any third-party processing and if so, also state that the third-party will process it in line with the initial collection purpose. Thirty-nine percent addressed Information Quality and 22% addressed Accountability. It is imperative that any changes to the online privacy policy be communicated with consumers, to allow consumers adequate consent to the continuation of processing their PI. This should be clearly stated in the content of the online privacy policy. The content of the online privacy policy should clearly state that the retailer takes full accountability for any loss or breach to consumer PI and disclose any breach to both the consumer and Information Regulator.

8 Limitations and future work

The proposed guidelines do not serve as a compliance measure for POPIA, however further work can be done assessing their comprehensiveness in improving the

online privacy policies, with guidance from a regulatory perspective, as well as validation from an expert panel. Further insights to this study can be derived from examining consumer opinions and encounters with the online privacy policies and how that affects consumer habits. This paper only sampled eighteen South African retail stores and this number could be increased for a broader view of the content of online privacy policies within the retail industry.

9 Conclusion

The objective of this study was to propose guidelines for the content of online privacy policies and to apply it to determine whether the online privacy policies on South African retail websites address the proposed guidelines, and to make recommendations for improvement. For this purpose, an embedded single case study, with multiple units of analysis, was used where eighteen different South African retail online privacy policies were analyzed against the proposed online privacy policy guidelines as derived from a scoping literature review. It was found that not all the guidelines were addressed in the online privacy policies. Access, third-party, information quality and accountability were aspects that required attention in online privacy policies. The guidelines and recommendations can aid retail website owners to improve their online privacy policies. Future research will focus on expanding the guidelines to incorporate more guidance from a regulatory perspective and to include a larger sample of retailers' online privacy policies in the review.

10 References

1. Izogo EE.: Online shopping experience in an emerging e-retailing market. Journal of Research in Interactive Marketing 12(2), 193–214 (2018).
2. Mapande FV, Appiah M.: The Factors Influencing Customers to Conduct Online Shopping : South African Perspective. In: International Conference on Intelligent and Innovative Computing Applications (ICONIC), pp.1–5. IEEE, Mon Tresor, Mauritius (2018).
3. Stanciu V, Rînd aşu SM.: Artificial Intelligence in Retail: Benefits and risks associated with mobile shopping applications. Journal of Amfiteatru Economic 23(56), 46-64 (2021).
4. Guru S, Nenavani J. Ranking of perceived risks in online shopping. Decision 47(1), 137-152 (2020).
5. Van der Walt W, Willems KA, Friedrich W, Hatsu S, Krauss K.: Retracted Covid-19 Papers and the Levels of 'Citation Pollution': A Preliminary Analysis and Directions for Further Research. Cahiers de la Documentation-Bladen voor Documentatie 3(4),206 -218 (2020). https://www.abd-bvd.be/nl/bladen-voor-documentatie/2020-3-4/

6. Moraka L.: The compliance framework for the 7th POPIA condition in the SME ICT Sector. Doctoral dissertation (2021). https://researchspace.ukzn.ac.za/handle/10413/20445
7. Nyoni P, Velempini M.: Privacy and user awareness on Facebook Social media: Facebook. South African Journal of Science 114(5), 1–5(2018).
8. Veiga A Da, Vorster R, Furnell SM, Clarke N, Li F. Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements. Information and Computer Security 28(3), 399–422(2019).
9. Libert T.: An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. In: 2018 World Wide Web Conference, Proceedings, pp.207–16. WWW, Lyon France (2018).
10. Lin X, Liu H, Li Z, Xiong G, Gou G.: Privacy protection of China's top websites: A Multi-layer privacy measurement via network behaviors and privacy policies. Journal of Computer and Security 114(1), 1-20 (2022).
11. Brien PO, Young SWH, Arlitsch K, Benedict K.: Protecting privacy on the web A study of HTTPS and Google Analytics implementation in academic library websites. Online Information Review 42(6), 734–51 (2018).
12. Obar JA, Oeldorf-hirsch A.: The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Journal of Information, Communication and Society 23(1), 1-20 (2018).
13. Anderson D, Bawa A, Branson N, Molefe M.: POPIA Code of Conduct for Research. South African Journal of Science 117(5), 1–12 (2021).
14. Vorster R, Pilkington C, Abdullah H, Veiga A Da. Compliance with the Protection of Personal Information Act and Consumer Privacy Expectations. In: Information Security for South Africa (ISSA*)* 2017 Proceedings, pp.16-23. IEEE, Johannesburg South Africa (2017).
15. Swales L.: The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock?. Potchefstroom Electronic Law Journal 25(1), 783–797 (2022).
16. Tesfay WB, Hofmann P, Nakamura T, Kiyomoto S, Serna J.: I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR. In: Companion of the World Wide Web Conference Proceedings, pp.163-166. WWW, Lyon, France (2018).
17. Pilton C, Faily S, Henriksen-Bulmer J, E.: Evaluating privacy - determining user privacy expectations on the web. Journal of Computer and Security 105, 1-16 (2021).
18. Case CJ, King DL.: Fair Information Practices : An empirical review of the fortune 500. Journal of Business and Behavioral Sciences 34(1), 49-630 (2022).
19. Pelteret M, Ophoff J.: Organizational information privacy strategy and the impact of the PoPI act. In: 2017 Information Security for South Africa (ISSA) Proceedings, pp.56-67. IEEE, Johannesburg South Africa (2017).
20. Bleier A, Goldfarb A, Tucker C, E.: Consumer privacy and the future of data-based innovation and marketing. International Journal of Research in Marketing 37(3), 466–80 (2020).

