The African Journal of Information Systems

Volume 13 | Issue 1 Article 1

December 2020

# Emerging Internet Technologies and the Regulation of User Privacy

Phil Nyoni
philnyoni@gmail.com

Mthulisi Velempini
*University of Limpopo*, mvelempini@gmail.com

Nehemiah Mavetera
*North West University*, nehemiah.mavetera@nwu.ac.za

The African Journal of Information Systems

# Emerging Internet Technologies and the Regulation of User Privacy

**Research Paper**

**Volume 13, Issue 1, January 2021, ISSN 1936-0282**

**Phil Nyoni**
North-West University
philnyoni@gmail.com

**Mthulisi Velempini**
University of Limpopo
mvelempini@gmail.com

**Nehemiah Mavetera**
North-West University
nehemiah.mavetera@nwu.ac.za

(*Received November 2019, accepted September 2020*)

## ABSTRACT

Modern Internet-based technologies pose a threat to privacy, as they possess multiple sensors or features that collect data about users. There is a need to determine the privacy risks that affect users in South Africa as there are a few studies on the subject. A qualitative study was done which involved interviewing seven experts and a survey consisting of 101 respondents. The results show that regulators view emerging technologies as potentially risky and are motivated by public interest to develop protective laws. It therefore is necessary that regulators develop robust laws to help prevent privacy violations. Furthermore, this paper proposes a conceptual framework that conceptualizes how emerging technologies affect users to inform policymaking.

## Keywords

Conceptual Framework, Data Protection, Emerging Technologies, Privacy, Privacy Calculus, Regulation, Technological Risk.

## INTRODUCTION

Emerging technologies are defined as new technologies that are coming into prominence and changing the way things currently are being done (Narayanan & O'Connor, 2015). One of the characteristics that distinguishes them from other technologies is their converging technology. This means that they have overlapping elements—they are embedded and connected (Herkert, 2011). For example, Internet of Things (IoT) devices rely on having both sensor and wireless networking technology. Smart devices are being used in healthcare, surveillance, and household electronics (Klitou, 2014).

One question raised by researchers is about the social impact of these new technologies (Lucivero, 2016; Aydos, Vural, & Tekerek, 2019). Recent international studies have highlighted the impact of these new technologies (Leenes, 2019; Urquhart, 2018; Bowman et al., 2017; Wright & de Hert, 2016). They show that personal data shared with other devices over the Internet has an impact on users' privacy (Johnson, 2019; Urquhart, 2018). This personal data makes them valuable to interested parties like hackers (Johnson, 2019; Peppet, 2014). The area of data protection in South Africa is, however, relatively understudied. Some of these studies are conceptual in nature, meaning no evidence has been obtained directly from regulators on the technological risks users face. This has left a gap regarding the factors that contribute to the loss of user privacy.

Privacy issues have become a major concern for users, prompting organizations to make note of them. Businesses that collect consumers' data for its commercial value have to be held accountable for their actions in storing and using this data (Corones & Davis, 2017; Conger et al., 2013). An example is when Facebook purchased Instagram and WhatsApp, thereby expanding their data collection capabilities. The integration of these platforms allows for cross-messaging across different platforms, which may be a challenge, as only WhatsApp has end-to-end encryption (Winder, 2019). This potentially could lead to the interception of messages by hackers (Winder, 2019).

Regulators face challenges when it comes to developing legislation that adequately covers innovations which process and store personal data. One of these challenges is the failure of the law to keep up with innovation (also known as the pacing problem) which leads to the creation of ineffective legislation for new technologies (Eggers et al., 2018; Butenko & Larouche, 2015). This is caused often by the rate at which technology keeps changing as well as regulators not understanding fully how these innovations operate; for example, Internet-of-Things (IoT) devices (Peppet, 2014). It therefore is necessary to understand data protection from a public policy perspective, as it helps to establish the importance of privacy in the law and how it can be protected moving forward. Regulating these technologies can help to mitigate the risks associated with using them (Ludlow et al., 2015).

