Published version can be found here:
Maguraushe, K., Da Veiga, A., & Martins, N. (2019, October). A conceptual framework for a student personal information privacy culture at universities in Zimbabwe. In *ICICIS* (pp. 143-156).
https://easychair-www.easychair.org/publications/download/kgNN

Pre-print version included below

A conceptual framework for a student personal information privacy culture at universities in Zimbabwe

Kudakwashe Maguraushe[1], Adéle da Veiga[2] and Nico Martins[3]
[1,2,3] School of Computing; College of Science, Engineering and Technology
University of South Africa, Florida, Johannesburg, South Africa
[1]kmaguraushe@gmail.com, [2]dveiga@unisa.ac.za, [3]martinsn@mweb.co.za

Abstract

In this research, an information privacy culture is proposed to be embedded in three basic concepts: students' privacy expectations, privacy awareness and confidence in universities' capability to uphold information privacy. The aim of this research was to address the lack of an information privacy culture framework in the context of universities in Zimbabwe, the upsurge of privacy breaches in these institutions and the need to assist them in processing the information in line with regulatory requirements. The main objective of this study was therefore to ascertain the key components of a student personal information privacy culture (SPIPC) conceptual framework for universities in Zimbabwe. A scoping review was conducted and a SPIPC conceptual framework is proposed.

1 Introduction

The protection of any natural person in relation to the processing of their personal data is a fundamental human right (Zimbabwe Data Protection Bill, 2013). The protection of privacy is enshrined in the Constitution of Zimbabwe (Zimbabwe Constitution Parliamentary Committee, 2013). However,, the Zimbabwe Data Protection Bill (ZDPB) still awaits presidential assent and promulgation (Chetty, 2013). Universities are public entities and hence the ZDPB will apply to them in terms of personal information usage. Universities will need guidance, like a framework (Ivanova, Grosseck & Holotescu, 2015), to implement the provisions of the bill but there are none yet. A privacy framework can assist institutions in leveraging student personal information self-determination (Mulligan, Koopman, Doty & Mulligan, 2016) and creating a culture of protecting student information.

Since an information security culture can be extended to encompass the concept of privacy by virtue of privacy being a subset of security (Da Veiga & Martins, 2015), it follows that awareness and training

are critical to the success of any information security initiative. This implies that in order to instil a privacy culture, awareness of personal information privacy is critical. It also follows that if an organisation (university) is to comply with regulatory requirements and protect their customers' (students') personal information, trust has to be accumulated (Da Veiga, 2017). Currently, in the Zimbabwean context, it is a difficult task to analyse and comprehend students' expectations of information privacy, their awareness levels of information privacy as well as their privacy confidence levels in universities' ability to indeed, meet privacy expectations and legal obligations. This is so because there is no reference point to measure these concepts from an industry or academic literature perspective. Privacy as a research area requires attention given the increase in data privacy breaches such as on Facebook where personal data were harvested to influence the 2016 US elections without users' knowledge (Santanen, 2018). In the Zimbabwean context, Harare Institute of Technology (a university) was attacked twice in the space of two years and sensitive information like names, registration numbers and passwords were stolen (Mudzingwa, 2018), which amounts to privacy breaches in terms of the personal information of students. With this background, it becomes essential to implement measures in order to improve the protection of personal information, including students' personal information.

The ZDPB, together with the Organisation for Economic Cooperation and Development's (OECD) Privacy Framework of 2013, the privacy principles of the General Data Protection Regulation (GDPR) and the Fair Information Practice Principles (FIPPs) as the baseline, will be used in designing a conceptual student personal information privacy culture (SPIPC) framework that universities can use when processing students' personal information to create a culture of privacy. This study was conducted in the context of information systems, considering the concept of data privacy to protect personal information from a regulatory perspective.

2 Background

An information privacy culture is defined by Da Veiga (2018a:2) as "the perceptions and beliefs a nation has about the processing of citizens' personal information, what expectations they have and how they believe organisations are meeting those expectations given certain information privacy principles (or requirements)". This privacy culture must be cultivated within an organisation so that individuals preserve information privacy, thereby upholding the confidentiality, integrity and availability aspects, which is evident when people comply with regulatory requirements (Da Veiga & Martins, 2015).

Within the context of this research, an information privacy culture is proposed to be embedded in three basic concepts: students' privacy expectations, privacy awareness and confidence that universities uphold information privacy.

The proposed information privacy framework hinges on privacy guidelines like the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data of 2013, GDPR and ZDPB in order to direct individuals within institutions in improving regulatory compliance (Chua, Herbland, Wong & Chang, 2017). Universities need to understand the privacy expectations of students so that they can better protect students' personal information that they collect. This will increase students' confidence in the processing of their personal information by the university and help them to have less privacy concerns (Iachello & Hong, 2007), and is a new dimension of information technology research (Mamonov & Benbunan-Fich, 2018).

