Validation of an Information Privacy Perception Instrument at a Zimbabwean University

Kudakwashe Maguraushe, Adéle Da Veiga, Nico Martins

Validation of an information privacy perception instrument at a Zimbabwean university

Kudakwashe Maguraushe [1] [0000-0003-2405-564X], Adéle da Veiga [2] [0000-0001-9777-8721], and Nico Martins [3] [0000-0002-6103-0217]

School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
[1]kmagraushe@gmail.com, [2]dveiga@unisa.ac.za, [3]martin@unisa.ac.za

Abstract
Privacy issues extend to students as universities acquire and use their personal information for various reasons. This research study was aimed at determining the awareness, expectations and confidence levels of students when the university processes their personal information. The research was also aimed at validating the Information Privacy Perception Survey (IPPS) instrument. The instrument was designed based on the Fair Information Practice Principles, incorporating privacy principles and guidelines from the Organisation for Economic Cooperation and Development's Protection of Privacy and Transborder Flows of Personal Data document, the General Data Protection Regulation and the Zimbabwe Data Protection Act bill. A survey research strategy was used following a quantitative research design where data were collected from 287 students at a selected university using a convenience sampling method. The IPPS instrument was validated using exploratory factor analysis. Seven factors resulted; university confidence, privacy expectations, individual awareness, external awareness, privacy education, practice confidence and correctness expectations. The IPPS can be used by universities to establish the level of awareness and confidence students have regarding how their privacy is upheld by the university. The results show the areas of improvement in the university's privacy practices to create an environment that instils and favours upholding the privacy of students' personal information. Aspects for improvement can be integrated in the university's awareness programmes or policies.

Keywords: Privacy, personal information, expectations, awareness, confidence, questionnaire

1 Introduction

Privacy of personal information differs from country to country and many nations now have privacy laws aligned to the international privacy principles [1]. This research focuses on privacy expectations, student privacy awareness and confidence levels of students in universities' capability to uphold privacy values. The protection of privacy within the Zimbabwean context is partly enshrined in the constitution, although there is no prescription on how it will be executed and enforced [2]. This led to the drafting of the Zimbabwe Data Protection Act (ZDPA) bill with the objective of guiding and

protecting the privacy of personal information of individuals/people and organisations/institutions [3], [4].

Many studies have been carried out on privacy, privacy breaches and concerns, privacy compliances, privacy culture, privacy practices, privacy and trust, privacy when online, privacy in eLearning environments, and all this was done in industries, the health sector, for consumers and for employees of organisations [5]–[9]. According to [10], it is not easy and clear as yet within the Zimbabwean context to comprehend the privacy expectations of students, their privacy awareness levels and their confidence in the university's ability to uphold the privacy of their personal information.

The objectives of this research were to determine the awareness, expectations and confidence levels of students when the university processes their personal information and to validate the Information Privacy Perception Survey (IPPS) instrument using factor and item analysis.

2 Background

Privacy has been defined [11] in terms of the confined mentality of individuals that it is always limited to the ability to access personal data and the impact of self-disclosure, especially on the internet. This is in line with the privacy definition that privacy is "the ability of an individual to control the terms under which their personal information is acquired and used" [12]. Privacy of students personal information at universities is now equally important, especially in the digital context where information can be collected anytime from anywhere [13]. According to research [10], it is important that a university has measures that help in improving students' personal information protection after grasping their awareness, expectations and confidence levels in privacy-related issues.

2.1 Privacy awareness

Students' awareness of their privacy rights, university privacy policies and university awareness programmes is prudent. Awareness provides a perception about a situation, similar to notice, which is one of the fundamental Fair Information Practice Principles (FIPPs) for information privacy [14]. The awareness is normally concealed through privacy notices by the university [14]. So it follows that students, as users, also need to be aware of the importance of awareness about their privacy rights and university privacy policies, especially when using electronic means [15]. University compliance with the privacy policies, as alluded to by [16] and [17], goes hand in hand with awareness because a lack of awareness means that a user is not privy to the finer details needed to comply, which may result in non-compliance with privacy issues even by the student. Research [18] has shown that awareness of privacy can also be used in creating an atmosphere where all students are knowledgeable about all privacy-related issues, which also assists in their participation in university-related tasks. This must be initiated by universities through the use of privacy policies and other awareness means. As acclaimed by [17], institutions are indebted in making sure that students are aware of

the legal, moral and ethical expectations when they share their personal information and one way of accomplishing that is through countless and timeous awareness campaigns.