Therefore, the purpose of our research was to determine if emerging technologies pose a threat to personal data and to highlight the privacy risks users face. This led to the development of an integrated framework for the regulation of privacy in emerging technologies. This required capturing the perspectives of experts regarding privacy regulation. The findings of the study will inform the decision-making of policymakers. Businesses and users will benefit also as privacy laws are improved, resulting in better data protection.

The rest of the paper is structured as follows: the next Section discusses the technological risks new technologies pose to users as well as the South African regulatory context in relation to privacy. This is followed by the research methodology, which is then followed by the results Section. Our conceptual framework, which was developed based on the results, is presented along with a general discussion of the main results. The paper concludes with some recommendations and guidelines for future research.

## LITERATURE REVIEW

### Regulation

Regulation is defined as the intervention of a government in markets to deal with suspected market failures (Moosa, 2015; Ogus, 2004). A concept related to regulation is data protection, which is a set of rules regarding the collection, processing, and storage of personal data (Zeegers, 2018). Regulation addresses market failures by solving systemic problems and deciding how funds are allocated in the manufacturing process and in distributing the multiple products (Morgan & Yeung, 2007). Regulation is

viewed as inevitable in managing different risks, whether they are diseases, inadequate safety precautions, or theft of taxpayer money by investment firms (Baldwin et al., 2012). Regulation is aimed mainly at gathering information, setting standards, and changing the actions of markets (Baldwin et al., 2012).

Regulation is necessary to incentivize service providers to respect users' privacy (Morgan & Yeung, 2007). This is done to avoid situations where new technologies are misused to violate users' privacy (Conger et al., 2013). This should be prevented as users have sensitive data, such as financial information, children's data, and health records (Vincent, 2016). Emerging technologies are appealing to new businesses as they can offer them ways to enter the market and compete with established companies (Narayanan & O'Connor, 2015). An example of this is mobile applications which have a low barrier of entry for new developers who potentially may develop popular applications.

## South African Regulatory Context

South Africa has in its constitution a common law—a right to privacy (Ntsaluba, 2018; Roos, 2016). This is similar to the European Union which also sees privacy as a right and dedicates significant financial resources to regulatory bodies, something which can be done elsewhere, including in South Africa (Hijmans, 2016). A number of different frameworks have been proposed to solve this issue. The main one is the National Cybersecurity Policy Framework (NCPF) of 2015, Cybersecurity and Cybercrime's Bill (CCB) and Protection of Personal Information Act (POPIA) are in place (Roos, 2016; Makulilo, 2016; Subrahmanian et al., 2015). The purpose of the NCPF is to create capacity by creating cybersecurity structures that help reduce threats and vulnerabilities (SSA, 2015). It also aims to develop relationships between industry and the government regarding cybersecurity. This also extends to local and international collaborations (Subrahmanian et al., 2015). Through the NCPF, a National Cybersecurity Advisory Council has been created to coordinate all security-related activities within the country. Furthermore, a National Computer Security Incident Response Team (CSIRT) and a Cybersecurity Hub were created to deal with incidents within different industries (DTPS, 2017). The framework also emphasizes the need to build more capacity and provide more people with the skills necessary to protect the nation's information assets. It is acknowledged that the framework is broad in its coverage, leaving room for additions of any relevant aspects in the future (DTPS, 2017). Sutherland (2017) states that the NCPF has some exemptions for national security which can leave users exposed to potential privacy violations.

The CCB of 2017 was developed after the establishment of the NCPF under the control of the State Security Agency (DTPS, 2017). Many of the aims of the NCPF are shared with the CCB, with the important distinction being that this Bill focuses on cybercrime investigations. It was created in response to the increasing number of data breaches and incidents to which normal enforcement was not empowered to investigate (DLA Piper, 2019). The main aim of the CCB is to deal with cybersecurity and crimes that take place in cyberspace (DOJ, 2017). The Bill provides an organized approach towards the enforcement of penalties on criminals by requiring organizations to report any breaches and empower law enforcement entities to investigate any cybercrime (DOJ, 2017). The Law Society of South Africa (LSSA) has raised concerns over this Bill, especially its lack of reference to the significance of individual privacy (LSSA, 2017). The Bill promotes collaboration between the private and public sector.