From a broader perspective on privacy compliance and abuse in Zimbabwe, Kaseke (2018) highlights that Zimbabwe needs legislation to protect its citizens against the misuse and abuse of their personal information. This follows the ruling party's use of citizens' personal information for campaigning purposes without their consent. This information was harvested by the Zimbabwe Electoral Commission (ZEC) for the biometric voters' roll and included names, addresses and cell phone details. Unfortunately, the lack of legislation and a well-articulated data controller for accountability purposes meant that no remedial action was taken. In addition, it is a norm that the voters' roll should be highly secured since it contains very sensitive information. In the case of Zimbabwe, this was made public online for anyone to see. If this could happen to the whole nation, there is no guarantee that universities will not fall victim to information privacy abuse. All these problems attest to the lack of a regulator and no documented penalties for the misuse of personal information as prescribed by the ZDPB.

Research (Chua et al., 2017) has revealed and exposed the failure of institutions to comply with privacy policies as well as regulatory requirements. A major concern with universities collecting students' personal information is that they often use it for purposes for which it was not originally intended and which result in privacy breaches (Arnold & Sclater, 2017). Personal information requires better safeguarding in order to prevent breaches and there is a need to develop incident response plans to improve the protection of privacy (OECD, 2013). Privacy breaches are mainly attributed to those who are supposed to safeguard the data (Iachello & Hong, 2007). The university is the safeguarding entity in the context of this research and they have a responsibility of instilling an information protection culture to aid in meeting students' expectations and regulatory requirements, suppressing privacy concerns. Information privacy concerns can affect one's intention to provide information due to lack of trust and willingness to engage with the university (Chua et al., 2017). Privacy breaches could be an indication of non-compliance with the regulations on data protection (Da Veiga, 2018a). Compliance can be achieved if suitable standards are incorporated in privacy regulatory frameworks in an effective manner.

2.1 Related Work

Limited frameworks for the privacy of students' personal information and the privacy of personal information in general are in use. Of note is the University of California, whose privacy framework derives from various privacy principles, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Yudof, 2013). It contains privacy principles guided by the Autonomy Privacy Principles (free inquiry, respect for individual privacy and surveillance) as well as information privacy principles guided by the six principles of privacy by design, choice, notice and transparency, information correction and review, information protection and accountability (Yudof, 2013). However, the framework does not touch on students' awareness of privacy regulations and there is no roadmap for how students can develop confidence in the university in terms of privacy. BSA, which is a leading global software company, has a 10-component privacy framework to uphold the privacy and security of their clients' personal data (BSA, 2018). These are transparency, purpose specification, informed choice, data quality, consumer control, security, facilitating data use for legitimate interest, accountability, legal compliance and enforcement, and international interoperability. The purpose of this is to give users more control over their personal information, which is in line with consumers' expectations (BSA, 2018). Another generalised privacy framework is that of the Office of the Australian Information Commissioner (OAIC) which was designed to assist in developing a privacy roadmap for any entity (including a university), with the explicit target being how it can be achieved (OAIC, 2015). The framework focuses more on information privacy compliance, with nothing in place for expectations and awareness thereof.

In comparison to this research, the abovementioned frameworks do not incorporate student privacy awareness and student privacy expectations. Although studies have been carried out to assess various concepts within university environments, none has been done on the awareness of students, their expectations and the attributes that increase students' confidence in the university's ability to uphold their privacy. The few frameworks do not take cognisance of the FIPPs, which is another motivating factor for this research as this study incorporates the FIPPs as the grounding privacy principles. Moreover, most of the frameworks focus on the implementation of privacy, highlighting various steps to be adhered to without necessarily looking at other components like awareness, expectations and confidence in the institution. Thus the need for a framework and diagnostic tool to assist universities in understanding students' privacy concerns and expectations of the protection of personal information, privacy and aid in giving effect to the constitutional right to privacy.

This study focused on the development of a SPIPC conceptual framework for the processing of students' personal information in Zimbabwe. This framework will not only incorporate students' privacy expectations but will also enhance their awareness in the process and instil confidence in them that the university is committed to preserving their privacy rights. The SPIPC framework will be used as a theoretical framework for the development of a validated SPIPC diagnostic instrument in future research.

2.2 Problem Statement

Partly inscribing the privacy requirements in the constitution is insufficient for providing a privacy compliance guideline on how personal information should be used. Since universities are public entities, the ZDPB will apply to them when processing the personal information of students. Universities will require guidance such as a framework to implement the requirements in the constitution and the ZDPB, but as yet, there are none in the context of Zimbabwe. A SPIPC conceptual framework can provide guidance to universities in the implementation of privacy requirements while addressing students' expectations of privacy in order to create a culture where privacy is uphold.

2.3 Research Question

This research study was guided by the following research question:

What are the key components of an SPIPC conceptual framework in the context of universities in Zimbabwe?

The remainder of this paper is structured as follows: In Section 3, the scoping review and methodology of the study are discussed. Section 4 contains a discussion of the privacy concepts of the SPIPC framework, Section 5 focuses on the privacy components of the SPIPC framework and Section 6 details the SPIPC framework. In Section 7, the expected contributions and some future work on this research were discussed; Section 8 concludes the study.

