Kudakwashe Maguraushe, Adéle da Veiga & Nico Martins (2024) A personal information privacy perceptions model for university students, Information Security Journal: A Global Perspective,
https://doi.org/10.1080/19393555.2024.2329554

Pre-print version

A personal information privacy perceptions model for university students

Kudakwashe Maguraushe[a]*, Adéle da Veiga[b] and Nico Martins[c]
[abc] School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Johannesburg, South Africa
*Corresponding author: Dr K. Maguraushe, kmaguraushe@gmail.com

ORCID:
Dr K. Maguraushe: 0000-0003-2405-564X
Prof. A. Da Veiga: 0000-0001-9777-8721
Prof. N. Martins: 0000-0002-6103-0217

A personal information privacy perceptions model for university students

Abstract: This study aims to address the lack of personal information privacy policies in Zimbabwean universities by proposing and validating a Student Personal Information Privacy Perception (SPIPP) model. The model helps institutions understand and implement data privacy principles based on students' perceptions. The students' perceptions were determined for the following privacy constructs: privacy awareness; privacy expectations; and student confidence in the university's data privacy practices. In this study, a quantitative research method using a cross-sectional survey with a closed-ended questionnaire was adopted to collect data from 284 student participants. To refine the preliminary instrument, an expert review and pilot study were conducted. The privacy model was validated using confirmatory factor analysis (CFA) and structural equation modelling (SEM). Seven new factors emerged from the validation of the instrument: university confidence; practice confidence; individual awareness; privacy awareness; external awareness; privacy expectations; and correctness expectations. SEM showed a good overall match between the suggested conceptual model and the empirically derived model. The validated questionnaire that was developed can be used by universities to ascertain students' perceptions of privacy to create a culture of privacy and to protect student data in line with regulatory requirements and best practices.

Keywords: awareness; confidence; expectations; personal information; privacy

1. Introduction

Personal information privacy is a growing concern in the digital era (Hallam and Zanella, 2017) and has significant implications for students at universities. To reduce the impact of privacy concerns, much emphasis must be placed on students and their preparedness to share sensitive personal information (Kim et al., 2019). Student privacy concerns need to be clearly understood and effectively managed within a university setting (Kizilcec et al., 2023). Thus, the privacy concerns raised by students about how universities handle and process their personal information must be considered a priority (Das, 2022; De Wolf et al., 2023). Privacy concerns occur when individuals are concerned about how their personal information is handled by responsible parties (Da Veiga and Ophoff, 2020). As a solution, Stange (2011) proposes that understanding the privacy of students' personal information should be a precondition for endorsing engagements and development plans. In a university setting, personal information privacy requires careful observation and understanding, and assimilation of students' privacy concerns is critical because it directs the expected behaviour of individuals within an organisation (university) (Da Veiga and Martins, 2015).

In Europe, the Data Protection Officers (DPO) Handbook elaborates on how the General Data Protection Regulation (GDPR) should be implemented as a way of guiding the public sector and ensuring compliance (Korff and Georges, 2019). However, there are no clear guidelines for implementing personal information privacy regulatory requirements in developing countries like Zimbabwe (Chetty, 2013; Ncube, 2016). Indeed, it might not be the purpose of the legislation to give instructions on how regulatory requirements should be applied in an institutional context but specific compliance requirements can be given, like in the case of a record of processing activities within the GDPR (Boardman et al., 2020). Studies (Fortes and Rita, 2016; Kruikemeier et al., 2020) have shown that individuals do not necessarily trust or have faith in institutions that process their personally identifiable information following privacy principles and norms. Similarly, students may lack faith or confidence in an institution's ability to protect their privacy, particularly if no implementation rules exist. Additionally, the existence and upsurge of violations of privacy within the digital realm are a major concern and ultimately a threat to the privacy of students' personal information (Anjum et al., 2018; Mamonov and Benbunan-Fich, 2015; Martin et al., 2020). In fact, privacy is a critical issue that

must be handled sensitively, particularly in today's increasingly digital-dependent society (Fatima et al., 2019). Institutions sometimes do not have clear indications of what to expect in terms of privacy (Degroot and Vik, 2017; Dwyer and Marsh, 2016; Schumacher and Ifenthaler, 2018).

In other jurisdictions, parents have control over what personally identifiable information the school can collect. For instance, the United States of America regulated the Family Educational Rights and Privacy Act (FERPA) to safeguard the personal information privacy of students, with parents in control of certain personally identifiable records of their children (Schrameyer et al., 2016). They can only transfer the rights to their children when they reach 18 years (Cole, 2021). FERPA gives parents and students peace of mind by assuring them that the data used to create school records is reliable, relevant and fair (Zeide and Nissenbaum, 2018). All education institutions have to abide by the regulations, as failure has repercussions that include restrictions on funding (Schrameyer et al., 2016). Unfortunately, such provisions on privacy are not available within the Zimbabwean context, leaving privacy as a prerogative of institutions. The autonomy of students depends greatly on their right to privacy, which makes it an endlessly fascinating and relevant topic (Botnevik and Khalil, 2020).

There are no explicit personal information privacy policies that govern how personal information must be handled and retained by universities in Zimbabwe. Unfortunately, the Zimbabwe Data Protection Act (ZDPA) does not provide instructions on how to carry out the requirements for ensuring the privacy of personal information but instead concentrates on declaring the privacy principles and regulations (Chetty, 2013; Elegbeleye et al., 2022; Ncube, 2016; Republic of Zimbabwe, 2013). It is not the function of legislation to provide instructions on how it may be used in an organisational environment; rather, dispelling privacy worries would be best served by establishing a model that aids privacy practice. Fortunately, using privacy models increases user trust, and compliance, resulting in fewer privacy breaches and incidences (Fox et al., 2022).

The main research question that this research study investigates are: What are the primary components that make up the perceptions of personal information privacy in the setting of Zimbabwean universities? To address this, the main objective of the research is to develop a Student Personal Information Privacy Perception (SPIPP) model that measures three key constructs: awareness, expectations, and confidence in the context of personal information privacy in Zimbabwean universities. The focus of this research is primarily on how university students in Zimbabwe perceive the privacy of their personal information, encompassing their awareness of privacy issues, their expectations regarding the handling and protection of their personal data, and their confidence in the university's ability to safeguard their privacy. In this research, a quantitative research approach was adopted, employing a cross-sectional survey and a closed-ended questionnaire. The study comprised 284 university students who were selected through probability random sampling. To validate the model, confirmatory factor analysis (CFA) and structural equation modelling (SEM) were employed. Before the main survey, expert reviews and a pilot study were conducted to refine the instrument. Statistical analyses were performed using SPSS version 25, incorporating descriptive statistics, explanatory factor analysis (EFA), CFA, and SEM. Additionally, the inter-factor association of the key variables/privacy constructs was analysed using the Pearson product-moment correlation coefficient (PPMCC). This study contributes to the literature by providing an understanding of how students' perceptions of privacy are conceptualised regarding awareness, expectations, and confidence. The empirical contribution of this study is the development of a statistically validated model and questionnaire for privacy perceptions that universities can utilise as part of their privacy program. This validated model is expected to help universities to better understand how students perceive privacy and ensure that when collecting and processing students' information, they meet the expectations for privacy and uphold privacy rights while implementing data protection regulations.

The remaining parts of this article are structured as follows: Section 2 presents a brief background of the study by describing the privacy perceptions of students based on the three privacy constructs of privacy awareness, privacy expectations and privacy

confidence. A discussion of the privacy regulations based on the Fair Information Practice Principles (FIPPs), the Organisation for Economic Cooperation and Development's (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (hereafter referred to as the OECD privacy guidelines), the GDPR and the ZDPA follows. These privacy regulations were used to formulate the privacy components. Section 3 discusses the research design and methodology used in testing the hypotheses. Section 4 presents the findings, where both descriptive and inferential analyses were done, and SEM was used to validate the model. Section 5 presents a discussion of the results and some recommendations, and Section 6 concludes the study.

2. Background of the study and problem conceptualisation

This section discusses privacy perceptions, the privacy paradox, and related studies on privacy models, including within a university context, leading to the statement of the problem and the purpose of the study.

2.1 Privacy perceptions

An imperative prerequisite in the present digital era is knowing and having control over the privacy of your personal information (Dervishi et al., 2022). Individuals' (students') perspectives on sharing sensitive personal information and their readiness to provide such information should be given more attention (Choi et al., 2017). Information privacy is perceived differently in different countries (Chua et al., 2017). The privacy perceptions of millennials, the category into which most students fall, are influenced by awareness and trust (Kuperus, 2016). Students' privacy perspectives can help universities to understand students' views on the privacy of their personally identifiable information. Students' views on privacy are predicted to vary when they are exposed to real-life events and students would prefer institutions to use their personal information predominantly for academic purposes (Future of Privacy Forum, 2021). According to a 2016 EDUCAUSE Centre for Analysis and Research (ECAR) survey, one-third of undergraduate students were concerned that privacy invasion through technology could worsen (Park and Vance, 2021). Furthermore, in a Gallup survey in 2016, 33% of the respondents had less faith in companies safeguarding their personal information (Park and Vance, 2021). Another Gallup survey in 2018 showed that 39% of the respondents between the ages of 18 and 49 years were "very concerned" about privacy invasions (Brooks, 2016). These polls are a testimony of students' increased awareness and mistrust of how institutions handle their personal information. In this study, students' perceptions relating to their awareness, expectations and level of confidence in the university were investigated; these would aid the university in satisfying student privacy standards (Alnatheer et al., 2012), resulting in the development of trust in the university. According to Elegbeleye et al. (2022), a data privacy model can help to safeguard the data better against any privacy breach and reduce the violation of personal information privacy. By assuring the end user of privacy compliance measures, privacy concerns are reduced and trust is fostered; as a result, people are more willing to divulge their personal information (Fox et al., 2022).

2.2 The privacy paradox

This study was also impacted by the emerging phenomenon of the privacy paradox. The privacy paradox is a phenomenon where customers act in a way that is inconsistent with their privacy attitudes or expressed privacy concerns (Bandara et al., 2020; Barth et al., 2019; Gruzd and Hernández-García, 2022). The attitudes toward protecting personal data and behaviour are actually at odds with one another (Muravyeva et al., 2020; Willems et al., 2022). According to the privacy paradox, people act irrationally and fail to act to preserve their privacy despite having legitimate worries (Masur, 2021). Although individuals are worried about their privacy, they tend to share their personal information (Willems et al., 2022), for instance when registering at institutions or accessing online applications. The conception of the privacy paradox is further restricted by the reality that social networking platforms have evolved into an integral part of our everyday lives and function as social actors, even though privacy has become a key issue worth addressing (Kim and Kim, 2020). The students struggle with how to balance their worries about the protection and handling of their personal information with their behaviour in willingly disclosing such information (Bentinck et al., 2020), especially when doing so online, and their failure to secure their personal information. Employees at the university are aware that

they must gather students' personal data for processing and that the collection must be restricted to predetermined goals. As a result, a paradox regarding privacy is produced (Martin, 2020). The university's efforts to collect as much data from students as possible for usage are at odds with the requirement for maintaining students' privacy, which Cloarec (2020) laments.

2.3 Conceptualisation of the problem

This section discusses the existing related privacy models from a broader privacy scale, as well as some universities that have compliance privacy models. It also summarises the statement of the problem and the research questions and objectives.

2.3.1 Related work

Kyobe (2010) created a framework that could be applied in a university setting to ensure compliance with information security regulations. The study suggested that existing controls be employed following the legal requirements because awareness was seen as one of the issues with compliance. The framework, unfortunately, provided direction for information security compliance in general and not privacy specifically. In another study on measuring privacy issues for mobile users, a new privacy model was created (Xu et al., 2012). Although users' perceptions were incorporated, it was only applicable in the context of mobile devices. A privacy model was also created by Samani et al. (2015), for the investigation of privacy ideas and issues, but the model's application was restricted to Internet of Things (IoT) technologies. As a result, it addressed the protection of personal information when operating IoT applications only. Martinet al. (2015) produced a 29-item questionnaire on the privacy of personal information with a greater focus on disclosure, storage, awareness, use and collection-related problems. They also created a conceptual framework that could help in achieving the privacy of personal information. The goal of their instrument and model was to consider how internet users felt about the privacy of their personal information. Since it was designed solely for a small sample, Martin et al.'s (2015) instrument could not be used for this study because it does not examine student perceptions from the awareness, expectations, and confidence perspectives. Victor et al. (2016) also attempted to analyse privacy models, although their model was restricted to large data privacy in the digital age. Furthermore, their conceptual model is vague about how to deal with students' perspectives and how the research's themes related to trust and confidence. Harborth and Pape (2020) employed the Internet Users Information Privacy Concerns, a paradigm that has been popular among scholars studying privacy issues. However, the instrument and model are not the best for measuring student perceptions of privacy because their primary focus was the assessment and analysis of online users' privacy concerns.

In summary, several researchers with a focus on privacy have developed privacy models and, to some extent, privacy instruments. Unfortunately, they only fit within specific defined scopes and situations, hence the models that had been established could not be used in this research. This study also could not use these models because many of them were not based on FIPPS or some other legal requirements for privacy. Consequently, a new privacy model had to be created for this study. This research used the local ZDPA and internationally recognised FIPPs, the OECD privacy regulations and the GDPR privacy principles.

2.3.2 Statement of the Problem

In the Zimbabwean context, there are currently no privacy guidelines to assist organisations and institutions to implement the privacy regulations in practice and complying with them. This is exacerbated by the fact that students in Zimbabwe are not aware of the best practices for how their personal information is protected, exposing them to various cyber-related attacks, as pointed out by Mutunhu et al. (2022). The ZDPA and the constitution are insufficient to provide organisations with instructions for implementing personal information privacy. The university, being the responsible party, oversees the implementation of the ZDPA in this study. Universities violate students' privacy when they do not follow the right privacy practices. Inadequate procedures governing access to personal information and the over-collection of information are further factors that contribute to privacy breaches (OECD, 2013). According to Martin (2020), some breaches occur because an organisation lacks internal controls over how personal information should be used.