Finally, the POPIA of 2013 seeks to reify the right to privacy, as highlighted in the constitution by requiring organizations that process South African users' data do it in a fair, responsible, and secure manner (Roos, 2016; DOJ, 2013). According to POPIA, personal information must be processed in line

with these specific guidelines: accountability, purpose specification, security safeguards, and data subject participation (DOJ, 2013). The act also applies to third parties which store and process information (Gcaza & Solms, 2017). One of the most important parts of the Act is that it provided for the creation of a national Information Regulator. The Regulator is responsible for coordinating data protection activities and it collaborates with private partners in industry to help strengthen privacy enforcement (DOJ, 2013). The establishment of an Information Protection Regulator is fundamental to user privacy protection (DLA Piper, 2019; Roos, 2016).

Criticisms from researchers about these frameworks are that they were not developed fast enough and that they lack implementation improvements designed to enhance them (Sutherland, 2017). Some frameworks are yet to be fully implemented and this leaves the country vulnerable to potential cyber-attacks (Ntsaluba, 2018). A lack of regulation has been highlighted by Gcaza and Solms (2017) as a potential threat to user privacy in South Africa.

Generally, emerging technologies were not factored into the design of these frameworks. As these frameworks were the first attempts at introducing privacy regulation, they have dealt only with general privacy violations. Our study focuses on new threats to privacy which are taking place and how they can be mitigated through regulation. It is necessary to avoid static frameworks that do not respond to the rapid pace of innovation and how they impact privacy.

## Privacy Threats and Emerging Technologies

This study adopts the data ownership definition of privacy which is stated as the right to control data flows about oneself (Westin, 1967). With this approach, it is clear that personal information is viewed as part of an individual's intellectual property and can be protected using data protection laws (Pelteret & Jacques, 2016). This right to control information allows users to limit how much data is revealed or shared (Westin, 1967). The latter view is supported by privacy experts who believe that privacy can be viewed also as a personal preference (Cohen, 2012).

Privacy researchers have stated that the Internet has become a growing concern about privacy (Moore, 2017; Belmas, Shepard, & Overbeck, 2017). A recent survey found that about 42% of South Africans had privacy concerns about their data being misused (Hootsuite, 2019). This development has led to privacy advocates calling for more data protection laws, but this has been met with resistance from certain groups who are against overregulation (Moore, 2017).

The main privacy threats identified by researchers include the sale of user data to third parties, profiling of users by web trackers, and data theft by hackers (Belmas, Shepard, & Overbeck, 2017). The South African Banking Risk Information Centre (SABRIC) has indicated that financial fraud is one of the biggest threats to South Africans' personal data (SABRIC, 2019). Indeed, press reports have shown that South Africa is the third country in Africa most exposed to cyber risks (IT News Africa, 2017). There are a number of different actors who could want to access users' personal data for various reasons. They range from spies, terrorists, hackers, cybercriminals, and some countries (Urquhart, 2018).

## Privacy Calculus

Privacy risk is described as "a situation where some undesirable event can happen" (Hansson, 2012). In the context of data protection, this risk is any harmful outcome that users face due to the loss of their personal data (Ching et al., 2016). Privacy calculus is a theory that has been developed to explain the kinds of risks users face from technology. This theory is defined as a rational analysis by an individual when they tradeoff between the perceived benefits and costs of disclosing personal data to a data

controller (Plangger & Montecchi, 2020). It is used to understand how users choose to disclose personal data (Ching et al., 2016). The theory states that users make a cost-benefit analysis when making decisions about using a given new technology. It describes how perceived risk influences an individual's tolerance towards possible risks when using new technology. This is the lens adopted by this study in an endeavor to understand privacy risks.