Awareness is typically conducted within organisations (universities) through privacy notices [14]. Research results [19] indicated students' lack of knowledge in appreciating privacy awareness within universities. Awareness is deemed a precondition for achieving compliance, as indicated by [20]. Results [21] also indicated that compliance to laws, privacy policies and privacy concerns are an end product of appropriate awareness lineups in organisations. Universities need to stimulate privacy awareness, which permits students to consent, particularly when handling personal information [22]. The Zimbabwean constitution declares that it is the prerogative of the data controller (university, in this case) to propagate and publicise knowledge, and hence awareness, to students [8].

2.2 Privacy expectations

FIPPs claim that individuals (students) expect privacy of their personal information [23]. There is an expectation that the collection of personal information will be as minimal as possible and relevant to the purpose of collection, even when there is a requirement that the organisation (university) acquire personal information and process it [23]. Research results [6] point to the fact that consumers regard organisations (institutions) with expectations of privacy when they process their personal information. In the event that the consumers (students) start to perceive the organisation (university) as having shortfalls in meeting their privacy expectations, they tend to become impassioned and consequently and might reject personal information sharing with the data collector (university) [24].

2.3 Privacy confidence

It was proved that sometimes students do not have a need to seek documentation related to privacy from the university because they have full confidence in their institutions upholding privacy [7]. According to [25], a sense of trust that implants confidence is strengthened if universities make privacy pledges which will eventually create a privacy culture that saturates the whole university as an institution. Research [26] corroborated by [27] indicated that trust is an element of confidence, which is to be tested within this research to validate its relevance for students'expectations and awareness. This implies that if privacy regulations and protection are improved and prioritised, the confidence levels of the users (students) will increase proportionally [28]. The lack of trust in using personal information can have negative implications like low confidence levels of students in the university [26], [29]. This was also emphasized by [27], which indicated that it would have undesirable retrogressive consequences. Low confidence levels in the business (university) by customers (students) can be a result of data and privacy breaches [30]. In the end, it is the mandate of the university to come up with privacy policies and make the students knowledgeable about it in a bid to increase confidence and compliance with the privacy policies [31]. The

implementation of an information privacy culture within institutions inspires trust and hence confidence as attested by [29].

3 Methods

This research study was conducted using a survey research strategy in a deductive approach of a quantitative research design. The questionnaire survey was used as a research method to gather information on students' perceptions and behaviour [32]. In terms of ethics [33], surveys tend to have the advantage of not exposing participants as it can be anonymous. The online distribution of a questionnaire is fast, inexpensive, with moderately faster turnaround time, easier administration and easy follow-ups, which all help to increase the reliability of the instrument since many responses reveal more detail [34]. Furthermore, most quantitative research adopts the survey design, as posited by [35]. Online surveys were chosen and according to [35], surveys are efficient and effective when the respondents are all information technology literate and have access to the internet, like in the case of students in this research.

3.1 Questionnaire

The quantitative IPPS instrument was developed with a set of 54 items based on a theoretical framework [10], all perceived to be of similar value, to which the respondents responded by agreeing or disagreeing with each item or statement. A five-point Likert scale was used with options being strongly disagree, disagree, do not disagree or agree, agree and strongly agree. After using theories from the literature to design the statements, the statements were subjected to a process of expert panel review. The experts assisted by undertaking a focused and comprehensive review of the questions, structure of the questionnaire and its suitability, and provided feedback or made recommendations [35], [36]. The expert review panel consisted of four people with experience in privacy consultancy, data protection, privacy compliance and privacy advisory services. The experts recommended the restructuring of some questions for clarity and some statements which were deemed inessential were adjusted.