3 Methodology

A scoping review was conducted and the conceptual SPIPC framework is proposed. A scoping review is "a form of knowledge synthesis that addresses an exploratory research question aimed at mapping key concepts, types of evidence and gaps in research related to a defined area or field by systematically searching, selecting, and synthesising existing knowledge" (Colquhoun et al.,

2014:1292). It is an overview of a larger field of research aimed at mapping the key concepts underpinning a research area and the main sources and types of evidence available (Colquhoun, 2016).

Data collection was in the form of literature searches of databases that include Web of Science, ACM, IEEE Xplore, Google Scholar and Scopus. The literature search period included years of publication ranging from 2000 to 2018. Relevant articles that matched the search were read and relevant ones were selected. Studies outside the publication dates were excluded; studies that did not address student expectations on privacy, awareness levels on privacy and confidence levels on privacy were also excluded.

Since the scoping review was adopted for this study, Figure 1 is a summary of how it was conducted during the literature search.

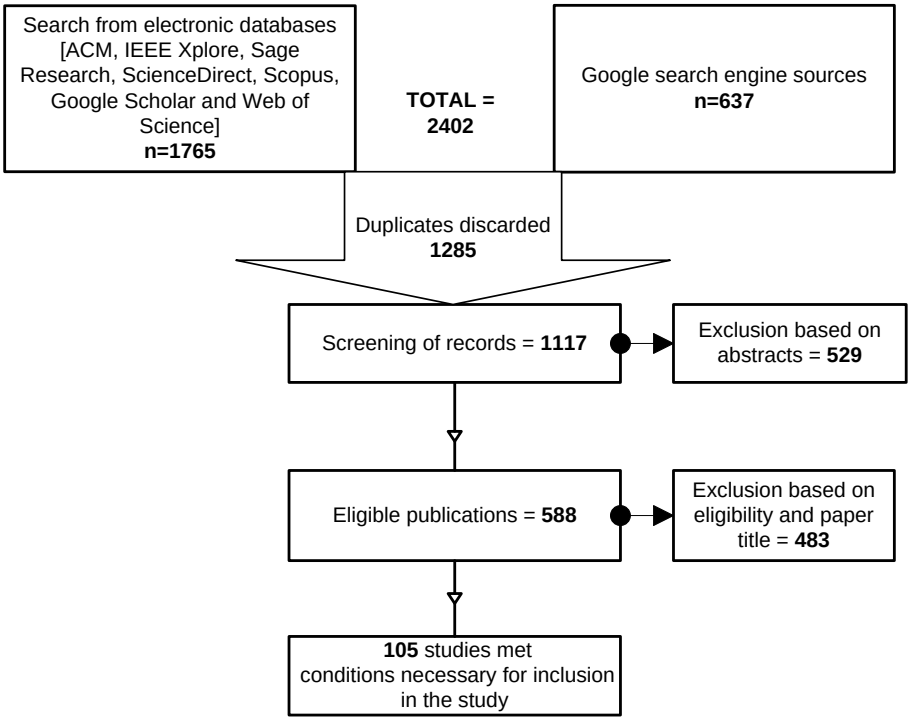

Figure 1: Scoping review literature search summary

The above figure of the scoping review for this study shows that a total of 1765 searches of electronic material from various electronic databases were done. These were uploaded to the Mendeley desktop library for easier management. Searches of literature material were also done, with 637 Google retrievals. This gives a total of 2402 literature sources. Among these, 1285 were discarded as duplicates, leaving 1117 literature sources for screening. For inclusion, the focus was on keywords such as the following: “personal information”, “privacy”, “information privacy culture”, “student privacy awareness”, “privacy and expectations”, “privacy and confidence”, “privacy concerns”, “privacy breaches”, “privacy compliance”, “privacy perceptions” and “student privacy frameworks”. For exclusion, two steps were followed. The first step was based on abstracts and 529 literature sources were excluded, leaving 588 sources. In the second step, sources were excluded based on title and

eligibility; 483 sources were excluded. This left 105 literature sources that met the conditions for inclusion into this study. These 105 sources were used to define the concepts of the SPIPC framework.

4 Privacy Concepts

Privacy is a paramount concept that needs to be observed within the university environment. Students have their own expectations as well as awareness levels of privacy, which must lead to the development of confidence that the university observes and upholds the privacy of their personal information. As pointed out by Da Veiga (2018b), confidence in terms of privacy indicates that an organisation implements privacy regulatory requirements when handling customers' (students') personal information. The three concepts namely, students' privacy awareness, privacy expectations and confidence in the university are depicted in Figure 2 as the first building blocks of the SPIPC framework. The three concepts are discussed from the student's perspective (i.e. the study was student centred).