21. Tjhin I, Vos M, Munaganuri S, A.: Privacy governance online: Privacy policy practices on New Zealand websites. In: 2016 Pacific Asia Conference on Information Systems (PACIS) Proceedings, Chiayi Taiwan (2016).
22. Larsen C.: Data Privacy Protection in South Africa: An analysis of vicarious liability in light of the protection of Personal Information Act 4 of 2013 (" POPIA "), Masters of Law (LLM) in Business Law Degree College of Law and Management Studies University of Kwazulu Natal. (2019).
23. Alzaidi MS, Agag G.: The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. Journal of Retailing and Consumer Services 68(C).103042, (2022).
24. Sigmund T.: Attention paid to privacy policy statements. Information 12(4), 144 (2021).
25. Wilson S, Schaub F, Dara AA, Liu F, Cherivirala S, Leon PG, et al.: The creation and analysis of a Website privacy policy corpus. In: Erk K, Smith N. (eds.) 54th Annual Meeting of the Association for Computational Linguistics, LNCS, vol.1, pp1330-1340. ACL, Germany (2016).
26. Ali AS, Zaaba ZF, Singh MM, Hussain A.: Readability of websites security privacy policies: A survey on text content and readers. International Journal of Advanced Science and Technology 29(6), 1661-1672 (2020).
27. Dias GP, Gomes H, Zúquete A.: Privacy policies and practices in Portuguese local e-government. Electronic Government, an International Journal 12(4), 301-318 (2016).
28. Isaak J, Hanna MJ:. User Data Privacy: Facebook, Cambridge Analytica and Privacy Protection. Computer 51(8), 56-59 (2018).
29. Boldt M, Rekanar K.: Analysis and text classification of privacy policies from rogue and top-100 fortune global companies. International Journal of Information Security and Privacy 13(2), 47–66 (2019).
30. Ginosar A, Ariel Y. An analytical framework for online privacy research: What is missing?. Information and Management 54(7), 948–57(2017).
31. Alabduljabbar A, Mohaisen D.: Measuring the Privacy Dimension of Free Content Websites through Automated Privacy Policy Analysis and Annotation. In: The Web Conference 2022 Proceedings, pp.860–867. ACM, Lyon France (2022). https://doi.org/10.1145/3487553.
32. Nwaeze AC, Zavarsky P, Ruhl R.: Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011.: In:12th International Conference on Digital Information Management, ICDIM Proceedings, pp.98–102. IEEE, Fukoaka Japan (2017).
33. Zaeem RN, Barber KS.: The Effect of the GDPR on Privacy Policies. ACM Trans Manag Inf Syst 12(1), 1-20 (2020).
34. Javed Y, Salehin KM, Shehab M.: A Study of South Asian Websites on Privacy Compliance. IEEE Access 8, 156067-156083 (2020).
35. Valentine G, Barron K.: An Examination of Academic Library Privacy Policy Compliance with Professional Guidelines. Evid Based Libr Inf Pract 17(3),77–96(2022).

36. Javed Y, Qahtani E Al, Shehab M.: Privacy policy analysis of banks and mobile money services in the middle east. Future Internet 13(1), 1–15 (2021).
37. Bello OW, Adeyemi R, Bello OW, Oyekunle A.: Analysis of the Privacy Policies of Nigerian Online Shops. International Journal of Information Processing and Communication (IJIPC) 6(1),347-362(2018).https://www.researchgate.net/publication/329872094
38. Pham L.: A review of advantages and disadvantages of three paradigms: positivism, interpretivism and critical inquiry.
39. Yin RK.: Case Study Research and Applications. 6th edn. Thousand Oaks CA, Sage Publications (2018).
40. The Parliament of the Republic of South Africa (2013) Protection of Personal Information Act, Act No. 4 of 2013, Government Gazette, Vol. 581, No. 37067. Cape Town, South Africa
41. The Bill of Rights of the Constitution of the Republic of South Africa Chapter 2(14). Government Gazette, Cape Town (1996).
42. Munn, Z., Peters, M.D.J., Stern, C et al.: Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodology 18(1), 143(2018).
43. Selcuk, A.A.: A guide for Systematic Reviews: PRISMA. Turkish Archives of Otorhinolaryngology 57(1), 57-58(2019).
44. Asif, M., Javed, Y., Hussain, M.: Automated Analysis of Pakistani Websites' Compliance with GDPR and Pakistan Data Protection Act. In: International Conference on Frontiers of Information Technology (FIT*)* Proceedings, pp. 234-239. IEEE, Islamabad Pakistan, (2021).
45. Etikan, I., Bala K.: Biometrics and Biostatistics International Journal 5(6), 215-217(201)