After the expert review, the instrument was used with a total of 15 students in a pilot study. The purpose was to make sure that the statements were clear, easily understood and comprehensive. A pilot study helps in assessing if the questions are comprehensible to the targeted audience, ensuring that the instrument used in the study is reliable and valid measures of the constructs of interest (i.e. face and construct validity) [37]. After the pilot study, the time was reduced from 20 to 15 minutes. Also, clarity was added to reduce the notion that some questions were repeated, since each statement was assessed from the three dimensions of awareness, expectations and confidence. A statement was consequently added to the instrument to this effect.

In the design of the IPPS, an introduction with a preface and some privacy definitions used in the research study were included in the front section. The research instrument was divided into two sections that would assist in achieving the stated purpose of the study: Section 1: Biographical Information and Section 2: Personal information privacy

– Awareness, expectations and confidence questions. Section 1 required personal information such as the age, gender, nationality, learning mode, year of study and programme. Section 2 contained nine components of the questionnaire. Each was measured in terms of the three dimensions (i.e. awareness, expectations and confidence). The nine components used the FIPPs as the baseline and were underpinned in the OECD's Protection of Privacy and Transborder Flows of Personal Data document of 2013, the General Data Protection Regulation and the Zimbabwe Data Protection Act [10].

3.2 Sampling

Students at a university in Zimbabwe were selected as the sample by virtue of them being registered students. The sample size was derived using the rule of thumb suggested by [32], multiplying the five-point scale with the number of items in the questionnaire in order to have enough responses to statistically validate the questionnaire. This gives the minimum number of responses expected from the respondents in the research. For the sample size, 270 was the minimum number of students required to participate. A non-probability sampling technique was used for the survey. The researchers chose purposive sampling for the selection of experts to participate in the expert panel research on the survey questions. The experts were recruited based on their expertise in the field of information privacy. The researchers also chose convenience sampling for the pilot study participants because it allows for a quicker way of obtaining the data since the researcher picks "whomever is convenient as a participant in the study" [38]. For the final survey, the convenience sampling method was considered the most appropriate [35], [39]. Two hundred and seventy eight students participated in the survey, which was an adequate sample. The researcher recruited the participants by means of a presentation to the students highlighting the purpose of the research and also seeking their participation. Participation in the research was voluntary, anonymous and confidential.

3.3 Questionnaire administration

In this research study, an invitation with a hyperlink to the html questionnaire was sent to the respondents through email as the primary method for sending out the survey. Hard-copy questionnaires were provided to some students who indicated their unavailability on the internet. The estimated completion time for the questionnaire was approximately 15 minutes and the collection period was five weeks. The electronic/online IPPS was administered using the Survey Tracker software [40]. There was a "Yes" and a "No" button to the questionnaire where the students could click on "Yes" if they consented to continue to participating and move to the next page or "No" if they no longer wanted to participate and it would move to the last page.

3.4 Data analysis

The data analysis was done using SPSS version 25 for the descriptive statistics per subscale (such as the means and standard deviations) and for the questionnaire

validation using the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's Test of Sphericity (BTS), factor analysis and Cronbach alpha analysis.

4 Results

The results of the responses per age band are shown in Table 1.

Table 1: Survey responses

Response	**Frequency**	**Percentage**
1996–2019	67	23.3
1977–1995	177	61.7
1965–1976	41	14.3
1946–1964	1	0.3
Born 1945 or earlier	1	0.3
No response	0	0.0

Of the 287 responses, 143 were female and 140 male respondents with four who selected the "Other" option. 284 were Zimbabweans and three were from other African countries.

4.1 Validation of measurement instrument

The collected data was first subjected to the KMO to measure the sampling adequacy and the BTS to ascertain the presence of correlations and significance among the variables [41]. The BTS is considered significant at the level of $p < 0.05$ [41].

Table 2: Test for sample adequacy and significance

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.647
Bartlett's Test of Sphericity	Approx. Chi-Square	231.517
	df	6.000
	Sig.	0.000

In this research, a KMO value of 0.647 was obtained – greater than the threshold value of 0.60 postulated by [41], [42], implying that there was a strong correlation structure. The BTS was significant at $p < 0.00$ for overall significance for the awareness, expectations and confidence concepts, adding further evidence of sampling validity and the conduct of exploratory factor analysis (EFA). The value showed that a meaningful factor analysis could be conducted, as attested to by [43].