When it comes to managing the privacy of their personal information, teenagers in general (including students) are deemed irresponsible. Several researchers have carried out empirical investigations focusing on various facets of privacy, including privacy in the context of online activities (Mohamud et al., 2017; Salleh et al., 2013); privacy in the context of student expectations (Ivanova et al., 2015; Kumaraguru and Cranor, 2005; Talib et al., 2014); and privacy in the context of student awareness (Chen and Ismail, 2013, Lawler and Molluzzo, 2011; Malandrino et al., 2013). None of the studies points to the university–student relationship considering the three constructs of awareness, expectations, and confidence. There is a gap in combining the three constructs in a privacy model; this study considered these three important constructs.

2.3.3 Research questions and objectives of the study

The research questions were:

i. *How can a SPIPP model measuring awareness, expectations, and confidence in Zimbabwean universities be developed?*
ii. *How can the SPIPP model be validated?*
iii. *What is the association between the three constructs of awareness, expectations, and confidence?*

To answer these questions, the objectives of the study were:

i. *To create a SPIPP model measuring awareness, expectations, and confidence in Zimbabwean universities*
ii. *To use SEM to validate the SPIPP model.*
iii. *To identify the association between the three constructs of awareness, expectations, and confidence.*

3. Theoretical model: Student Personal Information Privacy Perception (SPIPP) model

In this section, the theoretical foundations of privacy perceptions, regulations and principles are discussed. The theoretical constructs of privacy awareness, privacy expectations and privacy confidence are proposed as the three constructs of the proposed (SPIPP) model. The FIPPs, the OECD privacy guidelines and the GDPR were also considered to identify components of the SPIPP that could be investigated from a privacy awareness, privacy expectation and privacy confidence perspective. The ZDPA was also considered, as the fieldwork was conducted in Zimbabwe. The aforementioned were used in this study to identify nine privacy components that each mapped to the three main constructs of the SPIPP model. The hypotheses underpinning this research are presented in this section.

3.1 Privacy constructs

The study concerned the three privacy constructs, namely awareness, expectations and confidence in privacy.

3.1.1 Privacy awareness

Awareness of privacy frameworks and theories is the foundational step in advancing privacy in the modern world (Knijnenburg et al., 2022). According to Fortes and Rita (2016), individuals reflect a certain level of awareness of how their personal information is being used, which implies that they have an abstract idea of what their personal information will be used for. Moreover, based on Westin's perspective on personal information privacy, the rate of the "Unconcerned" has been decreasing as technology has made strides into people's lives together with the emergence of multiple means of protecting privacy (Kumaraguru and Cranor, 2005). Nonetheless, privacy awareness programmes are essential among millennials, who constitute the majority of the university student population (Hooda and Yadav, 2017) and would sacrifice their privacy for other applications like social media ones (Bhatnagar and Pry, 2020). This was also augmented by Alghamdi et al. (2023) who found in their survey that despite being aware of the potential dangers, over 50% of students are still willing to disclose personal information through applications that request private or sensitive data. This calls for universities to invest in educating students about privacy issues, which would

enable students to determine how their personal information is handled and used (Isabwe and Reichert, 2013; Lawler and Molluzzo, 2011). This would aid in inculcating positive attitudes toward privacy (Future of Privacy Forum, 2021). Furthermore, efforts to raise students' awareness increase their understanding, which would aid in mitigating negative privacy perceptions (Tikkinen-Piri et al., 2018). According to Tikkinen-Piri et al. (2018), negative privacy perceptions occur when there is scepticism about the collection, use, processing and dissemination of student personal information.

To raise privacy awareness, privacy notifications are very helpful (Vail et al., 2008). Students may fail to comply with privacy policies because of a lack of awareness about such policies/notices (Kyobe, 2010). Privacy awareness can be thought of as a component of a well-informed society in which everyone is aware of their privacy rights and responsibilities (Fink, 2012). Universities should make it a habit to hold privacy training sessions and workshops to raise awareness about their policies (OAIC, 2015). Because training serves as a warning function as well as fulfils an awareness-raising role, it is essential (Kävrestad et al., 2023). To ensure that such awareness campaigns are inclusive, it is also necessary to consider age groups so that programmes can be customised and tailored to correspond with the interests and cultural features of each demographic group (Mohammed and Tejay, 2017).

Although a privacy policy is seen as a document that raises awareness about privacy issues, it has been determined that most students do not read and examine privacy policy documents in their entirety (Chen and Ismail, 2013). To them, it is simply a matter of accepting the terms and conditions so that they can acquire the resources they need. Furthermore, it is believed that if students were aware of how much information they unknowingly share about themselves, they would do everything possible to protect the privacy of their personal information (Malandrino et al., 2013). With increased concern about privacy that might not affect self-disclosure practices by students comes the privacy paradox phenomenon (Gruzd and Hernández-García, 2022). Consequently, the need for universities to have privacy policies cannot be overemphasised; nevertheless, students need to familiarise themselves with the contents of the policies to know what information they can safely disclose. It stands to reason that inadequate consideration of the repercussions of an absence of privacy awareness would result in bad privacy perceptions (Fink, 2012). As a result, it is the university's responsibility to raise awareness about the students' information privacy, which will result in them being aware of their privacy rights.

3.1.2 Privacy expectations

People's opinions of an organisation's handling and use of their personal information can fluctuate, depending on their expectations (Martin, 2015). It is, however, critical for businesses to prioritise meeting the privacy expectations of their customers and to do so according to expected baseline privacy standards (Da Veiga and Ophoff, 2020). This can also be applied to a university setting. Furthermore, according to Da Veiga and Ophoff (2020), expectations for organisational adherence to privacy standards vary, depending on a variety of characteristics such as demographic profiles, recorded data breaches or culture. When individuals feel that their personal information has been compromised, they are more likely to react negatively (Schwaig et al., 2013). This, too, can be applied to students at universities.

Mamonov and Benbunan-Fich (2018) opine that when students enrol at a university, they have specific privacy expectations regarding the information they disclose to the university. Additionally, Talib et al. (2014) indicate that these expectations are occasionally misguided. As a result, it is the university's responsibility to educate the students on realistic expectations, which are in line with the regulatory requirements. Although Hossain and Zhang's (2015) study was restricted to social media sites, they concluded that if users' expectations were realised, they would have greater control over their personal information and would be more prepared to share it. This was confirmed by Schumacher and Ifenthaler (2018), who focused on e-learning analytics. Hence, a university must meet student privacy expectations, particularly in terms of controlling how it shares personal information.

In addition, the Republic of South Africa's constitution (1996) prescribes people's right to privacy of personal information (Capistrano and Chen, 2015). Although the right to privacy is also prescribed by the Zimbabwean constitution (Republic of Zimbabwe), the specifics of how it will be enforced is not comprehensively stated. Institutions must therefore also meet students' privacy expectations to avoid lawsuits (Smit et al., 2009) that may arise from a privacy breach. Students expect institutions to protect their privacy. Adherence to such expectations earns their trust in the institution (Callanan et al., 2016). Any institution may, however, have its own expectations of how personal data ought to be kept and used, as dictated by applicable legislation (Burdon et al., 2012). Students must be made aware of such expectations, since this would provide a basis for them to construct their expectations of the use of their personal information, allowing them to appreciate the privacy of such information (Krzych and Ratajczyk, 2013).

Hypothesis 1: Students expect their privacy to be protected when their personal information is processed in line with regulatory requirements.

3.1.3 Privacy confidence

Privacy confidence relates to students' trust in their university because of the latter's observance of their privacy rights and how their personal information is handled by the university. Trust is a source of confidence (Huang and Bashir, 2016). Thus, if universities could ensure transparency in the processing of student information, students would feel emboldened and there would be a sense of trust among them, boosting student confidence and making it easier for them to participate in disseminating more information (Dwyer and Marsh, 2016). In fact, universities should engage with students and be open and honest about how they will gather, use and share their personal information, which will ultimately foster trust and cooperation from students (Park and Vance, 2021). Students must be informed about what information will be collected, processed and stored, and the modalities of how it will be accessed and secured (Botnevik and Khalil, 2020). The presence of privacy notifications in organisations is one technique to build trust that eventually results in confidence (Stange, 2011). To establish trust, individuals must understand how their personal information will be used when collected (Miltgen, 2009). Trust is a measure of the user's confidence in the handling of their personal information by institutions (Zlatolas et al., 2019). Regardless of good intentions, any data-driven process by the university is bound to fail if students do not feel comfortable with how the institution handles personal information (Future of Privacy Forum, 2021).

Privacy concerns harm trust, resulting in poor student confidence levels (Chua et al., 2017; Fortes and Rita, 2016). The prevalence of privacy breaches, which are thought to have a negative influence on trust and consequently confidence, result in individuals becoming hesitant to disclose personal information because of privacy concerns (Anjum et al., 2018). Consequently, students may become hesitant to disclose personal information to a university. An institution of higher learning should, therefore, devise strategies to enhance students' trust that their personal information will be kept private.

Chua et al. (2017) suggest that when a university commits itself to protecting students' privacy, it establishes a sense of assurance and trust, creating confidence and positive data privacy perceptions throughout the institution. The commitment may assume many forms, including a privacy policy (described earlier), which will ultimately reduce unfavourable perceptions that result from privacy-related concerns (Hasbullah et al., 2013; Tan et al., 2014). Therefore, to instil confidence and protect data successfully, there is a need for a well-documented procedure for submitting a complaint or concern (Adelola et al., 2014; Sodiya and Adegbuyi, 2019).

In line with the aim of this study, the privacy constructs refer to the awareness, expectations and confidence levels that could have an impact on perceptions of information privacy. People (students) will develop negative privacy perceptions if they feel that their privacy has been violated or infringed, because they have their sense of how their personal information should be

secured, even in the absence of legislation to that effect (Schwaig et al., 2013). However, if students become aware of their privacy expectations and observe that these are respected/met, they are more likely to develop trust (and consequently confidence) in the institution; this helps to alleviate any privacy concerns and other unfavourable attitudes (Kurkovsky and Syta, 2011).

The focus of this study is on information privacy, particularly as it pertains to personal data that universities typically process. This includes but is not limited to personal identification details (like names, and student ID numbers); contact information (email addresses, phone); academic records; health and well-being information; and financial data related to tuition fees and scholarships. Information privacy in our study refers to students' right to control or influence the collection, use, and sharing of their personal information. It includes principles and practices that maintain the confidentiality and integrity of personal information, particularly in digital formats. Our research is pivoted around three main constructs which encapsulate privacy awareness (having an understanding and knowledge of how personal information is managed, the risks involved, and the rights of students concerning their personal data), privacy expectations (students' expectations about the level of confidentiality and security measures that should be in place to protect their personal data) and privacy confidence (the level of trust students have in their university's ability to protect their personal information effectively).

Hypothesis 2: A relationship exists between information privacy expectations, awareness, and confidence in students' perception.

3.2 Privacy regulations and principles

The FIPPs, the OECD privacy guidelines, the GDPR and the ZDPA are discussed in the next section to consolidate and define the components to measure privacy awareness, privacy expectations and privacy confidence constructs.

3.2.1 Fair Information Practice Principles (FIPPs)

The FIPPs were designed as a set of international privacy standards that apply to both the private and public sectors (Gellman, 2017) and describe accepted global standards for privacy in the use of personal data (Sargsyan, 2016). They provide an anthology of agreed-upon principles for incorporation into the policies of international organisations and institutions and can be used to assess individual information processing that affects privacy (Guffin, 2017). The main objective of FIPPs was government regulation of the processing of personal information of individuals. However, because technological advancement has had a significant impact on how personal information is handled, these principles were subsequently made available to the private sector (Chang et al., 2018; Schwaig et al., 2006).

Although the FIPPs have evolved since they were first formulated (Gellman, 2017), their main determination continues to be the protection of personal information privacy (Teufel, 2008). The eight FIPPs are:

(i) *Openness/transparency*. Organisations are required to display notices outlining how they plan to use personal data, as well as how it will be gathered, shared, protected and disposed of (Gellman, 2017). One way of achieving this is to develop a privacy statement/policy to increase transparency in an organisation (Teufel, 2008).

(ii) *Individual participation/choice*. This relates to a customer's ability to select personally identifiable information to be collected and the model for its use (Chang et al., 2018). In the context of a university, this could refer to the choice that students should have to give third parties access to their personal information or opt-in for direct marketing.

(iii) *Data quality/integrity*. To achieve information integrity, data should be complete, precise, relevant and suitable (Teufel, 2008). Students' addresses (both physical and email) and cell phone numbers may change, and they ought to have access to this information in case they want to update it.

(iv) *Security*. Refers to the safeguards put in place for securing personal information and correctness to maintain data integrity, availability and confidentiality (Chang et al., 2018). This is one of the reasons why institutions should

develop security policies to aid the adoption of various security controls that help to protect students' privacy (Chua et al., 2017).

(v) *Use limitation.* Personal information should be used solely for the mentioned purposes in privacy (Teufel, 2008). Guffin (2017) states that when a university shares personal information, it should do so with the consent of the individual involved or only for some other reason that is compatible with the original reason for gathering it.

(vi) *Purpose specification.* Cate (2006) states that personal information should be collected for a specific purpose and that the data subject must be aware of this purpose. An institution is required to post a notice explaining the reasons for collecting information, as well as the processing, storage, disclosure, maintenance, or distribution of personal information. The purpose should be defined before collection (Gellman, 2017; Guffin, 2017).

(vii) *Collection limitation.* The information obtained should be essential and appropriate for completing a certain aim, and no personal information collection beyond what is essential should be gathered (Teufel, 2008). Such data should be gathered legally and fairly without discrimination (Gellman, 2017).

(viii) *Accountability.* Organisations must be held accountable for enforcing the terms of data privacy regulation and including reporting (Chang et al., 2018). University-wide awareness efforts on privacy issues related to personal information are some of the ways that institutions could be held accountable for privacy-related issues.

Although the FIPPs are not laws, they provide the foundation for privacy legislation, directing in what ways personal information should be gathered, processed, kept, released and safeguarded (Teufel, 2008). According to Tikkinen-Piri et al. (2018), most nations base their data protection regulations on these principles. Therefore, for the current study, it was critical to ensure that the SPIPP model incorporated such international privacy principles to ensure that its implementation would meet international requirements.