## METHODS

### Population and Sampling

The selection of participants focused on individuals who could access new technologies and services. This led to the selection of technical users who actively use new technologies and are active on the Internet. These users have high exposure to privacy risks when storing their information online. The perspectives of experts were also solicited and were included in the sample for this study. Experts in this study are individuals who possess special knowledge (Creswell & Creswell, 2018). It was important to obtain experts' views on problems that they currently face in privacy enforcement as well as suggestions for improving the data protection processes.

A sample of 101 participants consisting of general technical users responded to the survey. The participants were recruited using a purposive sampling approach which focused on the specific characteristics of the research sites or individuals selected (Bryman, 2016). It sought to purposefully choose those who would participate in a study in order to help the researchers understand the problem. Survey participants were recruited from two South African information technology professional bodies which have technical users within their membership. The survey link was sent to members through newsletters, email service, or online. The professionals included executives and technical workers within organizations. The organizations ranged from small to medium-sized. Other technical users were selected as well.

Snowball sampling was used to recruit seven interview participants for the study based on the recommendations received by survey participants. This process was repeated until sufficient data had been collected. Regulatory agencies in South Africa were approached to recruit participants to obtain expertise.

### Survey and Interview Design

An online survey was done to capture the views of users and professionals on trends affecting emerging technologies and privacy. The survey was descriptive and strove to highlight key issues before an interview phase could be conducted. The survey made it possible to access multiple participants across a wide area via the Internet. Engaging with the participants from the technological aspects also allowed the researchers to learn the key issues and terms used by professionals before engaging in the interview phase of data collection. Google Forms was used to host the survey online. This was affordable and a cost-effective option which allowed a wide distribution of the survey link to many possible participants.

Semi-structured interviews were used to collect data from regulators to understand how regulation of privacy takes place. The interview method was selected as it allowed the researchers to investigate the experiences of experts. The interview provided an in-depth understanding of the phenomena while the questionnaire survey provided a wider view of users' perspectives (Tracy, 2019; Maxwell, 2014).

### *Questionnaire and Interview Design*

The survey consisted of 15 researcher-constructed questions, while the interview had 9 original questions. They were grouped according to their similarity under 3 headings which were emerging technologies, privacy, and regulation. The questions were original, researcher-constructed questions, as there has been limited prior research on this topic. This led the researchers to pick key statements from the literature and develop them into questions which were used in this survey. This process involved reviewing the literature, which resulted in the following headings: emerging technologies, privacy, and regulation. These constructs were measured by investigating a number of distinct components, such as threats, violations, challenges, and improvements. For example, are emerging technologies making it easier to be hacked? These components contributed to the understanding of emerging technologies as a factor of this study (this process was carried out until the researchers felt there were sufficient data collection questions).

### *Piloting the Instruments*

To ensure the validity of the data collection instruments, a short pilot study was done to refine the questions contained in both the questionnaire and the interview guide. The survey link was sent to a small sample of individuals, while the interview guide was used to interview some experts who provided feedback that was used to refine the phrasing and overall structure of questions.

The study was approved by the North-West University's ethics board (approval number: NWU-00575-17-A9) and the ethical guidelines were followed throughout the research process.

## Data Collection Procedure

### *Survey Procedure*

A call for participation was sent via email to members of the organizations. This email introduced the researchers, the topic, and invited members to participate. The link to the survey was included for participants to access the survey. Participants chose to respond to the survey based on their willingness to participate and their availability to answer the questions. Research ethics were followed in this study; approval was obtained from the university research committee before the data gathering phase of the research.

To understand how emerging technologies affect users' personal data, an online survey was used. The survey sought to solicit the usage patterns of technical users regarding the emerging technologies. The first section of the survey collected demographic data of the participants, such as gender, age, qualification level, role in the organization, and level of experience. The second section of the survey consisted of questions measuring the factors mentioned earlier. These factors were used to separate the questionnaire into 3 sections with 5, 7 and 3 questions in each respectively. After data was collected, the data was analyzed, and descriptive statistics were generated using SPSS statistical software.