4.2 Factor analysis

The IPPS was subjected to the EFA using the principal axis factoring with Oblimin rotation with Kaiser normalisation. The rotated pattern matrix for the 54-item instrument is shown in Table 3 in Appendix A.

In research, items with factor loadings that are less than the agreed threshold (≤ 0.40) [43] and those with cross loadings that are high (with < 0.20 difference) in a single factor are eliminated. In this research, items with lower factor loadings but above the cut-off loading included items 11, 23, 26, 27, 36, 38, 39, 45, 58 and 59. They were all retained except item 59, which had a cross loading together with item 41 which were excluded. Factor 6 had two items and therefore it was excluded. Furthermore, the Cronbach alpha of factor 6 was very low (0.225), which falls outside the cut-off Cronbach value (≥ 0.7).

The new factors were labelled based on the items in the respective factors. The Cronbach alpha measures the internal consistency of a scale [43]. The Cronbach alpha values for the new factors, number of items and the Cronbach alpha are shown in Table 4 below.

Table 4: Cronbach alpha values for the new factors

Factor/Dimension	**Number of items**	**Cronbach alpha**
Factor 1: University confidence (UC)	8	0.922
Factor 2: Privacy expectations (PE)	7	0.789
Factor 3: Individual awareness (IA)	5	0.820
Factor 4: External awareness (EA)	3	0.807
Factor 5: Privacy education (PE)	4	0.737
Factor 6 (eliminated factor)	2	0.225
Factor 7: Practice confidence (PC)	8	0.917
Factor 8: Correctness expectations (CE)	6	0.781
Total	**43**	

The final seven factors had Cronbach alpha coefficient values that were higher than 0.7, which indicated that there was a strong item covariance [32], [35] of between 0.7 and 0.9, rendering the values adequate as posited by [34]. This resulted in the Cronbach alpha values being considered suitable and adequate for the purpose of this study. The Cronbach alpha values for factor 6 (eliminated factor) was very low, with a loading of 0.225, and thus it was removed. An extract of the questionnaire statements per factor is shown in Table 5.

Table 5: Questionnaire statements extract for the new factors

New Factor	Statement	Component examined
University Confidence	I am confident that the university has reasonable justification (e.g. consent, a contract, legal requirement) for processing my personal information.	Use limitation
	I am confident that the university's privacy notice is easy to understand.	Notice/ openness
Privacy Expectations	I expect my personal information not to be disclosed, made available or used, unless it is in line with the law.	Use limitation
	I expect the privacy policy to be easily understood.	Privacy policy
Individual Awareness	I am aware that I should be able to request copies of the records of my personal information from the university.	Individual participation
	I am aware that the university should have a process whereby I can request whatever personal information the university has collected about me.	Individual participation
External Awareness	I am aware that the university should specify the purpose of collecting my personal information.	Purpose specification
	I am aware that the purpose should be specified no later than at the point of collection.	Purpose specification
Privacy Education	I am aware that the university should, as part of best practice, conduct privacy training for students.	Privacy education
	I expect the university to conduct privacy training for students.	Privacy education
Practice Confidence	I am confident that the university conducts privacy training for students.	Privacy education
	I am confident that the privacy policy is easily understood.	Privacy policy
Expect Correctness	I expect the university to take reasonable steps to ensure that my personal information processed by them is correct (e.g. accurate, up to date, complete and relevant) for the purpose of collection.	Information quality
	I expect the university to specify the purpose of collecting my personal information.	Purpose specification

4.3 Means and standard deviations of the factors interpretation

Research conducted by [44] used an average of 4.0 as a threshold for distinguishing between positive and potential negative perceptions given the importance of privacy and information security together with the legal requirements for privacy, and this was used as a baseline for this research. Table 6 shows the mean and the standard deviation values for the final seven factors.