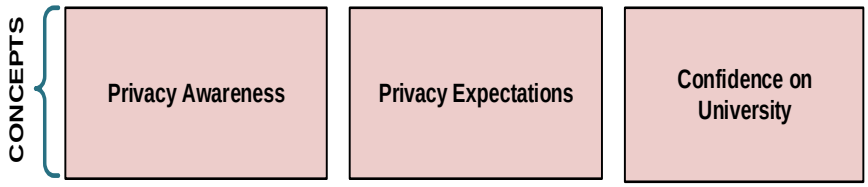

Figure 2: Privacy concepts

4.1 Privacy Awareness

Awareness is created through the privacy notices of the university (Vail, Earp & Antón, 2008). Research results (Chen & Ismail, 2013) show that students lack knowledge and understanding of privacy within universities. Awareness is a prerequisite of compliance (Aghasian, Garg, Gao, Yu & Montgomery, 2017). Research by Nwaeze, Zavarsky and Ruhl (2018) also show that compliance with privacy policies and laws, and privacy concerns, are a result of proper awareness programmes in organisations. Lawler and Molluzzo's (2011) research resonates with that of Isabwe and Reichert (2013) in recommending that universities should promote privacy awareness and allow students to exercise their right to privacy and have consent control, especially when processing personal information. As indicated in the Constitution of Zimbabwe, it is the duty of the data controller (the university) to disseminate knowledge and awareness about privacy (Republic of Zimbabwe, 2013). Awareness increases users' (students') compliance with policies and willingness to give or disclose their personal information for positive use by the data controller (university) (Kurkovsky & Syta, 2011).

4.2 Privacy Expectations

FIPPs recommend that individuals (students) must have the expectation of personal information privacy (Cate, 2006). Even when there is a need to obtain personal information for processing by the organisation (university), a considerable degree of expectation of privacy rests on the belief that the collection will be minimal and based on relevance (Cate, 2006). Empirical results obtained by Da Veiga (2018a) indicated that consumers have high expectations of privacy in organisations (institutions) when processing their personal information. If consumers (students) perceive the organisation (university) as failing to meet their privacy expectations, they tend to become impassioned and reject sharing their personal information with the organisation (university) (Morton & Sasse, 2014).

4.3 Confidence in the University

In some cases, students have confidence in their institutions to the extent that they do not seek privacy related to documentation (Stange, 2011). Privacy pledges by universities provide a sense of trust that instils confidence and this results in an information privacy culture that can permeate the whole institution (Alnatheer, Chan & Nelson, 2012). As Dwyer and Marsh (2016) point out, trust is an element of confidence; this is corroborated by the OECD (2013). If there is an improvement in privacy protection and privacy regulations, users' confidence tend to increase (BSA, 2018). Lack of trust in the use of personal information has a negative impact on the confidence levels of students (Dwyer & Marsh, 2016; OAIC, 2015). Data and privacy breaches result in low confidence in customers (students) towards the business (university) (Bush, 2016). Any loss of confidence or trust in the organisation or university will have undesirable retrogressive consequences (OECD, 2013). Therefore, there is a need for the university to be conversant of privacy policies with regard to students, which will eventually increase compliance with privacy policies (Kurkovsky & Syta, 2011). A personal information privacy culture within an organisation or institution inspires trust and confidence in the entity (OAIC, 2015).

5 Privacy Components

The FIPPs were used as the baseline for the components of this study and were complemented by the OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPB. The FIPPs were used as the baseline because they are believed to be the founding and underlying guidelines for personal information self-regulation in the digital world (Cate, 2006; Gellman, 2017). The OECD Protection of Privacy and Transborder Flows of Personal Data of 2013 was a revision of the original FIPPs, underpinning the fact that most privacy principles are anchored on the FIPPs (Gellman, 2017). In the context of this study, discussions on the SPIPC framework were done from the student's perspective. Two of the FIPPs components (i.e. security and accountability) are enforceable by the university since it is the university's prerogative. Accordingly, these components were excluded from adoption into the SPIPC framework. The final six components are notice/openness, information quality, purpose specification, use limitation, collection limitation, and individual participation or choice. Privacy policy, education and consent were added to these components.

5.1 Notice/Openness

While notices are believed to make students aware of privacy-related issues, they also provide trust and confidence in the data subject (student, in this case), which is important for fostering a relationship between the parties concerned (Guffin, 2017; Stange, 2011). Appropriate notice is needed before personal information is collected (Guffin, 2017). Students expect notices to be short, flexible and non-ambiguous (Preuveneers, Joosen & Ilie-Zudor, 2016). Notices are assumed to make institutions transparent and open in terms of how they use the personal information of the students as data subjects (Gellman, 2017). It is also important that if there is a privacy breach of a student's personal information, he or she has to be notified within the shortest period of time (Cornock, 2018).

5.2 Information Quality

Information quality is important in achieving integrity of information within an organisation (university) (Guffin, 2017; OECD, 2013; Zimbabwe Data Protection Bill, 2013). Personal information should be up to date, complete and accurate, without compromising its relevance to the purpose for which it is to be used (Gellman, 2017). It is the prerogative of the university to uphold personal information privacy for information quality (Guffin, 2017). This will increase students' confidence in

the university. The assurance of information quality is also measured by the presence of information security (Banerjee, 2015).

5.3 Purpose Specification

In terms of the ZDPB, Chetty (2013) highlights that individual personal information has to be processed for an explicit, specified and legitimate reason; and this must be done on or before the time of collection. In addition, once the information is collected, it must not be directed to or used for a purpose not previously specified unless this is done to comply with the law (Katurura & Cilliers, 2016). Before any collection of personal information is done, consent must be obtained from the subject matter (the student, in this case) (Johnston & Wilson, 2012).