3.2.2 OECD privacy guidelines

According to (Schwaig et al., 2006), the OECD privacy guidelines were developed by using the FIPPs as the point of departure. It is a unique meeting place for representatives from various governments to collaborate in confronting global difficulties such as environmental, economic, social and technological issues (OECD, 2013). These privacy guidelines are founded on the idea that the protection of personal data both within and across borders is a critical component of building trust in online activities that gather data (OECD, 2013). The OECD (2013) also states that the data controller has the responsibility for accounting for the security of individuals' personal information. The member states of the OECD meet frequently to discuss privacy concerns in their countries and they have drafted some recommendations for countries to help one another with privacy concerns (OECD, 2013).

The following eight privacy guidelines are included in the OECD Privacy Framework (OECD, 2013, p.14–15:

(i) The *collection limitation principle* prescribes restrictions on personal data collection and that the data should be collected lawfully and fairly. Furthermore, the data subject must give full consent for the collection.

(ii) The *principle of purpose specification* relates to the idea that the aim of personal data collection should be stated before the data are collected and that there must be limitations on the use of such data only for the stated purpose or any compatible purpose.

(iii) The *data quality principle* is concerned with how personal data are linked with the purpose for which they are intended. Such information should be current, comprehensive, and accurate.

(iv) *The use limitation principle* prevents personal information from being processed or disclosed for other purposes than those for which it was gathered, as described during the collection of the information.

(v) The *individual participation principle* focuses on an individual's rights, which include – but are not limited to – challenging any data relating to them (which may result in data being erased, amended or rectified, among other

things) and receiving communication on information about them in a sufficient amount of time and in a form that is understandable to them.

(vi) The *security safeguards principle* is aimed at ensuring that information is secure from risks such as unauthorised access, modification, disclosure, processing, destruction or loss and that appropriate security measures are in place.

(vii) The *openness principle* states that there is a need for transparency about personal data practices and policies, as well as methods for determining the nature and presence of personal data, the primary purposes for which they are used, and the data controller's identity and their usual residence.

(viii) The *accountability principle* means that the data controller is accountable for complying with all steps that give effect to the stated standards.

Tikkinen-Piri et al. (2018) state that the OECD privacy guidelines remain the most used of all international privacy rules. The constructs embedded in the guidelines are mirrored in existing and emerging privacy and data protection legislation, and they formulate the foundation of many countries' leading privacy programmes, practices and concepts (Johnston and Wilson, 2012). The OECD privacy guidelines were used to develop the conceptual SPIPP model. They were important in this study because mapping the proposed SPIPP model to the OECD privacy guidelines would facilitate its modification for other countries. Furthermore, since they are internationally recognised privacy guidelines, adherence to them would be per international norms.

3.2.3 General Data Protection Regulation (GDPR)

As a European Union (EU) policy, the GDPR was created to regulate the privacy of personal data (Larrucea et al., 2020). According to Bandara et al. (2020), organisations need to strengthen their transparency while handling consumers' personal information.

- *Territorial scope*

The GDPR's reach goes beyond EU countries. Tikkinen-Piri et al. (2018) lament that if the data of individuals in the EU are processed, all non-EU and foreign organisations should comply with the GDPR. Therefore, the GDPR is not constrained by the territorial scope (Pelteret and Ophoff, 2016), which establishes its importance in this study. While it is an EU directive, its scope is wide, encompassing many nations and, as a result, numerous organisations and institutions that process EU citizen data. The GDPR's fundamental purpose is the regulation of the acquisition of and how personal data are processed (Kaneen and Petrakis, 2020). As such, transparency and accountability in the usage of personal data are enhanced (Cornock, 2018). According to Cornock (2018) and Tankard (2016), one of the benefits of the current GDPR over previous privacy legislation is its encouragement of organisations and businesses to avoid data breaches by all means by safeguarding their systems.

- *Data breaches and reporting*

Severe penalties in the event of a breach, which are supposed to be reported within the prescribed 72-hour time, are articulated in Chapter VIII of the GDPR (Cornock, 2018). Massive fines of "a total of 20 million euros or an equivalent of 4% with respect to the total annual worldwide turnover of the previous financial year" are imposed in the event of non-compliance (Krempel and Beyerer, 2018). A breach happens when an organisation files a security incident notice (Hoofnagle et al., 2019). In any breach, the GDPR prescribes that the organisation must report it as soon as it happens (Presthus and Sønslien, 2021).

- *Aligning the SPIPP model with the GDPR*

If the GDPR is mapped to the SPIPP model, it could be used in additional jurisdictions in the future. Because Zimbabwe has yet to publish its privacy guidelines and materials, it is necessary to draw on what developed countries such as those in the EU have done and tailor it to the Zimbabwean context. That means that for the data protection law to be implemented effectively,

organisations should incorporate ideas from several global privacy laws (including that of the GDPR) to facilitate easier amalgamation. Such integration would aid Zimbabwean organisations in adhering to international privacy norms. Hence, to be used in other jurisdictions, the SPIPP model should be aligned with international privacy guidelines and best practices. The GDPR is included in this paper since it is a recently publicised European privacy development with the ability to influence every country in the world directly or indirectly. The fact that it can be adapted easily adds to its relevance, realising that every country that deals with EU individuals' data is required to follow the GDPR's requirements. The GDPR is aimed at improving and digitally integrating the protection of personal information across all EU states, as previous directives failed to satisfy the privacy needs of the digitalised world (Cornock, 2018).

3.2.4 Zimbabwe Data Protection Act (ZDPA)

The Zimbabwean regime has drafted several bills in many fields, with the ZDPA being one of the most notable in the previous decade (Chetty, 2013). A detailed examination of the ZDPA shows that it is a privacy regulation that is consistent with other worldwide legislation – a good thing from the Zimbabwean perspective. It is intended to be a law that governs how all entities (universities included) handle personal data, at the same time protecting improper data collection and use (Chetty, 2013). As specified in the ZDPA (Republic of Zimbabwe, 2021), the data controller's responsibilities include maintaining data integrity, confidentiality and privacy; processing sensitive information with permission; and ensuring the rights of the data subject and, at any time, withdrawing such consent without justification. The controller should ensure that personal data processing is done fairly and legitimately and for the defined and lawful resolve, with effective data protection and regulatory safeguards in place.

Articles 19, 20 and 21 of Part VI of the ZDPA state that the data controller should take all reasonable means to ensure privacy, following applicable information security standards. If a breach occurs, the data controller should inform the Zimbabwean Data Protection Authority immediately (Republic of Zimbabwe, 2021). The data subject should have access rights at any time to any of their personal information kept by the controller, as further emphasised in Article 14 of Part V of the ZDPA (Republic of Zimbabwe, 2021). This extends to the data subject’s right to alter, limit, or correct their personal information, and applies more broadly than when processing is required to execute the requirements and specific controller rights, for example, relevant to employment, the law or in accordance with security laws of the society. Furthermore, it extends to data made public by the data subject, like processing for scientific research or processing for the preparation of legal defence claims.

3.3 Comparison of the ZDPA with the FIPPs, the GDPR and the OECD privacy rules.

The ZDPA’s alignment with the GDPR, the OECD privacy guidelines and the FIPPs is discussed in this section. The ZDPA has an impact on the processing and use of student’s personal information by public bodies like universities. If institutions are to avoid non-compliance and paying penalties, they will have to align their privacy policies to comply with the legislation. It was necessary to match the ZDPA with the GDPR, the OECD privacy guidelines and the FIPPs, as outlined above, to gain a better understanding of it and its relationship with other privacy regulations and principles. This facilitated a comparison between the ZDPA and international norms such as the GDPR, the OECD privacy guidelines and the FIPPs. Table 1 shows the comparative analysis.

The provisions of the ZDPA cover various aspects that are part of the FIPPs, the OECD privacy guidelines and the GDPR, as can be seen in Table 1. The only distinction is that, except for the GDPR, the ZDPA makes provision for a unique aspect of whistleblowing, in comparison with many other principles and jurisdictions. Penalties and whistleblowers are not incorporated in the FIPPs or the OECD privacy guidelines. This whistleblowing clause was created to maximise the likelihood of getting more information from the public. Such inclusion requires adherence to certain protocols. These are included in Part IX of the ZDPA. In addition, the FIPPs do not cover internal controls and safeguards, transborder flow or the rights of the data subjects, whereas the ZDPA, the GDPR and the OECD privacy guidelines do.

Table 1: Matching the ZDPA with the FIPPs, the OECD privacy guidelines and the GDPR.

ZDPA sections	FIPPs	OECD	GDPR
Quality of data – Part III	√	√	√
Sensitive information – Part IV	√	√	√
Disclosure when collecting personal information – Part V	√	√	√
Security – Part V	√	√	√
Authority to process – Part V	√	√	√
Notice of a security breach, the need to notify and the content of the notification – Part V	√	√	√
The openness of the processing – Part V	√	√	√
Rights of the data subject – Part V	×	√	√
Accountability – Part V	√	√	√
Internal controls and safeguards – Part V	×	√	√
Penalties – Part X	×	×	√
Transborder flow – Part VII	×	√	√
Whistleblowing – Part IX	×	×	√

3.4 Privacy components

Listed below are the components that were regarded as fundamental for inclusion in the conceptual model; as such, they are discussed in more detail. The components were taken from the OECD privacy guidelines, the ZDPA and the GDPR, which were mapped to the FIPPs as a base. Since personal information privacy perceptions were developed from a student perspective, the principles of accountability, security safeguards and control were excluded, as depicted in Table 1. Such exclusions were necessary because students do not have the authority to put in place security systems and cannot be held accountable for the information processed by a university. Compliance with privacy regulations is a university's prerogative and responsibility as the data controller. Hence, openness/notice, information quality, collection limitation, use limitation, choice/individual participation and purpose specification remained and are discussed below.

3.4.1 Notice/openness

Although notices are intended to raise awareness of privacy matters, they tend to result in trust and thus confidence among data subjects (students), which are critical for the parties' relationship (Stange, 2011). Students must be informed that privacy policies exist (Sargsyan, 2016). Furthermore, in case of a breach of privacy, a notice of such breach must be given as soon as feasible; the GDPR specifies that this should happen within 72 hours (Cornock, 2018). Students want notices to be brief, accessible and unambiguous (Preuveneers et al., 2016), and a privacy policy could be used at institutions to facilitate and raise awareness. The publication of privacy notices would ensure that all practices involving personal information are transparent, including the storing and use of personal information by organisations (Katurura and Cilliers, 2016; Sargsyan, 2016).

3.4.2 Information quality

According to Gellman (2017), personal information is expected to be comprehensive, current and accurate, as well as appropriate for the intended use. Agencies and universities have the responsibility and right to maintain information security to ensure information quality, as well as to manipulate personal information under the required characteristics of comprehensiveness, accuracy, relevance and suitability. This should be done reasonably to ensure equality for people (Guffin, 2017) – in this case, students – and it would boost student trust in a university because they would know that information quality is maintained.

3.4.3 Purpose specification

As explained by Chetty (2013), the ZDPA demands an explicit, specific and genuine purpose for the processing of personal information. Such a purpose must be declared at or before the time of data collection. Additionally, the purpose specification must be used together with the consent clause because it specifies the required information and its intended use (Vand der Merwe and Van Staden, 2015). This component, therefore, obligates the data collector to state the reason for collecting personal information before collection starts (Cavoukian, 2009). Katurura and Cilliers (2016) propose that information should not be applied for any purpose other than what was specified previously, unless for reasons such as fraud, harm avoidance or the law.

3.4.4 Use limitation

The OECD privacy guidelines specify that "personal data should not be disclosed, made available or otherwise used for purposes other than those specified following [the purpose specification principle] except (a) with the consent of the data subject; or (b) by the authority of law" (OECD, 2013, p.14). This means that an institution is compelled to use students' personal information solely for the purposes stated within the notice (Guffin, 2017), which necessitates a clear and explicit goal definition (Robbins and Sabo, 2006). It stands to reason that a student would comply should other legal reasons arise for their personal information to be used (Preuveneers et al., 2016).

3.4.5 Collection limitation

Personal information should be obtained in a lawful, fair and limited manner for the stated purposes (Cavoukian, 2009). Restrictions and limits should furthermore be placed on the procedures for collecting personal information and the data must be attained with the data subject's full knowledge and full consent (OECD, 2013). Limiting personal information collection motivates users to provide personal information (Kokolakis, 2017). However, to ensure such motivation, all organisations (universities) should abide by the limitations on the information that may be collected about individuals (students) in terms of what is regarded as necessary for such information collection (Cavoukian, 2009; Gellman, 2017). It should not include the collection of information on non-essential issues such as ethnic group, political affiliation, or religion.

3.4.6 Individual participation/choice

Regarding their collected personal information, individuals (students) may decide whether they wish to participate (Robbins and Sabo, 2006). Every person whose personal information is processed also has the right to have that information amended at any time (Gellman, 2017). That means that institutions seeking consent to use students' personal information should involve the students in the collection processes and provide redress and correction mechanisms if necessary. Even if the personal information collected has been confirmed, the data controller (university) should respond to requests for amendments from data subjects (students) (OECD, 2013). In a university setting, it would also be critical to know who accesses the personal information of students and how it is kept (Katurura and Cilliers, 2016).

3.5 Additional privacy components

Apart from the abovementioned components, a privacy policy, privacy education and consent should be considered as additional components to assess student expectations, awareness, and confidence in the university. These were included in the consolidated SPIPP model in addition to the six components outlined above.

A privacy policy serves as an educational tool by outlining how an institution must gather, maintain, disclose and use personal information about individuals (Chua et al., 2017). A simple and straightforward privacy policy also assists in alleviating privacy concerns (Vail et al., 2008). According to Chua et al. (2017), privacy policies handle privacy concerns. The statements in a privacy policy must be brief, precise and clear; in the case of universities, students should find it easy to read the policy.

Institutions should also demonstrate how the information will be handled and processed (Rao et al., 2014). It could thus be concluded that a university would need a privacy policy to assist in raising awareness among its students.

According to a study conducted by Farooq et al. (2016), a key measure to minimise information security issues in an organisation/institution is privacy education. This implies that any privacy model developed for a university setting should include privacy education as one of its key components. Coleman and Purcell (2015) argue that a university should prioritise educating students on the importance of privacy, particularly concerning social media identity theft, the privacy of their financial information, the protection of their mobile devices and the monitoring of unauthorised access to their e-mail accounts. Sargsyan (2016) adds that such privacy education sessions should be held regularly since people (students) must be reminded continually.