Table 6: Mean and standard deviation values for the final seven factors

Descriptive statistics					
Factor	**N**	**Min**	**Max**	**Mean**	**Std deviation**
University confidence	287	1.25	5.00	3.5740	0.90282
Privacy expectations	287	2.86	5.00	4.5610	0.41050
Individual awareness	287	1.80	5.00	4.0774	0.75485
External awareness	287	1.67	5.00	4.1429	0.77054
Privacy education	287	1.75	5.00	4.1254	0.73406
Practice confidence	287	1.63	5.00	3.4194	0.88332
Correction expectation	287	2.33	5.00	4.5296	0.45205
Valid N (listwise)	287				

Using the cut-off value adopted from [44] as the baseline, the following were observed:

- A mean value of 4.56 was recorded for the privacy expectations (factor 2), which is more than the cut-off value of 4.0 prescribed. It shows that students had positive perceptions about how the university handled and used their personal information.
- Correction expectation (factor 8) showed a mean value of 4.53, which was also considered to be highly positive in terms of students' perceptions.
- External awareness (factor 4) recorded a mean value of 4.14. This also shows positive perceptions.
- Privacy education (factor 5) recorded a mean value of 4.13, which is also above the cut-off value. This also shows positive perceptions of students.
- Individual awareness (factor 3) recorded a mean value of 4.08, showing slightly positive perceptions of students.
- University confidence (factor 1) scored 3.57, which is lower than the cut-off mean value. This shows that the perceptions of confidence and the confidence in the university could be improved.
- The lowest mean value was recorded under practice confidence (factor 7) with a value of 3.43. This represents the most negative dimension, for which improvement was required.

From the results, it can be drawn that privacy expectations and correction expectation are meaningful factors which are pivotal for the development of personal information privacy for a university, resulting in students developing confidence with the university in upholding the privacy of their personal information.

5 Discussion

The results show that the students had both positive and negative perceptions about how the university handled and used their personal information. Based on the research instrument used, the students had positive perceptions and expectations of privacy components like the use limitation, privacy policy, collection limitation, consent and notice/openness privacy components. These included the expectation and awareness that the university would justify the need for information collection and processing, confidence to be given, the provision to review collected personal information, confidence in the existence of the publishing privacy notices and privacy policy, and that these would be easy to comprehend.

The students had positive perceptions on the correction expectations. This focused on students' expectations of the university, on how the university had to come up with privacy policies and notices that were easily understandable, that the university would only use students' personal information for extreme scenarios like legal requirements and that this would be done with the students' consent. They expected the university to justify the collection and processing of their personal information, the information should not be just disclosed. Students also seemed to be aware of what they needed to do individually to uphold the privacy of their personal information. Individual awareness recorded positive perceptions by students in terms of consent, use limitation and individual participation. These included being aware of when to opt in for the use of their personal information, their rights to opt out in case they no longer chose to share their personal information and being aware that they had the right to decide who to share their personal information with.The university can focus on increasing the students' individual awareness levels by engaging in privacy training sessions, sending short message service (sms) or emails, letters and other notices.

External awareness also showed positive perceptions. This revealed perceptions about students' awareness levels in specifying the purpose of collection and the limitations of information use thereof. Students seemed to be aware and expected the university to remind them continuously of privacy-related issues through privacy newsletters, magazines, notices and so on as part of privacy best practices. Students were aware and expected the university to conduct privacy training to increase their privacy awareness.

The results showed that practice confidence was an area needing improvement, especially in terms of how to handle consent, privacy education, individual participation and privacy policy. Another area of improvement could be the university's privacy practices in creating an environment that favours the upholding of privacy of personal information. The university has to improve and create an environment that instils student confidence in the university regarding privacy.

The contribution is the identification of the factors and validation of the questionnaire. Further more the questionnaire can aid univeristies to identify how to further improve student awareness about privacy to be in line with their expectations. This will ultemately aid in better protection of student personal information also aiding in addressing concerns for information privacy amongst students.

6 Limitations and future research

This research was conducted on one institution. In future, research will aim to extend the study to wider sample of universities. There is also need to validate the conceptual framework using structural equation modelling (SEM).

7 Conclusion

An IPPS questionnaire was developed for this research to measure the expectations, awareness and confidence of students in the university upholding the privacy of their personal information. After the questionnaire was used at a university in Zimbabwe, the data obtained was used to validate it by means of the EFA. The results from the validated instrument led to the formulation of seven new factors. The questionnaire can be used by other universities to measure and improve the privacy awareness and confidence based on the expectations of students thereby aiding to improve the protection of personal information

Acknowledgement - The researchers are grateful to Organisational Diagnostics for hosting the survey and Liezel Korf Associates for assisting in the statistical analysis. This research paper is wholly supported by Unisa's Master's and Doctoral Research Bursary funding.