5.4 Use Limitation

The individual (student) will expect the organisation (university) to limit the amount of information they collect for use (Cate, 2006). The OECD Privacy Framework of 2013 specifies that "personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except: with the consent of the data subject; or by the authority of law" (OECD, 2013:14). The importance of mandatory and fundamental consent in the collection or use of any personal information is also stressed (Cate, 2006). The purpose has to be explicit and clearly spelt out (Robbins & Sabo, 2006).

5.5 Collection Limitation

Collection minimisation is important because the organisation (university) should collect information lawfully, fairly and only for the specified purposes (Chetty, 2013). In this case, the university should limit collection of personal information that is not necessary for academic purposes. If the organisation (university) is to collect a large amount of personal information from the user (student), it will raise privacy concerns among the students (Rasmussen & Dara, 2014). In reality, limiting the amount of information collected increases participation by students and consequently information privacy (Kokolakis, 2017).

5.6 Individual Participation/Choice

Individuals, including students, must be given the right to participate in activities related to their personal information (OECD, 2013; Zimbabwe Data Protection Bill, 2013). Their participation increases the knowledge and assurance on how their personal information is being used by the university, ultimately building confidence in the university (Cate, 2006). The right of participation principle increases transparency in the use of students' personal information (Tikkinen-Piri, Rohunen & Markkula, 2018). The university must be able to provide a response as confirmation to the data subject (student) about personal information collected (OECD, 2013). When making a request for conformation about personal information collected, the data subject (student) has the right to follow clearly set processes as stated in the individual participation principle (OECD, 2013). Moreover, students must be able to amend their personal information as and when the need arises (Gellman, 2017). Technology must not affect how personal information is accessed by students (Chetty, 2013).

Studies have shown that privacy policies address privacy concerns and universities need it to instil awareness in students (Chua et al., 2017). Students also need to be educated on privacy-related issues. Farooq, Kakakhel, Virtanen and Isoaho (2016) reveal that privacy education is a key measure for reducing information privacy concerns. Central to the processing of any personal information is consent, which must be granted by the student as a basic human right (European Union, 2016; OECD,

2013; Zimbabwe Data Protection Bill, 2013). This creates three more components, which were added to the SPIPC framework (i.e. privacy policy, privacy education and consent).

5.7 Privacy Policy

A privacy policy is a document that discloses how organisations should collect, manage, disclose or use an individual's personal information (Chua et al., 2017). It is a way of achieving privacy of personal information and it should be in place (Chua et al., 2017). Privacy policies should be easily understood and should be short, precise and to the point (Vail et al., 2008). It is an expectation of the university administrators that students need to read the whole privacy policy document in order to be aware of privacy-related issues (Lawler, Molluzzo & Doshi, 2012). Changing privacy policies continuously and frequently will confuse students (OECD, 2013).

5.8 Privacy Education

Education increases awareness (Rezgui & Marks, 2008). Privacy education is very important as it informs the students about the reasons for collecting their personal information, how the information will be used, the sensitivity of the personal information and what they will receive after sharing their personal information with the university (Isabwe & Reichert, 2013). Students need to be continuously reminded of the privacy-related issues through privacy education (Sargsyan, 2016). The Expert Group on privacy proposed that in order for the OECD Protection of Privacy and Transborder Flows of Personal Data framework to be effective, privacy education is critical in reducing privacy breaches (Gellman, 2017). Therefore, lack of privacy awareness can be solved by providing privacy education to the students (Fink, 2012).

5.9 Consent

Consent is not a principle but rather a fundamental right that should be clear before information is shared (European Union, 2016; OECD, 2013; Tikkinen-Piri et al., 2018; Zimbabwe Data Protection Bill, 2013). It is an individual's right to receive communication about, and to give confirm or withhold confirmation for, when information about them is to be used (OECD, 2013; Zimbabwe Data Protection Bill, 2013). Students have the right and choice of consent to opt to share their personal information (Chua et al., 2017). If a student does not require the continued sharing or receiving of certain messages, he/she has the right to opt out (Krishnan & Vorobyov, 2015). Individuals, including students, must not be harassed or intimidated into giving consent (Cornock, 2018; Zimbabwe Data Protection Bill, 2013). It is imperative that the university is clear when they want to collect personal information by consent (Taddei & Contena, 2013). By seeking consent from the students, the university will increase the students' trust in the institution regarding the use of their personal information (OAIC, 2015; Sargsyan, 2016).

6 Conceptual Framework

The SPIPC framework has two sections: the privacy components section and the privacy concepts section. When combined, the researcher perceives the two sections as formulating the information privacy culture within the university environment, which must be cultivated to enhance privacy of personal information. Figure 3 shows the SPIPC framework: expectations, awareness and confidence in the university, with the adopted components.