Consent is one of the legal bases for processing personal information, as provided by the OECD, the GDPR and the ZDPA, since it ensures that personal data are gathered and used only for the purpose stated when consent was provided (De Hert and Papakonstantinou, 2012). Concerning this study, consent included giving people the authority to decide how their personal information would be used, barring cases where this was not acceptable (Muravyeva et al., 2020). If a person does not want to receive particular communications or share personal information, they have the option to opt-out (Swartz and Da Veiga, 2016). That would apply to university students too. A component must have two ticks in the measuring perspective, from both the student perspective and the university perspective, to be adopted into the SPIPP conceptual model. The suggested SPIPP conceptual model could not contain a component with one check in the viewpoint column. The university could implement the security and accountability components, as was mentioned. Since these are the responsibilities and duties of the institution, students are unable to implement security measures, hold their universities accountable for how their information is processed and/or ensure that privacy laws are followed. The criterion leads to the conclusion that the SPIPP paradigm does not have accountability, security controls or safeguards. In summary, the nine privacy components focused on in this study were notice/openness, information quality, purpose specification, collection limitation, use limitation, choice/individual participation, privacy policy, privacy education and consent. These are shown in the conceptual model in Figure 1. An assumption was made to measure all the factors with the same weight, applying to the privacy expectations, awareness and confidence of students. This allowed for the statements in the questionnaire in Appendix 1 to be assessed equally.

Hypothesis 3: The nine-dimensional privacy components measure the three privacy constructs (expectations, awareness and confidence).

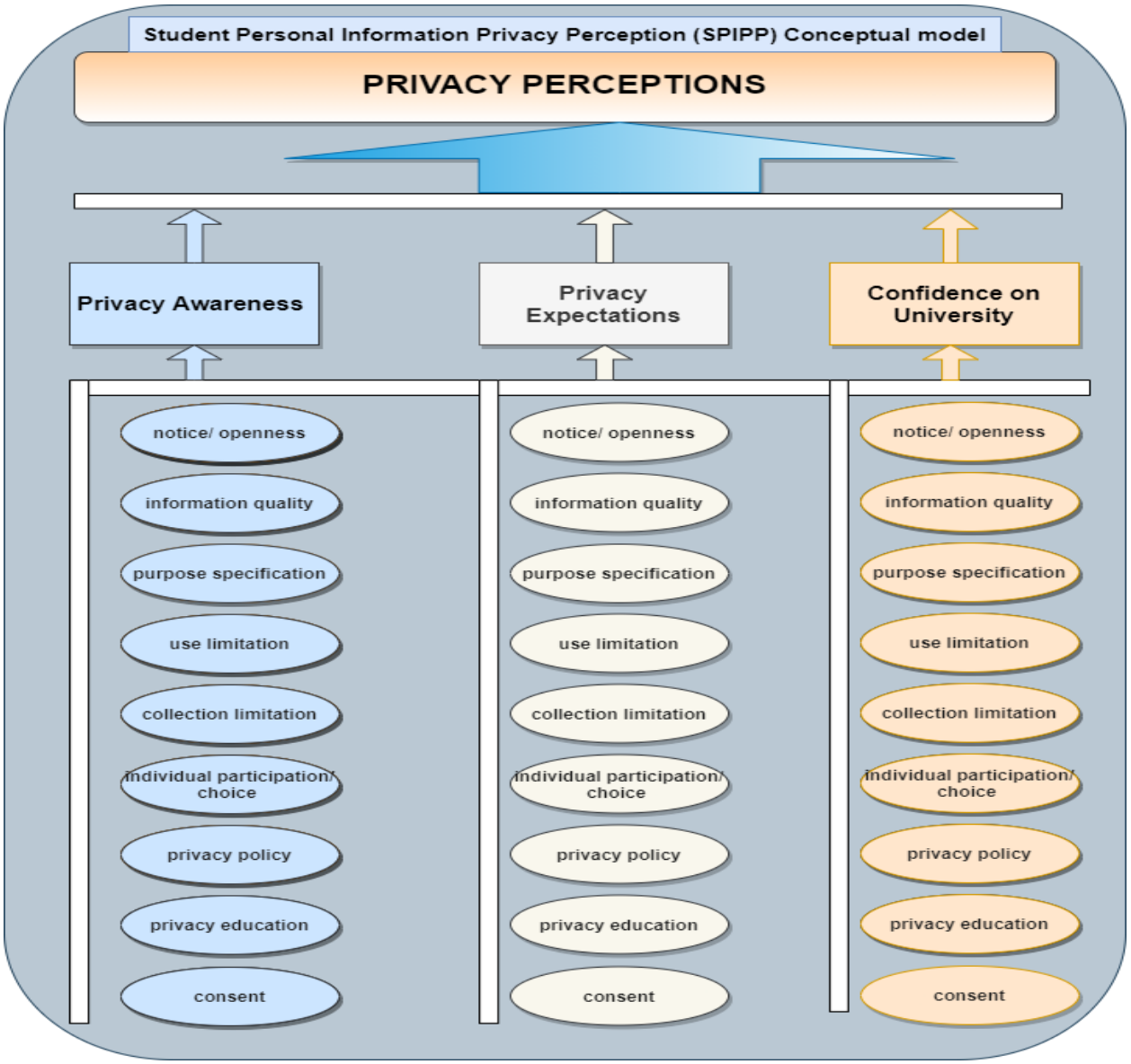


Figure 1: The SPIPP conceptual model for a university (Maguraushe et al., 2019)

In summary, the three constructs (expectations, awareness, and confidence) can be conceptualised to find the relationship among the various themes. This can be explained as follows.

Awareness is an important concept in privacy matters. Students are aware of their right to opt in when providing personal information and their right to opt-out when they no longer want to participate in providing their personal information (Kokolakis, 2017). Privacy education can be implemented through various options that include reminding students of privacy issues by using privacy notices, newsletters and magazines (Knijnenburg et al., 2022). Additionally, training on privacy can be done by the institution (Kävrestad et al., 2023). From the instruction side, the students are aware that the university can only collect their personal information if they explicitly specify and justify the purpose of collection, and this must be done on or before the point of collection (Presthus and Sønslien, 2021).

Equally important are the expectations, as students expect the university to justify the reason for collecting their personal information fairly and lawfully (OECD, 2013). In fact, no disclosure is permissible unless it is in line with the regulatory

requirements (Guffin, 2017). Privacy policies and privacy notices need to be simple to understand, as this helps students to know the privacy regulations and raise awareness of privacy (Vail et al., 2008). Students have the right to make sure that the collected personally identifiable information about them is correct, used for the specified purpose, and they can update it as and when the need arises (Chang et al., 2018). Furthermore, students expect to follow a particular due process as they try to update their personal information (Knijnenburg et al., 2022).

Students can also gain confidence in the university if they notice that the university seeks consent from students for the processing of their personal information (Merwe and Staden, 2015; OECD, 2013). Another factor that increases students' confidence is to specify the reason for collecting their personal information before the collection process (Da Veiga, 2018). Furthermore, the option of reviewing their personal information to ensure that it is correct increases their confidence in the university. Efforts by the university to uphold privacy also play a pivotal role in increasing their confidence in the university. For instance, the publication of privacy notices, the presence of a privacy policy, students' right to opt in or opt-out, and the presence of due process when checking or updating collected information (Knijnenburg et al., 2022).

Figure 2 outlines the conceptual model tested with SEM in the research methodology section. Hypothesis 1 investigated whether students expect their privacy to be protected when their personal information is processed in line with regulatory requirements depicted by the nine privacy components derived from the regulatory requirements. Hypothesis 2 related to establishing if a relationship existed in students' perceptions, namely a relationship between information privacy expectations, awareness and confidence. Hypothesis 3 established if the nine-dimensional privacy components measured the three privacy constructs (expectations, awareness and confidence).

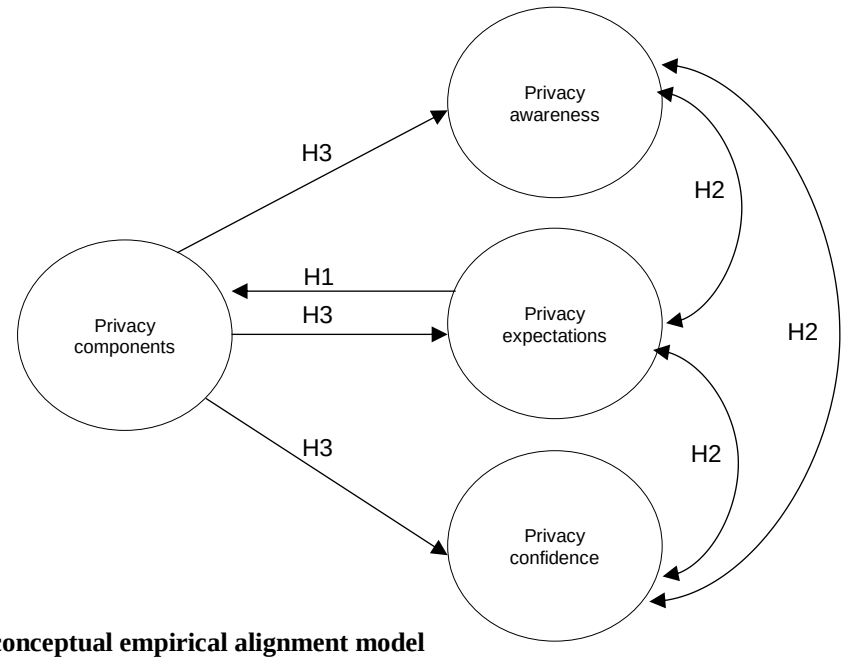


Figure 2: The conceptual empirical alignment model

4. Research design and methodology

This section covers the research paradigm, research method, research strategy, population and sampling, research instrument and data collection, data analysis and ethical considerations.

4.1 Research paradigm

The research employed a positivist philosophy, giving emphasis to the collection of empirical data and the analysis of cause-and-effect (Saunders et al., 2016). Positivism relies on observable truths and seeks regularities and patterns in data to create generalizations. It is founded on the belief that scientific methods offer the most accurate knowledge, favouring objective and

empirical approaches to comprehend social phenomena. This study collected empirical data about the perceptions of students toward privacy constructs which was analysed statistically.

4.2 Research method

A quantitative research method was employed for this study (Saunders et al., 2016). This approach begins with a theoretical concept or hypothesis, which is then empirically tested. In this study a conceptual framework was developed with corresponding hypotheses (figure 2) and a related questionnaire in order to collect data which can be analysed statistically.

4.3 Research strategy

This study adopted the survey, which gives the numerical descriptions of trends and opinions within a population (Kazi and Khalid, 2012). They are cost-effective and enable comparisons across large samples, making them appropriate for achieving the objectives of this study. The research instrument in this study is a self-designed questionnaire, Information Privacy Perception Survey (IPPS), which was developed based on the theoretical model (figure 1). Data was collected using the questionnaire which was set up in an electronic and hard copy format as part of the survey process.

4.4 Population and sampling

The instrument was subjected to expert review, applying the purposive sampling technique (Neuman, 2014). According to Holbrook et al. (2007), a comprehensive expert review panel should comprise between two and five reviewers. Four reviewers were purposively used in this study to review the instrument, all of whom had at least three years of experience in information privacy, privacy advisory services, data protection, privacy compliance and cyberspace consulting. Convenience sampling was adopted for piloting with a total of 15 students who participated. Figure 3 provides more information about the expert review and pilot study.

The determination of the sample size for the survey was based on the requirements of the instrument, ensuring adequate representation and statistical validity. Using the formula 5(n) where n signifies the number of items in the instrument (Gerber & Hall, 2017), it was computed to 5 x 54 statements require a minimum 270 responses. The survey was sent out to a larger sample of +/- 350 in order to obtain the minimum number of responses. The students were selected through probability random sampling (Neuman, 2014). A list of all registered students at the university was acquired from the administrative records to carry out the random sampling technique. Students were chosen at random from this list, ensuring equal chances for everyone (Saunders et al., 2016). This method ensured that there was no bias in the selection process and that the sample accurately reflected the various characteristics of the university's student population. The chosen students were then invited to participate in the survey through their university email addresses, adhering to the principles of randomness and impartiality (Saunders et al., 2016) and total of 284 responses were received. Due to practical constraints, the study was limited to one university. The sampling method aimed to represent the larger population and included registered students.

4.5 Instrument and data collection

A self-administered questionnaire, the Information Privacy Perception Survey (IPPS), was used as the instrument to collect numerical data that could be confirmed quantitatively (Jain et al., 2016; Kazi and Khalid, 2012). In research, the process of creating an instrument has several iterations. After the theoretical research process was completed, a validity and reliability study was conducted (Kumar, 2011). In this study, the constructs of the instrument were designed using literature theory. The steps followed are shown in Figure 3.

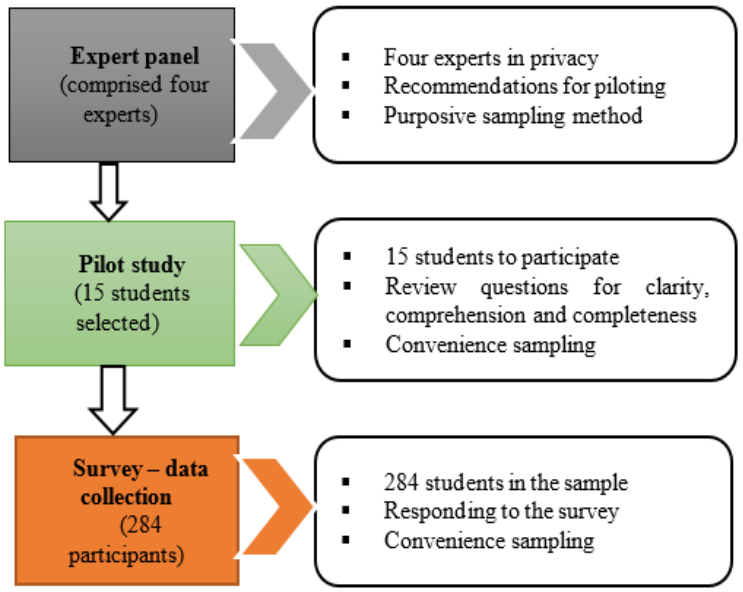


Figure 3: The instrument design process

Expert reviewers assist in providing a focused and detailed directive on issues and making recommendations (Kumar, 2011). The expert reviewers had to indicate whether a statement was necessary as well as whether all the statements were clear before a pilot study could be undertaken. The purpose of the pilot study was to adjust the statements and ascertain whether they were clear, complete, and comprehensive.