Appendix A

Table 3: Rotated pattern matrix for the eight-factor model

Item number	Factor							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
q30	0.77							
q19	0.76							
q18	0.73							
q24	0.62							
q31	0.62							
q13	0.60							
q25	0.60							
q12	0.56							
q28		0.63						
q29		0.60						
q46		0.59						
q47		0.58						
q34		0.54						

Item Number	1	2	3	4	5	6	7	8
q58		0.44						
q11		0.42						
q56			-0.89					
q57			-0.87					
q27			-0.46					
q38			-0.45					
q39			-0.44					
q20				-0.80				
q21				-0.68				
q26				-0.47				
q59			-0.40	0.47				
q51					0.70			
q50					0.70			
q52					0.58			
q53					0.56			
q41		0.46				0.61		
q40						0.56		
q36						0.40		
q61							-0.84	
q54							-0.81	
q60							-0.80	
q55							-0.74	
q43							-0.65	
q49							-0.58	
q48							-0.54	
q42							-0.53	
q16								-0.75
q22								-0.63
q17								-0.58
q14								-0.53
q23								-0.48
q45								-0.45

Extraction method: Principal axis factoring
Rotation method: Oblimin with Kaiser normalization

a. Rotation converged in 25 iterations

References

[1] D. L. A. Piper (2020) Data protection laws of the world, Attorney Advertising, [Online]. Available: https://www.dlapiperdataprotection.com/index.html.

[2] Republic of Zimbabwe (2013) Constitution of the Republic of Zimbabwe 2013.

[3] Chetty P (2013) Presentation on Zimbabwe Data Protection Bill, Harmon. ICT Policies Sub-Sahara Africa.

[4] Zimbabwe Data Protection Act Bill (2013) The Zimbabwe Data Protection Act Bill. Harare, Zimbabwe, pp. 1–47.

[5] Ivanova M, Grosseck G, Holotescu C (2015) Researching data privacy in eLearning, in 2015 International Conference on Information Technology-Based Higher Education and Training (ITHET), pp. 1–6.

[6] Da Veiga A (2018) An information privacy culture instrument to measure consumer privacy expectations and confidence, Inf. Comput. Secur., vol. 26, no. 3, pp. 338–364.

[7] Stange C (2011) Privacy concern and student engagement in the virtual classroom, Univ. Victoria, pp. 1–73.

[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, vol. 34, no. 4, pp. 157–170.

[9] Katurura M, Cilliers L (2016) The extent to which the POPI Act makes provision for patient privacy in mobile personal health record systems, in Conference, IST-Africa 2015, pp. 1–8.

[10] Maguraushe K, Da Veiga A, Martins N (2019) A conceptual framework for a student personal information privacy culture at universities in Zimbabwe, Kalpa Publ. Comput., vol. 12, pp. 143–156.

[11] Miltgen CL (2009) Online consumer privacy concerns and willingness to provide personal data on the internet, Int. J. Netw. Virtual Organ., vol. 6, no. 6, p. 574.

[12] Schwaig SK, Kane GC, Storey VC (2006) Compliance to the fair information practices : How are the Fortune 500 handling online privacy disclosures? Inf. Manag., vol. 43, no. 7, pp. 805–820.

[13] Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Comput. Secur., vol. 64, pp. 122–134.

[14] Vail MW, Earp JB, Antón AL (2008) An empirical study of consumer perceptions and comprehension of web site privacy policies, IEEE Trans. Eng. Manag., vol. 55, no. 3, pp. 442–454.

[15] Kyobe M (2010) Knowledge management using information technology: Ethical and legal issues in a university, Inf. Soc. Int. Conf., pp. 592–597.

[16] Botha JG, Eloff MM, Swart I (2015) The effects of the POPI Act on small and medium enterprises in South Africa, 2015 Inf. Secur. South Africa – Proc. ISSA 2015 Conf..