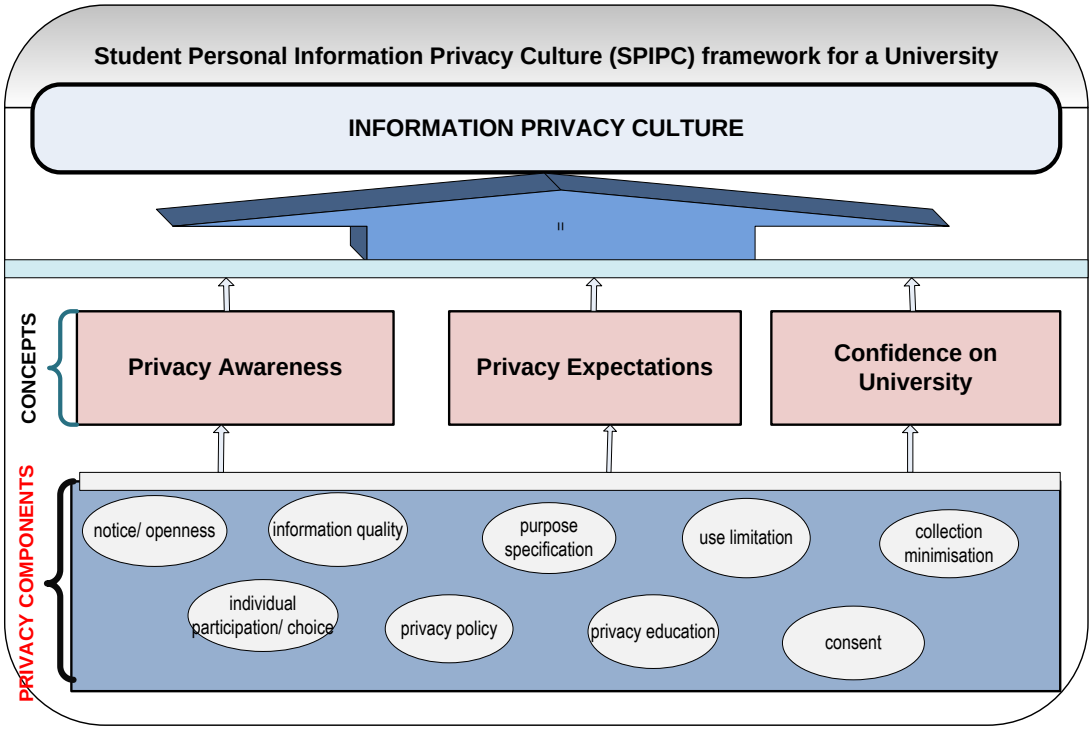

Figure 3: The SPIPC framework

The privacy concepts and privacy components in the above diagram are discussed below:

Privacy Concepts: A university must thrive to fulfil and meet the three privacy concepts so that privacy of students' personal information is well articulated. The three privacy concepts are used to measure the components. This means that every component must be tested for awareness, expectations and confidence.

Privacy Components: The framework's scope is grounded on personal information from the student's perspective on the university, as derived from the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPB. The components are considered fundamental and every student must play a role in adhering to them in a bid to have a positive information privacy culture. When combined, these components aid in understanding the information privacy culture in terms of students' awareness, expectations and confidence in the university.

7 Expected Contributions and Future Work

This study involved developing the SPIPC framework based on the three concepts of students' privacy awareness, privacy expectations and confidence in the university. The research also contributed to articulating the three concepts from a student perspective. The integration of the principles of the OECD Protection of Privacy and Transborder Flows of Personal Data, the privacy guidelines of the FIPPs, the GDPR directive and the ZDPB allows for easy adoption even beyond Zimbabwe.

The SPIPC will be used to develop a diagnostic instrument (questionnaire) with statements addressing each concept of the FIPPs, together with the additional concepts from an awareness, expectation and confidence perspective. The questionnaire will be validated in a university environment and the framework will be validated using structural equation modelling (SEM). This will aid universities in implementing privacy expectations while aiming to meet regulatory requirements. The SPIPC framework can also be used in other universities in Africa and other parts of the world to improve the protection of privacy of students.

8 Conclusion

The SPIPC framework was presented as formulated from the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPB, with nine components for building and ensuring a privacy culture within a university environment. Relevant literature relating to the concepts and components were explored to develop the framework. The framework will be used in future studies for the empirical investigation of the relationships between the various concepts and components. It can also be used in other parts of the world or by industry in a bid to uphold information privacy.

Acknowledgment

This paper is based on the thesis document for the Doctor of Philosophy in Information Systems degree at the University of South Africa (Unisa) and was wholly supported by the Unisa Master's and Doctoral (M+D) Research Bursary disbursed in 2019.