The nine privacy components in Figure 1 were used to develop two statements on each privacy construct, namely awareness, expectations, and confidence. A total of 54 statements were created. The statements in the appendix were further refined to create a final instrument that allowed the researcher to gather data from the respondents. The data were obtained by way of a self-administered survey instrument. To score the variables, the researcher used a five-point Likert scale spanning from strongly disagree to strongly agree. Follow-up e-mails to ensure that the statements were concise to boost the response rate in the study were implemented (Kazi and Khalid, 2012). In addition, the researcher printed and delivered hard copies to the students.

4.6 Data analysis

SurveyTracker was used to collect the data, which was then imported into the Statistical Package for Social Sciences (SPSS), version 25, for statistical analysis. Two types of analysis were used: descriptive (mean, standard deviation, frequency, and percentages) and inferential (ANOVA, t-test, Pearson product-moment correlation coefficient (PPMCC), Spearman correlation and SEM). By comparing a specific descriptive statistical feature, such as the means of populations, ANOVA and t-tests were employed to examine the spread of the data values (variance) between and within data (Saunders et al., 2016). The strength of the correlations between the two variables was assessed using PPMCC (Rossiter, 2017). The group mean differences were tested using the Spearman correlation (Cohen et al., 2011). The model was validated using SEM (Kline, 2011).

4.7 Ethical considerations

Research ethical considerations were considered in this study. The researchers obtained authorisation from the Zimbabwean University's Research Ethics Committee to conduct research at different campuses in Zimbabwe. The researchers further received research ethical approval from the Research Ethics Review Committee at the University of South Africa (UNISA) (Ref: 030/KM/2019/CSET_SOC). All participants were provided with an information letter that covered the research study objectives,

participation requirements, confidentiality, anonymity, and researcher contact details. Informed consent was obtained from both expert panel members and pilot participants including consent for all student participants within the first page of the electronic survey. No personally identifiable information was collected, and all participants participated anonymously and voluntarily.

5. Data analysis and results

5.1 Demographic data

The demographical statements in the instrument addressed the respondents' age, gender distribution, nationality, mode of study, year of study and the learning programmes that the students were pursuing. Table 2 gives a summary of the respondents' demographic information.

Table 2: Respondents' demographic data

Feature	Frequency	Percentage (%)
Age band		
1996–Present time	67	23.34
1977–1995	177	61.67
1965–1976	41	14.29
1946–1964	1	0.35
Born in or before 1945	1	0.35
No response	0	0.00
Gender		
Male	140	48.78
Female	143	49.83
Other	4	1.39
No response	0	0.00
Nationality		
Zimbabwean	284	98.95
Another African country	3	1.05
European	0	0.00
American	0	0.00
Australian	0	0.00
Asian	0	0.00
Other	0	0.00
No response	0	0.00
Mode of study		
Conventional mode	141	49.13
Parallel mode	89	31.01
Block mode	47	16.38
Other modes	10	3.48
No response	0	0.00
Study year		
1st	57	19.86
2nd	81	28.22
3rd	28	9.76
4th	91	31.71
Master's level	0	0.00
Doctorate level	11	3.83
Certificate (6 months)	19	6.62
No response	0	0.00
Programme distribution		
BBM & IT programme	164	57.14
BAcc programme	15	5.23
BBM Finance programme	21	7.31
BBM Marketing programme	16	5.57
BA Development Studies programme	22	7.67
BA Dual Honours programme	15	5.23
BA Theology programme	2	0.70
MBA programme	0	0.00
DPhil programme	11	3.83
6-month certificate	19	6.62

Feature	Frequency	Percentage (%)
Other	2	0.70
No response	0	0.00

An EFA was done (Maguraushe et al., 2020), with the following seven new factors emerging: university confidence, practice confidence, external awareness, individual awareness, privacy education, privacy expectations and correction expectations. These new factors were used to propose the conceptual model and to test the hypotheses. The relationships between the factors were investigated and Figure 4 reflects the SPIPP empirical model with the new factors, following the EFA.

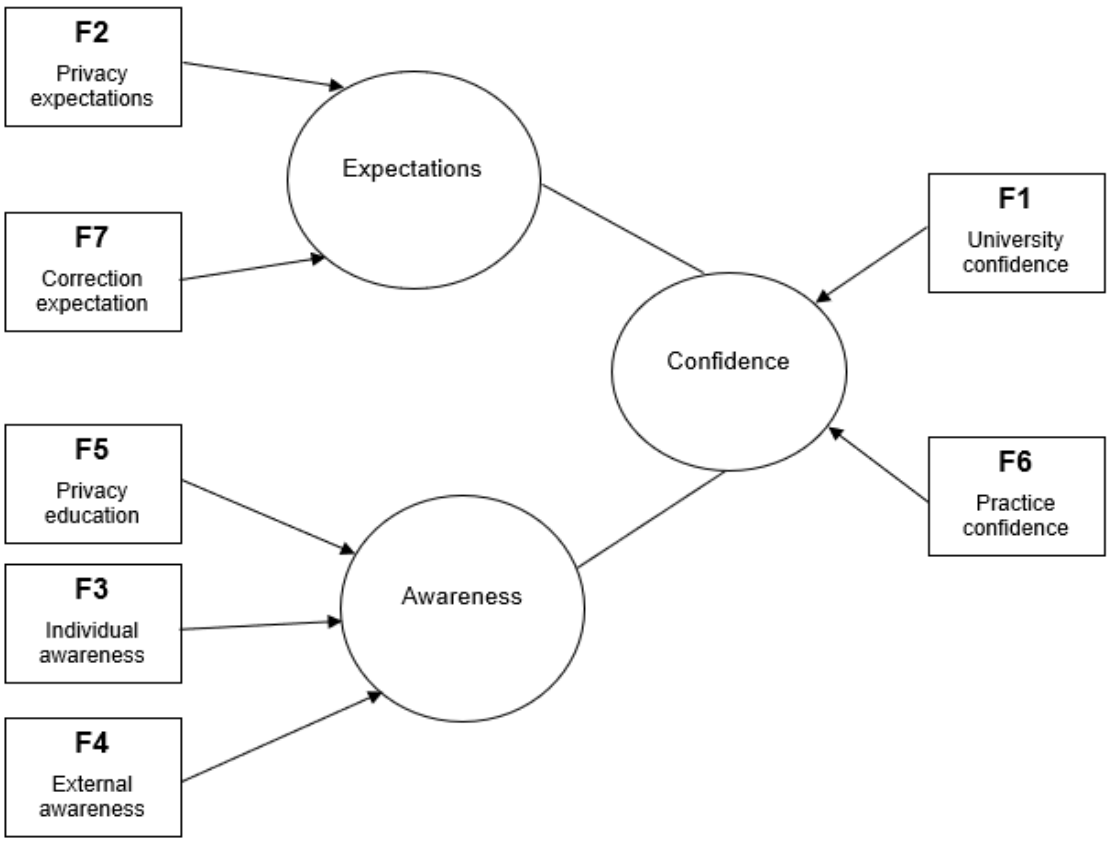


Figure 4: The SPIPP empirical model (Maguraushe, 2021)

The EFA showed seven valid and reliable factors with Cronbach's alpha values between 0.781 and 0.922 (Maguraushe et al., 2020). These were university confidence, privacy expectations, individual awareness, practice confidence, correction expectations, privacy education and external awareness. These factors were used in the confirmatory factor analysis (CFA).

5.2 Confirmatory Factor Analysis (CFA)

The Confirmatory factor analysis (CFA) technique is used to test a predefined factor model's fit in an observed dataset (Hair et al., 2014). Analysis of Moment Structures (AMOS), an extension of the SPSS package, was used for CFA. CFA tests various factors against a hypothesised model to confirm or reject preconceived theories (Ellis, 2017). It is used for confirmatory tests of measurement theory and construct validity (Hair et al., 2014). In fact, CFA increases research item validity and helps to answer research questions which drives research forward (Greenfield and Greener, 2016). In this study, the researcher analysed both absolute and incremental fit indices. Absolute fit indices assess how well a model fits the data without comparing it to other models (Ma and Shek, 2018). In this research, the Chi-Square (CMIN), Relative Chi-square (CMIN/ df), Root mean squared error of approximation (RMSEA), Standardized root mean squared residual (SRMR), and PCLOSE were used as absolute fit indices. Incremental fit indices, on the other hand, compare the researcher's model to a baseline model (Kline, 2011). The Comparative fit index (CFI) and Tucker-Lewis index (TLI) were used as incremental fit indices.

The following criteria were used in CFA in this study:

- The Chi-Square (CMIN) is a fit index for structural models that measures the divergence between the model and covariance matrices (Newsom, 2018).
- The Relative Chi-square (CMIN/ df) is a statistical analysis that adjusts for sample size on the chi-square, with values less than 3 considered good, and values less than 5 are sometimes acceptable (Hooper et al., 2008). However, the CMIN/ df should not be heavily relied upon for model fit assessment due to its limited statistical relevance (Kline, 2011).
- The Root mean squared error of approximation (RMSEA) measures how well the model fits the covariance matrix of the population. It also provides a confidence interval for its value. A value close to zero indicates a good fit, and it is considered acceptable if it is less than or equal to 0.08 (Hooper et al., 2008; Kline, 2011).
- The Standardized root mean squared residual (SRMR) is a measure of the difference between observed and projected correlations. It assesses the overall fit of a model and a value of zero indicates a perfect fit. It is accepted when it is less than or equal to 0.08 (Kline, 2011).
- The PCLOSE statistics gives the possibility of a hypothesis assessment that the population RMSEA is not greater than 0.05, indicating that the predicted moments are close to the moments in the population (Hu and Bentler, 1999).
- The Comparative Fit Index (CFI) evaluates model fit by comparing the actual data to the hypothesised model, while also considering sample size. Values range from 0.0 to 1.0, with values closer to 1.0 indicating a good fit. A value greater than 0.90 is acceptable (Kline, 2011).
- The TLI compares CMIN/df values for specified and null models. It can range from below 0.0 to above 1.0, with values approaching 1.0 indicating a good fit. A TLI value of 0.9 or higher is considered acceptable (Hair et al., 2014).

Table 3 reflects a summary of the privacy components' fit indices.

Table 3: The privacy components' fit indices

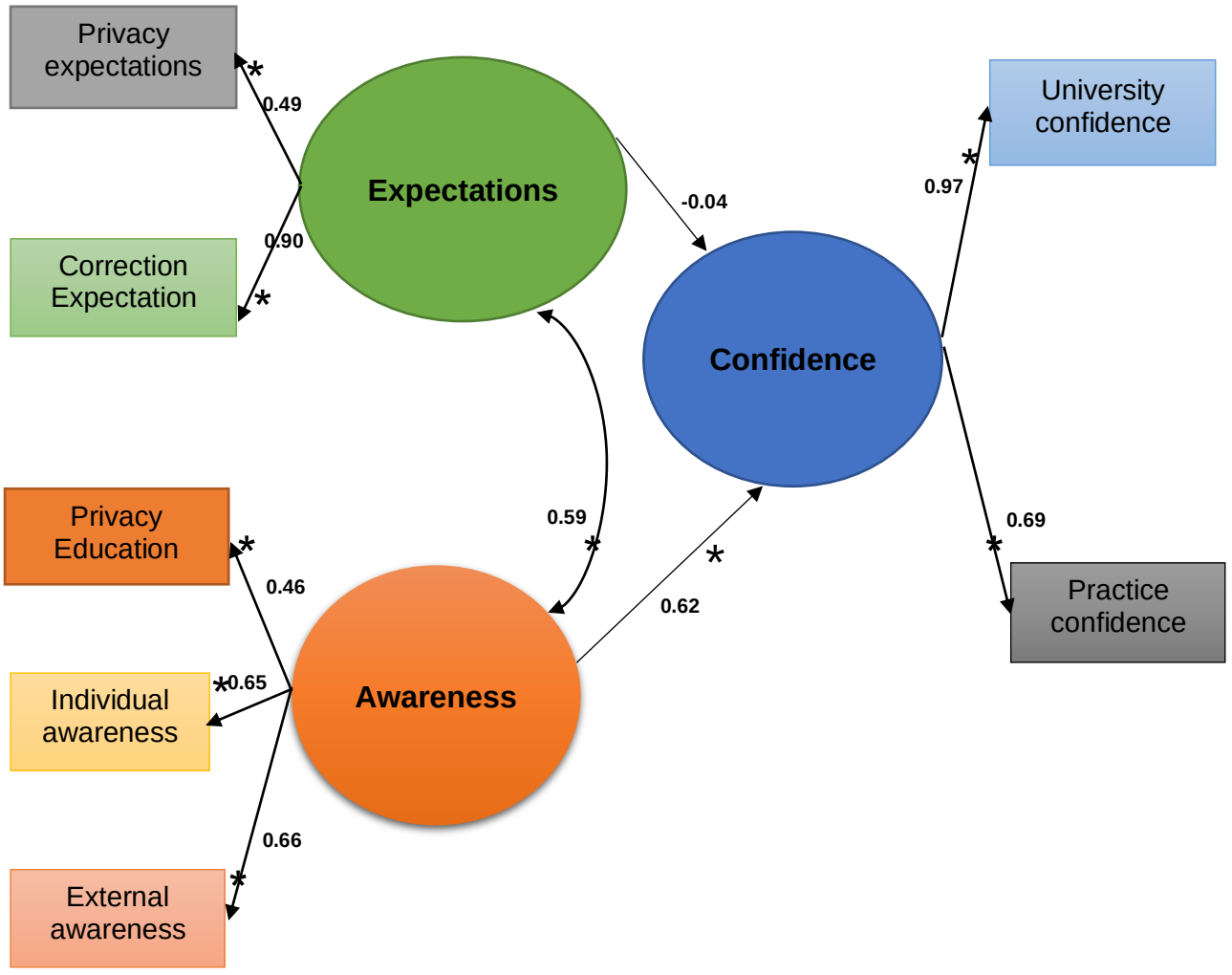
Component	**CMIN**	**df**	**CMIN/ df** **< 3 = *good*** **< 5 = *sometimes acceptable***	**PCLOSE** p> 0.05	**RMSEA** ≤ 0.06	**SRMR** ≤ 0.08	**CFI** > 0.90	**TLI** ≥ 0.90
University confidence	57.69	16	3.61	0.003	0.095	0.026	0.98	0.96
Privacy expectations	28.57	12	2.38	0.148	0.037	0.042	0.97	0.95
Individual awareness	7.99	3	2.66	0.046	0.076	0.019	0.99	0.98
Practice confidence	114.2	13	18.16	0.000	0.158	0.052	0.96	0.91
Correction expectations	13.40	7	1.91	0.354	0.056	0.031	0.99	0.97
External awareness	There were too few degrees of freedom, hence the model could not be projected.							
Privacy education	There were too few degrees of freedom, hence the model could not be projected.							