[17] Kyobe M (2010) Towards a framework to guide compliance with IS security policies and regulations in a university, Proc. 2010 Inf. Secur. South Africa Conf. ISSA 2010.

[18] Fink C (2012) Privacy and confidentiality in the virtual classroom : Instructor

perceptions, knowledge and strategies.
[19] Chen LF, Ismail R (2013) Information technology program students' awareness and perceptions towards personal data protection and privacy, in International Conference on Research and Innovation in Information Systems (ICRIIS), vol. 2013, pp. 434–438.
[20] Aghasian E, Garg S, Gao L, Yu S, Montgomery J (2017) Scoring users' privacy disclosure across multiple online social networks," IEEE Access, vol. 5, pp. 13118–13130.
[21] Nwaeze AC, 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 Int. Conf. Digit. Inf. Manag. ICDIM 2017, vol. 2018–Janua, no. Icdim, pp. 98–102.
[22] Isabwe GMN, Reichert F (2013) Revisiting students' privacy in computer supported learning systems, in International Conference on Information Society (i-Society), pp. 256–262.
[23] Cate F (2006) The failure of fair information practice principles, in Conference on Consumer Protection in the Age of the Information Economy, pp. 341–378.
[24] Morton A, Sasse AM (2014) Desperately seeking assurances: Segmenting users by their information-seeking preferences A Q methodology study of users' ranking of privacy, security & trust cues, in PST2014 International Conference on Privacy, Security and Trust Proceedings. IEEE, April, pp. 1–10.
[25] Alnatheer M, Chan T, Nelson K (2012) Understanding and measuring information security culture, in Pacific Asia Conference on Information Systems (PACIS), vol. 144, no. 12, pp. 1–15.
[26] Dwyer N, Marsh S (2016) How students regard trust in an elearning context, in 14th Annual Conference on Privacy, Security and Trust, PST, pp. 682–685.
[27] OECD (2013) Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, no. C(2013)79, pp. 11–37.
[28] BSA (2018) BSA privacy framework, The Software Alliance, pp. 1–2.
[29] OAIC (2015) Privacy management framework. Office of the Australian Information Commissioner, pp. 1–4.
[30] Bush D (2016) How data breaches lead to fraud, Network Security. pp. 11–13.
[31] Kurkovsky S, Syta E, "Monitoring of electronic communications at universities: Policies and perceptions of privacy," in Proceedings of the 44th Annual Hawaii International Conference on System Sciences, 2011, pp. 1–10.
[32] Gerber H, Hall R (2017) Quantitative research design. HR Statistics, Pretoria, pp. 1–64.
[33] Mathers N, Fox N, Hunn A (2009) Implementing adminstrative surveys and questionnaires.
[34] Creswell JW, Creswell JD (2018) Research design: Qualitative, quantitative and mixed methods approaches, 5th ed. Los Angels, USA: Sage Publications.
[35] Saunders M, Lewis P, Thornhill A (2016) Research methods for business students, 7th ed. Essex, England: Pearson.
[36] Kumar R (2011) Research methodology: A step-by-step guide for beginners, 3rd Editio. London: Sage Publications.
[37] Bhattacherjee A (2012) Introduction to research, social science research:

Principles, methods, and practices.
[38] Jackson SL (2009) Research methods and statistics: A critical thinking approach.
[39] Salkind NJ (2017) Exploring research, 9th ed. Essex, England: Pearson Education Limited.
[40] Scantron, Online & paper survey management – SurveyTracker,. [Online]. Available: https://www.scantron.com/assessment-solutions/surveys/online-paper-survey-management-survey-tracker-plus/#surveytracker-plus. [Accessed: 15 April 2020].
[41] Gie A, Pearce S, "A beginner's guide to factor analysis: Focusing on exploratory factor analysis," 2012.
[42] O'Rourke N, Hatcher A (2013) A step-by-step approach to using SAS for factor analysis and structural equation modelling. Cary, NC.
[43] Hair JF, Black WC, Babbin BJ, Anderson RE (2014) Univariate data analysis, 7th ed. Essex, England: Pearson Education Limited.
[44] Da Veiga A, Martins N (2014) Information security culture : A comparative analysis of four assessments.