References

Aghasian, E., Garg, S., Gao, L., Yu, S., & Montgomery, J. (2017). Scoring users' privacy disclosure across multiple online social networks. *IEEE Access*, *5*, 13118–13130. Retrieved from https://doi.org/10.1109/ACCESS.2017.2720187

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Pacific Asia Conference on Information Systems (PACIS)*, *144*(12), 1–15. Retrieved from http://aisel.aisnet.org/pacis2012/144

Arnold, K. E., & Sclater, N. (2017). Student perceptions of their privacy in leaning analytics applications. *Proceedings of the Seventh International Learning Analytics and Knowledge Conference*, 66–69. Retrieved from https://doi.org/10.1145/3027385.3027392

Banerjee, S. (2015). Development and validation of a conceptual framework for IT offshoring engagement success (University of Bedfordshire). Retrieved from http://hdl.handle.net/10547/583209

BSA. (2018). *BSA PRIVACY FRAMEWORK* (pp. 1–2). Retrieved from https://www.bsa.org/files/policy-filings/BSA_2018_PrivacyFramework.pdf

Bush, D. (2016). How data breaches lead to fraud. *Network Security* (pp. 11–13). Retrieved from https://doi.org/10.1016/S1353-4858(16)30069-1

Cate, F. H. (2006). The failure of fair information practice principles. *Conference on Consumer Protection in the Age of the Information Economy*, 341–378. Retrieved from https://ssrn.com/abstract=1156972

Chen, L. F., & Ismail, R. (2013). Information technology program students' awareness and perceptions towards personal data protection and privacy. *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 434–438. Retrieved from https://doi.org/10.1109/ICRIIS.2013.6716749

Chetty, P. (2013). Presentation on Zimbabwe Data Protection Bill. *Harmonization of the ICT policies in sub-Sahara Africa*. Retrieved from

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157–170. Retrieved from https://doi.org/10.1016/j.tele.2017.01.008

Colquhoun, H. (2016). Current best practices for the conduct of scoping reviews. *Impactful Biomedical Research: Achieving Quality and Transparency*, 1–24. Retrieved from https://doi.org/10.1093/ptj/pzx074

Colquhoun, H. L., Levac, D., O'Brien, K. K., Straus, S., Tricco, A. C., Perrier, L., … Moher, D. (2014). Scoping reviews: Time for clarity in definition, methods, and reporting. *Journal of Clinical Epidemiology*, *67*(12), 1291–1294. Retrieved from https://doi.org/10.1016/j.jclinepi.2014.03.013

Cornock, M. (2018). General Data Protection Regulation (GDPR) and implications for research. *Maturitas*, *111*, 20–21. Retrieved from https://doi.org/10.1016/j.maturitas.2018.01.017

Da Veiga, A. (2017). An information privacy culture index framework and instrument to measure privacy perceptions across nations : Results of an empirical study. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security and Assurance (HAISA)*, 196–209. Retrieved from http://hdl.handle.net/10500/23566

Da Veiga, A. (2018a). An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information and Computer Security*, *26*(3), 338–364. Retrieved from https://doi.org/10.1108/ICS-03-2018-0036

Da Veiga, A. (2018b). An online information privacy culture: A framework and validated instrument to measure consumer expectations and confidence. *2018 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. Retrieved from https://doi.org/10.1109/ICTAS.2018.8368759

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, *31*(2), 243–256. Retrieved from https://doi.org/10.1016/j.clsr.2015.01.005

Dwyer, N., & Marsh, S. (2016). How students regard trust in an elearning context. *14th Annual Conference on Privacy, Security and Trust (PST) 2016*, 682–685. Retrieved from https://doi.org/10.1109/PST.2016.7906956

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation). 59 Official Journal of the European Union §.

Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2016). A taxonomy of perceived information security and privacy threats among IT security students. *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 280–286. Retrieved from https://doi.org/10.1109/ICITST.2015.7412106

Fink, C. (2012). Privacy and confidentiality in the virtual classroom: Instructor perceptions, knowledge and strategies (University of Victoria). Retrieved from http://hdl.handle.net/1828/4176

Gellman, R. (2017). Fair information practices: A basic history. *SSRN Electronic Journal* (Version 2.18), 1–46. Retrieved from https://doi.org/10.2139/ssrn.2415020

Guffin, P. (2017). FIPPs and PIA. State of the Judicial Branch, 1–6. Retrieved from https://www.courts.maine.gov/maine_courts/committees/tap/FIPPs-and-PIA-email.pdf

Iachello, G., & Hong, J. (2007). End-user privacy in human–computer interaction. *Foundations and Trends® in Human-Computer Interaction*, *1*(1), 1–137. Retrieved from https://doi.org/10.1561/1100000004

Isabwe, G. M. N., & Reichert, F. (2013). Revisiting students' privacy in computer supported learning