From the seven components, four (individual awareness, privacy expectations, university confidence and correction expectations) provided acceptable fit indices during CFA. The RMSEA value for the factor of practice confidence was beyond the allowed range, even though the SRMR, the TLI and the CFI were all within the permissible range. However, in applying the reasoning of Hair et al. (2014) and Hooper et al. (2008), if at least two fit indices were within the range, it was deemed as acceptable. The two remaining components (privacy education and external awareness) had insufficient degrees of freedom to calculate to estimate the fit index, hence no fit indices were calculated or estimated. This means that the model could be estimated notwithstanding the difficulty in determining the fit. There was enough evidence to proceed with the model estimates, as shown in Figure 5.

5.3 Structural Equation Modelling (SEM)

SEM confirmed the inclusion of the three major study constructs, namely expectations, awareness, and confidence. Figure 5 depicts the relationships between the various components generated and the three key constructs in the SPIPP model. The first strong associations identified indicate that privacy expectations and correction expectations were 0.49 and 0.90 respectively, thereby influencing expectations. The figure also shows that privacy education was 0.46, individual awareness was 0.65 and external awareness was 0.66, which all had a significant impact on awareness. Additionally, the diagram suggests that university confidence and practice confidence had 0.97 and 0.69 respectively, which means that both influenced confidence. The constructs of expectations and awareness had a strong link (0.59). Students' privacy confidence grew as they become more aware (0.62). As reflected in the very low score, expectations had little effect on confidence (0.03).

The model passed all the fit indices for the final information privacy perception model, including CMIN/ df, SRMR, RMSEA, PCLOSE, TLI and CFI, indicating that the model is acceptable and, as such, validated. As can be seen in Table 4, the model demonstrated an overall satisfactory fit between the theoretically hypothesised privacy model and the empirically derived structural model.



Note:
indicates a direct causal relationship.
indicates correlations between variables.
indicates an error between the predicted value and the actual value.

Figure 5: The SPIPP model (Maguraushe et al., 2021)

Table 4 shows the equivalent model fit indices for information privacy perceptions.

Table 4: Information privacy perceptions fit indices

Fit index	Attained value	Set threshold	Satisfactory fit: Yes/No
Absolute fit indices			
Chi-square (CMIN)	351.64		
Degree of freedom	194		
CMIN/ df – Relative Chi-square	1.81	< 3=*Good* < 5= *Sometimes acceptable*	Yes
PCLOSE	0.092	> 0.05	Yes
Root mean squared error of approximation (RMSEA)	0.059	≤ 0.08	Yes
Standardised root mean squared residual (SRMR)	0.041	≤ 0.08	Yes
Incremental fit indices			
Comparative Fit Index (CFI)	0.937	> 0.90	Yes
Tucker-Lewis Index (TLI)	0.921	≥ 0.90	Yes

6. Discussion and recommendations

This section discusses the findings and the practical and theoretical implications of the study.

6.1 Discussion of the findings

The first objective of the study was to create a SPIPP model measuring awareness, expectations and confidence in Zimbabwean universities. In achieving this objective, the first hypothesis (namely, that students expect their privacy to be protected when their personal information is processed) was confirmed. The following factors emerged after EFA: university confidence, practice confidence, external awareness, individual awareness, privacy education, privacy expectations and correction expectations. Figure 4 and Table 3 depict the model created using the evolving factors. The following findings on the various factors also emerged.

Privacy expectations: Students had certain expectations for how the university should manage their data. They believed that the institution should endorse the collection purpose and that this should be done at the time of collection. Furthermore, data collection should be done fairly and legally. Personal information about students should not be divulged or made public unless required by law. A university's privacy policy and privacy notices should not only exist but should also be easy to read and understand. Students expected to be able to opt in to allow the university to use their personally identifiable information and to opt-out if they were no longer interested in disclosing and sharing their information. This is consistent with the observations made by Brown and Klein (2020), who stated that institutional accountability and student agency underpin privacy solutions, that educational records are static artifacts, and that legitimate educational interests in data are broadly defined by institutions.

Correction expectations: Students anticipated that the institution would devise procedures to guarantee that their personal information was accurate, correct, current and comprehensive. They also wanted the university administrator to explain why their personal information was being collected before or during collection. After collection, the university should ensure that the information collected could be verified. As such, students would be able to edit and update their information as needed. Although in the context of learning analytics, Kimmons (2021) and Asher et al. (2022) both emphasise the significance of student privacy and trust, with students expecting institutions to guarantee the confidentiality and accuracy of their personal information.

Individual awareness: Students' degree of awareness reflected an understanding of their opt-in right if the institution requested their participation in data sharing and their opt-out right if they decided against sharing. Students were also aware that the university should be prohibited from disclosing or sharing their personal information without their permission. More importantly, they were mindful of the fact that they would have to follow a specific procedure if they required access to personal information collected about them. In a different yet similar study, Ozturk, Eyuboglu, and Baykara (2022) underlined the value of education in raising students' privacy awareness and stressed the necessity of education, especially in issues related to health.

Privacy education: Apart from personal knowledge, the institution should be aware that the aim of collecting students' personal information should be specified. Such a purpose must be expressed at the onset of data collection and the institution must substantiate it to the contentment of the students throughout the process. As stated by Alier et al. (2021), educational institutions should collect students' personal information with a clear purpose and transparency, and they should also convey the purpose to students.

External awareness: Another important factor is privacy education because it raises awareness. Students needed to be reminded regularly of privacy issues to raise their awareness levels. Newsletters, notifications, and publications could all be used for this purpose. Furthermore, awareness could be raised by offering privacy training, which should be a top priority at institutions. This is concurred by Mohammed (2022), who emphasised the value of privacy awareness in lowering threats to student information.

University confidence: Based on the results, this indicated an area requiring attention, and the university should aim to improve its performance in this regard. To instil student trust in the university, the institution should first obtain consent from students to process their personal information. If the purpose of collection is defined before collection, there is a likelihood of the students gaining confidence in the collection process. Furthermore, students will trust an institution that does not share or divulge their personal information, unless this is required by law. The publication of privacy rules would assist in boosting students' confidence regarding privacy-related issues. As noted by Jones (2019), open and clear permission procedures and privacy policies might help students feel more confident in a university, although their study context was about learning analytics approaches.

Practice confidence: How the university handled and used students' personal information would either instil or destroy trust; furthermore, the option of opting in or out would enhance student confidence in privacy matters at the university. Privacy education at the university would also promote confidence, as would constant reminders regarding privacy issues. Additionally, a university privacy policy and privacy notifications would serve as privacy practices that would build student confidence in the institution. Law and Le (2023) emphasised the need for more research on the dynamics of trust in universities' connections with society, especially with the larger populations they serve like the students.

Therefore, the privacy model that was developed measured the three constructs with respect to Zimbabwean students within a university and in line with studies conducted previously. For instance, on awareness, Kyobe (2010) contends that educational institutions have a responsibility to educate students about the need of protecting their privacy online. This is also highlighted by Fink (2012), who found that knowledge using privacy policies was essential in reducing privacy issues. Students' expectations were also discussed, and the results agreed with the findings of Pelteret and Ophoff (2016) that personal information should be used in accordance with the wishes of the individuals and not be disclosed to third parties without the data subject's consent. Students also expect and believe that their personal information should not be disclosed unless it is required by law. Therefore, the university must disclose the purposes for collecting students' personal information before doing so. Lastly, on confidence, Sherman (2019) cited by Da Veiga and Ophoff (2020) suggested that consumers (students) appeared to be particularly worried about how organisations (institutions) use their personal information, which had an impact on their trust in those organisations

(institutions). It follows that if a university commits to upholding privacy, it fosters faith and trust, which inspires confidence and results in a favourable perception of privacy that is visible throughout the entire institution (Chua et al., 2017). By insinuation, it can be claimed that trust is the root of confidence (Shen et al., 2019).

The second objective was to use SEM to validate the SPIPP model. SEM was conducted on the theoretical SPIPP model, and the model fit indices (see Table 4) were recorded. The model displayed absolute and incremental good fit indices. This objective was achieved, and a model was validated using the CMIN, CMIN/ df, PCLOSE, RMSEA, SRMR, CFI and TLI (as depicted in Table 4). The final validated SPIPP model is portrayed in Figure 5. The three key constructs (awareness, expectations and confidence) were included, as proven by the SEM. Privacy expectations, correction expectations, privacy education, individual awareness, external awareness, university confidence and practice confidence were also validated as extracted elements from the factor analysis. This is consistent with the results of Feri et al. (2016) and Vail et al. (2008), namely that people (students) expect an organisation (university) to protect their personal information with care and comply with the applicable privacy standards. According to the model, correction expectations and privacy expectations are important components in the establishment of a university student privacy model, as they enable students to trust in the university's ability to protect their personal information. Based on this, students want universities to keep their personal information private. With students being aware of their privacy obligations and an institution honouring its commitments, the result is the evolvement of trust in the institution and hence confidence (Alnatheer et al., 2012).

The third objective was to identify the association between the three constructs (awareness, expectations, and confidence). This objective was analogous to the second hypothesis, that a relationship exists between expectations, awareness, and confidence (as supported by Figure 5 and Appendix 2). While privacy education, individual awareness and external awareness were the main indicators for instilling awareness within a university, privacy expectations and correction expectations were the indicators of students' privacy expectations within universities. The factors showed small, medium, and large positive relationships using the PPMCC, which is confirmed in Appendix 2. SEM also confirmed some direct causal associations between the variables, indicating that university confidence and practice confidence were the main indicators of confidence. The Pearson correlation coefficient assisted in determining the association between the three study constructs. The empirical findings supported Hypothesis 2, namely that a relationship exists between expectations, awareness and confidence. The practice confidence, individual awareness and external awareness factors all indicated a positive significant relationship with university confidence. These findings were in line with Ortiz et al.'s (2018) findings, which showed a direct relationship between concern about information privacy and security awareness, which is important in demonstrating the significance of and correlation between information privacy and security. Minor (weak) positive associations were also observed, indicating that while such associations could exist, they had little impact on one another. In one research study, students were more likely to develop trust in a university if they were made aware of privacy issues (Kurkovsky and Syta, 2011). That would alleviate their privacy concerns and mitigate other unfavourable privacy attitudes.

The last hypothesis, namely the nine-dimensional privacy components measure the three privacy constructs (expectations, awareness, and confidence), was partly confirmed. SEM showed some direct causal relationships among the variables, demonstrating that practice confidence and university confidence were the most important indicators relevant to privacy confidence. Privacy education, external awareness and individual awareness were found to be the most important indicators for creating privacy awareness, while correction expectations and privacy expectations were the principal indicators affecting privacy expectations in such an institution.

There was one key unexpected finding from the research. The model did not meet the fit indices examined using CMIN/ df, RMSEA, SRMR, PCLOSE, CFI and TLI regarding external awareness and privacy education. Because there were insufficient degrees of freedom, it was impossible to evaluate the fit. Consequently, SEM analysis was used to examine the correlations in more detail. Mulia, Azzahro, & Handayani (2020) discovered that privacy concerns are shaped by a combination of internal and external factors, including information collecting and privacy awareness.

6.2 Practical implications of the research

A validated model for personal information privacy perceptions was generated as a result of the study. When universities collect and handle student information, this developed validated model could assist them in forming a better comprehension of students' privacy perceptions. Furthermore, institutions could use the model as a guide in raising privacy awareness among students, which would result in students' confidence growing in the university's ability to uphold their privacy. EFA was used to create a valid and reliable survey instrument, which was essential in the formulation of the SPIPP model.

6.3 Theoretical implications of the research

The literature provided new insights into the conceptualisation of student privacy expectations, awareness, and confidence. It revealed many privacy principles and guidelines, leading to the development of the conceptual and theoretical models shown in Figures 1, 2 and 3. These models could be used to enhance our understanding of students' perceptions of privacy in terms of expectations, awareness and confidence. Future scholars studying privacy and related theories could use the theoretical conclusions of this study to assist them in refining their searches. Overall, the findings of the study could contribute to an assessment of privacy issues in a university setting, which is significant in comprehending privacy when students are engaged.
In summary, the SEM findings revealed a strong overall match between the empirically created SPIPP model and the hypothesised SPIPP conceptual model, allowing all three study hypotheses to be accepted.

6.4 Future research directions

One institution served as the sample for the study that was carried out. It will be necessary to conduct, validate and perhaps standardise an instrument and model that are relevant to students in all the universities in Zimbabwe. The findings would produce a model that is highly implementable and reflects students from a wider spectrum. This would necessitate a bigger sample size, reflecting the views of many students on privacy. As the sample size increases, so do accuracy, dependability, and validity (Gerber and Hall, 2017). The study can be performed with the same constructs and components, but targeting perceptions in different spheres, such as consumer perceptions of privacy. Due to the extensive scope of the ZDPA provisions, it is also necessary to measure consumer awareness, expectations, and confidence to recommend appropriate corrective actions. The nature of this study was quantitative. The research can be expanded to qualitative or mixed studies because these studies are known for their thorough clarity on facts based on their examination and attempt to understand how people or groups feel about phenomena, for instance through using interviews (Creswell and Creswell, 2018). This would reveal in-depth subjective views of the participants, as opposed to generalised quantitative studies.