systems. *International Conference on Information Society (i-Society)*, 256–262.
Ivanova, M., Grosseck, G., & Holotescu, C. (2015). Researching data privacy in eLearning. *2015 International Conference on Information Technology Based Higher Education and Training (ITHET)*, 1–6. Retrieved from https://doi.org/10.1109/ITHET.2015.7218033
Johnston, A., & Wilson, S. (2012). Privacy compliance risks for Facebook. *IEEE Technology and Society Magazine*, *31*(2), 59–64. Retrieved from https://doi.org/10.1109/MTS.2012.2185731
Kaseke, P. (2018). Protect personal data breaches, *Newsday*. Retrieved from https://www.newsday.co.zw/2018/10/protect-personal-data-breaches/
Katurura, M., & Cilliers, L. (2016). The extent to which the POPI Act makes provision for patient privacy in mobile personal health record systems. *2016 IST-Africa Week Conference*, 1–8. Retrieved from https://doi.org/10.1109/ISTAFRICA.2016.7530595
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*(C), 122–134. Retrieved from https://doi.org/10.1016/j.cose.2015.07.002
Krishnan, P., & Vorobyov, K. (2015). ScienceDirect enforcement of privacy requirements. *Computers & Security*, *52*, 164–177.
Kurkovsky, S., & Syta, E. (2011). Monitoring of electronic communications at universities: Policies and perceptions of privacy. *Proceedings of the 44th Annual Hawaii International Conference on System Sciences*, 1–10. Retrieved from https://doi.org/10.1109/HICSS.2011.312
Lawler, J. P., & Molluzzo, J. C. (2011). A survey of first-year college student perceptions of privacy in social networking. *Journal of Computing Sciences in Colleges*, *26*(3), 36–41.
Lawler, J. P., Molluzzo, J. C., & Doshi, V. (2012). An expanded study of net generation perceptions on privacy and security on social networking sites (SNS). *Information Systems Education Journal*, *10*(1), 21–36.
Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*(C), 32–44. Retrieved from https://doi.org/10.1016/j.chb.2018.01.028
Morton, A., & Sasse, A. M. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences: A Q methodology study of users' ranking of privacy, security & trust cues. *PST2014 International Conference on Privacy, Security and Trust Proceedings*, (April), 1–10. Retrieved from https://www.researchgate.net/publication/324167424%0ADesperately
Mudzingwa, F. (2008). HIT hacked again? More than 3 500 student cccount credentials leaked [Blog post]. Retrieved from https://www.techzim.co.zw/2018/05/hit-hacked-again-more-than-3-500-student-account-credentials-leaked/
Mulligan, D. K., Koopman, C., Doty, N., & Mulligan, D. K. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy subject areas. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 1–17. Retrieved from https://doi.org/http://dx.doi.org/10.1098/rsta.2016.0118
Nwaeze, A. C., Zavarsky, P., & Ruhl, R. (2018). Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011. *2017 12th International Conference on Digital Information Management (ICDIM)*, 98–102. Retrieved from https://doi.org/10.1109/ICDIM.2017.8244644
OAIC. (2015). *Privacy management framework*, 1–4. Retrieved from https://www.oaic.gov.au/resources/agencies-and-organisations/guides/privacy-management-framework.pdf
OECD. (2013). Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data. The OECD Privacy Framework § (2013) 11-37. Retrieved from https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2016). Data protection compliance regulations and implications for smart factories of the future. *12th International Conference on Intelligent Environments (IE'16)*, 40–47. Retrieved from https://doi.org/10.1109/IE.2016.15

Rasmussen, C., & Dara, R. (2014). Recommender systems for privacy management: A framework. *IEEE 15th International Symposium on High-Assurance Systems Engineering Recommender*, 243–244. Retrieved from https://doi.org/10.1109/HASE.2014.43

Republic of Zimbabwe. (2013). Zimbabwe' s Constitution of 2013, www.constituteproject.org § (2013). Retrieved from https://www.parlzim.gov.zw/component/k2/download/1290_da9279a81557040d47c3a2c27012f6e1

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers and Security*, *27*(7–8), 241–253. Retrieved from https://doi.org/10.1016/j.cose.2008.07.008

Robbins, J., & Sabo, J. (2006). Managing information privacy: Developing a context for security and privacy standards convergence. *IEEE Security and Privacy Magazine*, *4*(4), 92–95. Retrieved from https://doi.org/DOI: 10.1109/MSP.2006.98

Santanen, E. (2018). The value of protecting privacy. *Business Horizons*, *62*(1), 5–14. Retrieved from https://doi.org/10.1016/j.bushor.2018.04.004

Sargsyan, T. (2016). The privacy role of information intermediaries through self-regulation. *Internet Policy Review Journal on Internet Regulation*, *5*(4), 1–17. Retrieved from https://doi.org/10.14763/2016.4.438

Stange, C. (2011). Privacy concern and student engagement in the virtual classroom (University of Victoria). Retrieved from https://docplayer.net/13882757-Privacy-concern-and-student-engagement-in-the-virtual-classroom.html

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. Retrieved from https://doi.org/10.1016/j.chb.2012.11.022

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, *34*(1), 134–153. Retrieved from https://doi.org/10.1016/j.clsr.2017.05.015

Vail, M. W., Earp, J. B., & Antón, A. I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management*, *55*(3), 442–454. Retrieved from https://doi.org/10.1109/TEM.2008.922634

Yudof, M. (2013). *Privacy and Information Security Initiative Steering Committee Report to the President*, 1–43. Califonia, USA.

Zimbabwe Constitution Parliamentary Committee. (2013). *The Constitution of Zimbabwe Amendment (No. 20) Act, 2013*. , 51 § (2013).

Zimbabwe Data Protection Bill. (2013). *The Zimbabwe Data Protection Bill Draft.* Retrieved from https://t3n9sm.c2.acecdn.net/wp-content/uploads/2016/08/Zimbabwes-Draft-Data-Protection-Bill-v-1-June-2013.pdf