7. Conclusion

The study contributes toward the creation of a SPIPP model for student privacy perceptions at a university. The factors identified in the literature were investigated and adopted in the development of the SPIPP model. The SPIPP model was validated using SEM providing a theoretical contribution. The validated SPIPP model and be used by universities to raise privacy awareness and instil more trust among its students in the university's aptitude to protect the privacy of their personal information. Correction expectations and privacy expectations are significant components in designing a university privacy program because they contribute to students developing confidence in the institution's ability to secure their personal information. This study focused on a single institution in Zimbabwe. In future studies, an appropriate instrument for students at both public and private institutions

should be validated and standardised. Additionally, it could be argued that the study's sample size was inadequate to reflect student attitudes about privacy in institutions accurately. According to Visser et al. (2013), increasing the size of a sample reduces sampling errors and results in improved reflection of a study population's perspectives and perceptions. A bigger sample size should thus be considered in future relevant studies. It is furthermore recommended that institutions should concentrate on determining students' privacy expectations and understanding their awareness of their privacy rights. That could be accomplished by institutions reminding students of privacy issues regularly through privacy awareness education and the use of privacy newsletters, magazines, and notifications.

Acknowledgement

The researchers appreciate the assistance they received from University of South Africa (UNISA)'s Postgraduate Bursaries Administration Office. This research was approved by the UNISA Research Ethics Committee (Ethical Clearance Number: 030/KM/2019/CSET_SOC).

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Adelola, T., Dawson, R., & Batmaz, F. (2014). Privacy and data protection in e-commerce: The effectiveness of a government regulation approach in developing nations, using Nigeria as a case. The 9th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 234–239. https://doi.org/10.1109/ICITST.2014.7038812

Alghamdi, F. A., Alanazi, W. S., & Snoussi, S. (2023). Awareness of Mobile operating system privacy among computer science students. In 2023 1st International Conference in Advanced Innovation on Smart City, ICAISC, 1–5. https://doi.org/10.1109/ICAISC56366.2023. 10085581

Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C. R., & Fonseca, D. (2021). Privacy and E-Learning: A pending task. Sustainability, 13(16), 1–17. https://doi.org/10.3390/ su13169206

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. In Proceedings of the 16th Pacific Asia Conference on Information Systems, 144, 1–15. Ho Chi Minh City, Vietnam.

Anjum, A., Malik, S. R., Choo, K. K. R., Khan, A., Haroon, A., Khan, S., Khan, S. U., Ahmad, N., & Raza, B. (2018). An efficient privacy mechanism for electronic health records. Computers & Security, 72, 196–211. https://doi.org/10.1016/j.cose.2017.09.014

Asher, A. D., Briney, K. A., Jones, K. M., Regalado, M., Perry, M. R., Goben, A. H., Smale, M. A., & Salo, D. (2022). Questions of trust: A survey of student expectations and perspectives on library learning analytics. The Library Quarterly, 92(2), 151–171. https://doi.org/10.1086/718605

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. Journal of Retailing and Consumer Services, 52, 101947. https://doi.org/10.1016/j.jretconser.2019.101947

Barth, S., De Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviours among users with technical knowledge, privacy awareness, and financial resources. Telematics and Informatics, 41, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Bentinck, S. A., Van Oel, C. J., & Van Dorst, M. J. (2020). Perception of privacy in a university building: The transparency paradox. Frontiers of Architectural Research, 9(3), 579–587. https://doi.org/10.1016/j.foar.2020.03.004

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Information Systems Education Journal, 18(1), 48–58. https://files.eric.ed.gov/fulltext/EJ1246231.pdf

Boardman, R., Mullock, J., & Mole, A. (2020). Guide to the General Data Protection Regulation.

Botnevik, S., & Khalil, M. (2020). Student awareness and privacy perception of learning analytics in higher education. In C. Alario-Hoyos, M. J. Rodríguez-Triana, M. Scheffel, I. Arnedillo-Sánchez, & S. Dennerlein (Eds.), Addressing glob. challenges qual. educ (pp. 374–379). Springer International Publishing. https://doi.org/10.1007/ 978-3-030-57717-9

Brooks, D. C. (2016). ECAR Study of Undergraduate Students and Information Technology. https://doi.org/10.3389/feduc.2022.914857

Brown, M. G., & Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. The Journal of Higher Education, 91(7),1149–1178. https://doi.org/10.1080/00221546.2020.1770045

Burdon, M., Lane, B., & Von Nessen, P. (2012). Data breach notification law in the EU and Australia – where to now? Computer Law & Security Review, 28(3), 296–307. https://doi.org/10.1016/j.clsr.2012.03.007

Callanan, C., Jerman-Blažič, B., & Blažič, A. J. (2016). User awareness and tolerance of privacy abuse on mobile inter- net: An exploratory study. Telematics and Informatics, 33(1), 109–128. https://doi.org/10.1016/j.tele.2015.04.009 Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. Computer Standards and Interfaces, 42, 24–31. https://doi.org/10.1016/j.csi.2015.04.001

Cate, F. H. (2006). The failure of fair information practice principles. In J. Winn (Ed.), Consumer protection in the age of the'Information Economy' (pp. 341–378). Routledge.

Cavoukian, A. (2009). Privacy by design – the 7 foundational principles: Implementation and mapping of fair information practices. Information and Privacy Commissioner of Ontario, Canada, 5. https://doi.org/10.1007/s12394010-0062-y

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. Government Information Quarterly, 35(3), 445–459. https:// doi.org/10.1016/j.giq.2018.04.002

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

Chetty, P. (2013). Presentation on Zimbabwe Data Protection Bill.

Choi, H. S., Lee, W. S., & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modelling. Computers & Security, 67, 244–253. https://doi.org/10.1016/j.cose.2017.03.007

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. https://doi.org/10.1016/j.tele.2017.01.008

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. Technological Forecasting, 161, 120299. https://doi.org/10.1016/j.techfore.2020.120299

Cohen, L., Manion, L., & Morrison, K. (2011). Research meth- ods in education (7th ed.). Routledge.

Cole, J. (2021). The family educational rights and privacy act (FERPA). Legal Issues, 1–17.

Coleman, L., & Purcell, B. M. (2015). Data breaches in higher education. Journal of Business Cases and Applications, 15(3), 1–7. https://www.aabri.com/manu scripts/162377.pdf

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

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (5th ed.). Los Angeles, USA: SAGE Publications.

Das, M. C. (2022). Data privacy on the internet: A study on awareness and attitudes among the students of the University of Chittagong in Bangladesh. Advances in Journalism and Communication, 10(2), 70–80. https://doi.org/10.4236/ajc.2022.102006

Da Veiga, A. (2018). An online information privacy culture: A framework and validated instrument to measure consumer expectations and confidence. In 2018 Conference on Information Communications Technology and Society, 26, 1–6. 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. https://doi.org/10.1016/j.clsr.2015.01.005

Da Veiga, A., & Ophoff, J. (2020). Concern for information privacy: A cross-nation study of the United Kingdom and South Africa, vol. 1. Springer International Publishing. https://doi.org/10.1007/978-3-030-57404-8

Degroot, J. M., & Vik, T. A. (2017). "We were not prepared to tell people yet": Confidentiality breaches and boundary turbulence on Facebook. Computers in Human Behavior, 70, 351e359. https://doi.org/10.1016/j.chb.2017.01.016

De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection regulation replacing directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review, 28(2), 130–142. https://doi.org/10.1016/j.clsr.2012.01.011

Dervishi, R., Neziri, V., & Rexha, B. (2022). Transactions privacy on the blockchain using a web of trust concept. Information Security Journal, 00, 1–13. https://doi.org/10. 1080/19393555.2022.2100844

De Wolf, R., Martens, M., Vanden Abeele, M., & De Marez, L. (2023). Predicting teens' privacy management and attitude toward data protection on social media. Cyberpsychology, Behavior, and Social Networking, 26(3), 153–160. https://doi.org/10.1089/cyber.2021.0338

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

Elegbeleye, F. A., Mbodila, M., Mabovana, A., & Esan, O. A. (2022). Data privacy on using four models – a review. In 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–9. https://doi.org/10.1109/ICE-CET55527.2022.9872999

Ellis, J. L. (2017). Factor analysis and item analysis. https://www. applyingstatisticsinbehaviouralresearch.com/documenten/factor_analysis_and_item_analysis_version_11_.pdf

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, London, UK, 280–286. https://doi. org/10.1109/ICITST.2015.7412106.

Fatima, R., Affan, Y., Liu, L., Wag, J., Afzal, W., & Awaid, Y. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using the serious game. Journal of Information Security and Applications, 48, 102351. https://doi.org/10.1016/j.jisa. 2019.06.007

Feri, F., Giannetti, C., & Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. Journal of Economic Behavior and Organization, 123, 138–148. https://doi.org/10.1016/j.jebo.2015.12.001

Fink, C. (2012). Privacy and confidentiality in the virtual class- room: Instructor perceptions, knowledge and strategies. University of Victoria.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. European Research on Management and Business Economics, 22(3), 167–176. https://doi.org/10.1016/j.iedeen.2016.04.002

Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: A GDPR label perspective. Information Technology & People, 35(8), 181–204. https:// doi.org/10.1108/ITP-09-2021-0706

Future of Privacy Forum. (2021). Higher education voices: College students' attitudes toward data privacy. 1–16. https://studentprivacycompass.org/resource/higheredvoices2021

Gellman, R. (2017). Fair information practices: A basic history. https://doi.org/10.2139/ssrn.2415020.

Gerber, H., & Hall, R. (2017). Quantitative research design. HR Statistics.

Greenfield, T., & Greener, S. (2016). Research methods for postgraduates (3rd ed.). John Wiley & Sons Inc. https://doi.org/10.1002/9781118763025

Gruzd, A., & Hernández-García, Á. (2022). A balancing act: How risk mitigation strategies employed by users explain the privacy paradox on social media. Behaviour & Information Technology, 43(1), 21–39. https://doi.org/10.1080/0144929X.2022.2152366

Guffin, P., & FIPPs and PIA. (2017). State of the judicial branch. https://www.courts.maine.gov/maine_courts/committees/tap/FIPPs-and-PIA-email.pdf

Hair, J. F., Black, W. C., Babbin, B. J., & Anderson, R. E. (2014). Multivariate data analysis (7th ed.). Pearson Education Limited. https://doi.org/10.1007/978-3-319-01517-0_3

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Computers in Human Behavior, 68, 217–227. https://doi.org/10.1016/j.chb.2016. 11.033

Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 51(1), 51–69. https://doi.org/10. 1145/3380799.3380805

Hasbullah, N. A., Md Noor, N. L., & WARWM, I. (2013). Towards t-government in Malaysia: Investigation of citizens' willingness to participate in democratic services and information privacy concern. In International Conference on Research and Innovation in Information Systems (ICRIIS), 366–369. https://doi.org/10.1109/ICRIIS.2013. 6716737.

Holbrook, A. L., Krosnick, J. A., & Pfent, A. (2007). The causes and consequences of response rates in surveys. Adv Teleph Surv Methodol, 599–678. https://doi.org/10.1002/ 9780470173404.ch23

Hooda, M., & Yadav, B. (2017). Perceptions of millennials towards social media privacy issues: A survey. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE. https://doi.org/10.1109/CTCEEC.2017.8455161

Hoofnagle, C. J., Van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural equation modelling: Guidelines for determining model fit. Electronic Journal of Business Research Methods, 6(1). https://doi.org/10.21427/D7CF7R

Hossain, A. A., & Zhang, W. (2015). Privacy and security concerns of online social networks from a user perspective. In 2015 1st International Conference on Information Systems Security and Privacy (ICISSP) Angers, France: IEEE.

Huang, H., & Bashir, M. (2016). Privacy by region: Evaluation of online users' privacy perceptions by geographical region. In 2016 Future Technologies Conference. IEEE. https://doi. org/10.1109/FTC.2016.7821721

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, structural equation modelling. Structural Equation Modelling: A Multidisciplinary Journal, 6(1), 1–55. https://doi.org/10.1080/10705519909540118

Isabwe, G. M. N., & Reichert, F. (2013). Revisiting students' privacy in computer-supported learning systems. International Conference on Information Society, Toronto, ON, Canada, 256–262.

Ivanova, M., Grosseck, G., & Holotescu, C. (2015). Researching data privacy in e-learning. In 2015 International Conference on Information Technology Based Higher Education and Training (ITHET). https://doi.org/10.1109/ITHET.2015.7218033

Johnston, A., & Wilson, S. (2012). Privacy compliance risks for Facebook. IEEE Technology and Society Magazine, 31, 59–64. https://doi.org/10.1109/MTS.2012.2185731

Jones, K. M., & Afnan, T. (2019). "For the benefit of all students": Student trust in higher education learning analytics practices. Proceedings of the Association for Information Science and Technology, 56. https://doi.org/10.1002/pra2.132

Kaneen, C. K., & Petrakis, E. G. M. (2020). Towards evaluating GDPR compliance in IoT applications. 24th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, 176, 2989–2998. https://doi.org/10.1016/j.procs.2020.09.204

Katurura, M., & Cilliers, L. (2016). The extent to which the POPI Act makes provision for patient privacy in mobile personal health record systems. In 2016 IST-Africa Week Conference, Durban, South Africa: IEEE, p. 1–8. https://doi.org/10.1109/ISTAFRICA.2016.7530595.

Kävrestad, J., Furnell, S., & Nohlberg, M. (2023). User perception of context-based micro-training – a method for cyber- security training. Information Security Journal, 33, 1–17. https://doi.org/10.1080/19393555.2023.2222713

Kazi, A. M., & Khalid, W. (2012). Questionnaire designing and validation. Journal of the Pakistan Medical Association, 62(5), 514–516. https://pubmed.ncbi.nlm.nih.gov/ 22755326/

Kim, B., & Kim, D. (2020). Understanding the key antecedents of users' disclosing behaviours on social networking sites: The privacy paradox. Sustainability, 12(12), 12. https://doi. org/10.3390/su12125163

Kimmons, R. (2021). Safeguarding student privacy in an age of analytics. Educational Technology Research & Development, 69(1), 343–345. https://doi.org/10.1007/ s11423-021-09950-1

Kim, D., Park, K., Park, Y., & Ahn, J. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. Computers in Human Behavior, 92, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kizilcec, R. F., Viberg, O., Jivet, I., Martinez Mones, A., Oh, A., & Hrastinski, S., et al. (2023). The role of gender in students' privacy concerns about learning analytics: Evidence from five countries, vol. 1. Association for Computing Machinery. https://doi.org/10.1145/3576050.3576142

Kline, R. B. (2011). Principles and practice of structural equation modelling. The Guilford Press.

Knijnenburg, B. P., Page, X., Wisniewski, P., Richter, H., Proferes, N., & Romano, J. (2022). Modern socio-technical perspectives on privacy. Springer. https://doi.org/10.1007/ 978-3-030-82786-1

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 34, 122–134. https://doi.org/10.1016/j.chb.2018.01.028

Korff, B. D., & Georges, M. (2019). The DPO handbook guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 1–245.

Krempel, E., & Beyerer, J. (2018). The EU General Data Protection Regulation and its effects on designing assistive environments. In Proceedings of the 11th Pervasive Technologies Related to Assistive Environments Conference, New York, USA: ACM, 327–330. https://doi.org/10.1145/ 3197768.3201567.

Kruikemeier, S., Boerman, S. C., & Bol, N. (2020). Breaching the contract? Using social contract theory to explain individuals' online behaviour to safeguard privacy. Media Psychology, 23(2), 269–292. https://doi.org/10.1080/ 15213269.2019.1598434

Krzych, Ł. J., & Ratajczyk, D. (2013). Awareness of the patient's rights by subjects on admission to a tertiary university hospital in Poland. Journal of Forensic and Legal Medicine, 20(7), 902–905. https://doi.org/10.1016/j.jflm.2013.06.006

Kumar, R. (2011). Research methodology: A step-by-step guide for beginners (3rd ed.). Sage Publications.

Kumaraguru, P., & Cranor, L. (2005). Privacy indexes: A survey of Westin's studies. Institution Software Research International, 1–22.

Kuperus, D. (2016). Security and privacy perceptions of millennials vs non-millennials in digital environments. 7th IBA Bachelor Thesis Conference, 1–8. Enschede, Netherlands.

Kurkovsky, S., & Syta, E. (2011). Monitoring of electronic communications at universities: Policies and perceptions of privacy. In Proceedings on 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 1–10. https://doi.org/10.1109/HICSS.2011.312.

Kyobe, M. (2010). Towards a framework to guide compliance with IS security policies and regulations in a university. In 2010 Proceedings on Information Security for South Africa Conf (ISSA), 1–6. https://doi.org/10.1109/ISSA.2010.5588651

Larrucea, X., Asaf, S., & Santamaria, I. (2020). Towards a GDPR-compliant way to secure European cross-border healthcare industry 4.0. Computer Standards and Interfaces, 69, 1–7. https://doi.org/10.1016/j.csi.2019.103408

Law, S. F., & Le, A. T. (2023). A systematic review of empirical studies on trust between universities and society. Journal of Higher Education Policy and Management, 45(4), 393–408. https://doi.org/10.1080/1360080X.2023.2176598

Lawler, J., & 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. https://dl.acm.org/doi/abs/10.5555/1859159.

Maguraushe, K. (2021). Development of a Diagnostic Instrument and Privacy Model for Student Personal Information Privacy Perceptions at a Zimbabwean University [Doctoral thesis]. University of South Africa. http://hdl.handle.net/10500/27557

Maguraushe, K., Da Veiga, A., & Martins, N. (2019). A conceptual framework for a student personal information privacy culture at universities in Zimbabwe. In 2019 Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems, Kalpa Publications in Computing, 12, 143–156. Johannesburg, South Africa.

Maguraushe, K., Da Veiga, A., & Martins, N. (2020). Validation of an information privacy perception instrument at a Zimbabwean University. In N. Clarke & S. Furnell (Eds.), Human aspects of information security and assurance. HAISA 2020. IFIP advances in information and communication technology (Vol. 593, pp. 300–314). Springer. https://doi.org/10.1007/978-3-030-57404-8_23

Malandrino, D., Scarano, V., & Spinelli, R. (2013). How increased awareness can impact attitudes and behaviours toward online privacy protection. In 2013 International Conference on Social Computing. IEEE. https://doi.org/10.1109/SocialCom.2013.15

Mamonov, S., & Benbunan-Fich, R. (2015). An empirical investigation of privacy breach perceptions among smart- phone application users. Computers in Human Behaviour, 49, 427–436. https://doi.org/10.1016/j.chb.2015.03.019

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviours. Computers in Human Behaviour, 83, 32–44. https://doi.org/10.1016/j.chb.2018.01.028

Martin, K. (2020). Breaking the privacy paradox: The value of privacy and associated duty of firms. Business Ethics Quarterly: The Journal of the Society for Business Ethics, 30, 65–96. https://doi.org/10.1017/beq.2019.24

Martin, K. E. (2015). Understanding privacy online: Development of a social contract approach to privacy. Journal of Business Ethics, 137(3), 551–569. https://doi. org/10.1007/s10551-015-2565-9

Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. M. (2015). An analysis of personal information privacy concerns using Q-Methodology. In Proceedings of the 26th Australasian Conference on Information Systems, 1–10. https://arxiv. org/abs/1606.03547

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., Wang, Y., & Weaven, S. K. (2020). Data privacy in retail. Journal of Retailing, 96(4), 474–489. https://doi.org/10.1016/j.jretai.2020.08.003

Ma, C., & Shek, D. (2018). Structural equation modelling. In The SAGE encyclopaedia of educational research, measurement, and evaluation (Vol. 4, pp. 1625–1629). AGE Publications, Inc. https://doi.org/10.4135/9781506326139

Masur, P. K. (2021). Understanding the effects of conceptual and analytical choices on 'finding' the privacy paradox:
specification curve analysis of large-scale survey data. Information, Communication & Society, 26(3), 584–602. https://doi.org/10.1080/1369118X.2021.1963460

Miltgen, C. L. (2009). Online consumer privacy concerns and willingness to provide personal data on the internet. International Journal of Networking and Virtual Organisations, 6(6), 574. https://doi.org/10.1504/IJNVO.2009. 027790

Mohammed, M., & Bamasoud, D. M. (2022). The impact of enhancing awareness of cybersecurity on university students: A survey paper. Journal of Theoretical and Applied Information Technology, 100(15), 4756–4766.

Mohammed, Z. A., & Tejay, G. P. (2017). Examining privacy concerns and e-commerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. Computers & Security, 67, 254–265. https://doi.org/10.1016/j.cose.2017.03.001

Mohamud, I. K., Saidin, A. Z., & Zeki, A. M. (2017). Attitude towards information property rights among students: The case of International Islamic University Malaysia. In 2017 4th International Conference on User Science and Engineering, i-USEr, 145–148. Melaka, Malaysia.

Mulia, R. A., Azzahro, F., & Handayani, P. W. (2020). Analysis of internal and external factors affecting online privacy concern in E-commerce: Comparative study by gender. In 2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS), 187–192. Depok, Indonesia.

Muravyeva, E., Janssen, J., Specht, M., & Custers, B. (2020). Exploring solutions to the privacy paradox in the context of e-assessment: Informed consent revisited. Ethics and Information Technology, 22, 223–238. https://doi.org/10.1007/s10676-020-09531-5

Mutunhu, B., Dube, S., Ncube, N., & Sibanda, S. (2022). Cyber security awareness and education framework for Zimbabwe universities: A case of National University of Science and Technology. In Proceedings of the International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria, 5–7. https://ieomsociety.org/proceedings/2022nigeria/111.pdf

Ncube, C. B. (2016). Data protection in Zimbabwe. African Data Privacy Laws, Law Governance Technology Services, 33, 99–116. https://doi.org/10.1007/978-3-319-47317-8_5

Neuman, L. W. (2014). Social research methods: Qualitative and quantitative approaches. Pearson Education Limited.

OAIC. (2015). Privacy management framework. Office of the Australian Information Commissioner.

OECD. (2013). Recommendation of the council concerning guidelines governing the protection of privacy and trans- border flows of personal data (2013). OECD Privacy Framework, 11–37.

Ortiz, J., Chih, W. H., & Tsai, F. S. (2018). Information privacy, consumer alienation, and lurking behaviour in social networking sites. Computers in Human Behaviour, 80, 143–157. https://doi.org/10.1016/j.chb.2017.11.005

Ozturk, D., Eyuboglu, G., & Baykara, G. Z. (2022). Privacy consciousness of university students. Gazi Sağlık Bilimleri Dergisi, 7(4), 68–77. https://doi.org/10.52881/gsbdergi.1014500

Park, J., & Vance, A. (2021). Data privacy in higher education: Yes, students care. Educational Review. https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. Informing Science: The International Journal of an Emerging Transdiscipline, 19, 277–301. https://doi.org/10.28945/3573

Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. International Journal of Information Systems & Project Management, 9(1), 38–53. https://doi.org/10.12821/ijispm090102

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

Rao, A. A., Chen, L. F., & Dhillon, J. S. (2014). A preliminary study on online data privacy frameworks. In Proceedings of the 6th International Conference on Information Technology and Multimedia, Putrajaya, Malaysia: IEEE, 15–20. https://doi.org/10.1109/ICIMU.2014.7066596.

The Republic of Zimbabwe. (2021). The Data Protection Act, vol. 41. https://doi.org/10.1108/eb051133

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

Rossiter, D. G. (2017). Technical note: An example of statis- tical data analysis using the R environment for statistical computing.

Salleh, N., Hussein, R., Mohamed, N., & Aditiawarman, U. (2013). An empirical study of the factors influencing information disclosure behaviour in social networking sites. In International Conference on Advanced Research in Computer Science and Information Technology, 181–185. https://doi.org/10.1109/ACSAT.2013.43

Samani, A., Ghenniwa, H. H., & Wahaishi, A. (2015). Privacy in the Internet of Things: A model and protection framework. Procedia Computer Science, 52, 606–613. https://doi.org/10.1016/j.procs.2015.05.046

Sandesh, J., Dubey, S., & Sandhya, J. (2016). Designing and validation of a questionnaire. International Dental & Medical Journal of Advanced Research – VOLUME 2015, 2(1), 1–3. https://doi.org/10.15713/ins.idmjar.39

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

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for business students (7th ed.). Pearson.

Schrameyer, A. R., Graves, T. M., Hua, D. M., & Brandt, N. C. (2016). Online student collaboration and FERPA considerations. Tech Trends, 60(6), 540–548. https://doi. org/10.1007/s11528-016-0117-5

Schumacher, C., & Ifenthaler, D. (2018). Features students really expect from learning analytics. Computers in Human Behavior, 78, 397–407. https://doi.org/10.1016/j.chb.2017.06.030

Schwaig, S. K., Kane, G. C., & Storey, V. C. (2006). Compliance with the fair information practices: How are the Fortune 500 handling online privacy disclosures? Information & Management, 43(7), 805–820. https://doi.org/10.1016/j.im.2006.07.003

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. Information & Management, 50(1), 1–12. https://doi.org/10.1016/j.im.2012.11.002

Shen, N., Bernier, T., Sequeira, L., Strauss, J., & Pannor, M. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. International Journal of Medical Informatics, 125, 1–12. https://doi.org/10.1016/j.ijmedinf.2019.01.014

Sherman, E. (2019). Theory, not practice, says new study. Fortune. International Journal of Medical Informatics, 125, 1–12. https://fortune.com/2019/02/25/consumers-data-privacy/

Smit, M., Lyons, K., McAllister, M., & Slonim, J. (2009). Detecting privacy infractions in applications: A framework and methodology. In 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 694–701. https://doi.org/10.1109/MOBHOC.2009.5336935.

Sodiya, A. S. & Adegbuyi, B. (2019). A Framework for Protecting Users' Privacy in Cloud. In Information Reso Management Association (editor.), Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 378–389). IGI Global. https://doi.org/10.4018/978-1-5225-7113-1.ch021.

Stange, C. (2011). Privacy concern and student engagement in the virtual classroom. University of Victoria.

Swartz, P., & Da Veiga, A. (2016). PoPI act – opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment. 2016 Information Security for South Africa (ISSA) Conference, 9–17. https://doi.org/10.1109/ISSA.2016.7802923.

Talib, S., Ismail, N. A., Olowolayemo, A., Syed Naser, S. A., Haron, S. Z., & Mohammad Yusof, A. H. (2014). Social networks privacy policy awareness among undergraduate students: The case of Twitter. In The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M). https://doi.org/10.1109/ICT4M.2014.7020674.

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Tan, A. Z. Y., Yong Chua, W., & Chang, K. T. T. (2014). Location-based services and information privacy concerns among literate and semi-literate users. In 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA: IEEE, 3198–3206. https://doi.org/10.1109/HICSS.2014.394.

Teufel, H. (2008). The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security. Memorandum Number: 2008-01. https://www.dhs.gov/sites/default/files/202401/Fair%20Information%20Principles_12_2008.pdf

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

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

Van der Merwe, M. D., & Van Staden, W. J. C. (2015). Unsolicited short message service marketing: A preliminary investigation into individual acceptance, perceptions of content, and privacy concerns. In 2015 Information Security for South Africa (ISSA) (pp. 1–7). IEEE. https://doi.org/10.1109/ISSA.2015.7335072

Victor, N., Lopez, D., & Abawajy, J. H. (2016). Privacy models for big data: A survey. Big Data Intel, 3(1), 61–75. https://doi.org/10.1504/IJBDI.2016.073904

Visser, P. S., Krosnick, J. A., & Lavrakas, P. J. (2013). Survey research. In H. Reis & C. Judd (Eds.), Handbook res. Methods soc. Personal. Psychol (pp. 1–30). Cambridge University Press.

Willems, J., Schmid, M. J., Vanderelst, D., Vogel, D., & Ebinger, F. (2022). AI-driven public services and the privacy paradox: Do citizens really care about their privacy? Public Management Review, 25(11), 2116–2134. https://doi.org/10.1080/14719037.2022.2063934

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. 33rd International Conference Information Systems, 1–16. https://doi.org/10.1037/t44647-000

Zeide, E., & Nissenbaum, H. (2018). Learner privacy in MOOCs and virtual education. Theory and Research in Education, 16, 280–307. https://doi.org/10.1177/1477878518815340

Zlatolas, L. N., Welzer, T., Hölbl, M., Hericko, M., & Kamisalic, A. (2019). A model of perception of privacy, trust, and self-disclosure on online social networks. Entropy, 21(8), 772–800. https://doi.org/10.3390/e21080772