### *Interview Procedure*

The researchers contacted potential interview participants via email to introduce themselves and the research topic. When the experts showed an interest in participating, a date was agreed upon and whether the interview would be conducted in-person or through Skype. On average, the interviews took 33 minutes. The interviews were semi-structured, with participants given room to discuss the interview

topics freely. The interviewer also took notes of the conversations that were used in the interpretation of the findings at the analysis stage.

### *Triangulating the Data*

Triangulation was used in this study to improve the reliability of the data collected. This involved member checks, where participants who were interviewed checked the responses to ensure that they were correct. Another strategy used to triangulate the data involved going through the survey and interview data to check which themes were emerging from the collected data. This was helpful in the coding phase, as the codes were refined through constant comparison to ensure that common themes were being obtained from the data.

### *Data Analysis*

After the data was collected the coded responses were exported from the Google Forms to be analyzed in SPSS. The survey data was summarized using descriptive statistics in SPSS. The qualitative data that was collected was coded using the principles of qualitative analysis. NVivo was used to help create the codes to enable more in-depth data analysis.

The process of qualitative analysis involved examining the interview transcripts and memos from the interview phase. These memos helped in interpreting the findings by providing preliminary impressions of the interview data. The data were analyzed using coding and inductive thematic analysis. Categories were compared to each other in order to refine them. Both sets of data enhanced each other as they provided depth of contextual understanding and numerical evidence. The analysis phase was completed when no new themes emerged from the data.

## RESULTS

### Respondent Profile: Survey Respondents

Table 1 presents the demographic profile of the respondents for this survey. Most participants were male, with a smaller percentage of female participants. The largest age group was aged 25 to 34; this was also reflected in the user survey results. The next was the 35 to 44 group, with the 45+ age group being the smallest. Most participants have honors degrees followed by bachelor's degrees. The next largest group held a national certificate while the smallest group held either a masters or doctoral degree. Most participants held a technical role in their organizations with the next largest group belonging to management.

The banking sector was the most represented industry from the participants while the technology sector was the second most represented one. The government and education sectors were both third highest represented sectors. Most participants had less than 5 years of experience in their current position while the next largest group had at least 10 years or more in their current roles. The smallest group of participants had less than 10 years of experience in their current roles.

| Demographics | Count | Percentage |
|---|---|---|
| *Gender* | | |
| Male | 64 | 63 |
| Female | 37 | 37 |
| *Age* | | |
| 18–24years old | 5 | 5 |
| 25–34years old | 53 | 52 |
| 35–44years old | 32 | 32 |
| 45 years + | 11 | 11 |
| *Qualification* | | |
| National Certificate | 20 | 20 |
| Bachelor's Degree | 24 | 24 |
| Honors Degree | 33 | 33 |
| Master's Degree | 17 | 17 |
| Doctoral Degree | 7 | 7 |
| *Role* | | |
| Academic | 7 | 7 |
| Executive | 12 | 12 |
| Management | 18 | 18 |
| Technical | 64 | 63 |
| *Industry* | | |
| Banking and Financial Services | 26 | 25 |
| Construction | 4 | 4 |
| Consulting | 6 | 6 |
| Education | 14 | 14 |
| Government | 14 | 14 |
| Healthcare | 6 | 6 |
| Information Technology | 18 | 18 |
| Insurance | 5 | 5 |
| Other | 8 | 8 |

**Table 1. Survey demographic profile**

## Interview Respondents

In the first Section of the interview, the respondent's data on gender, age, experience, role and the sector within which the organization is in was gathered. Table 2 presents an overview which shows that most of the respondents were male with the largest age group being the plus 45 years. Most had less than 10 years of experience with the largest number being at the executive level. The legal and networking sectors were the most represented sectors.

| Demographics | Count | Percentage |
|---|---|---|
| *Gender* | | |
| Male | 6 | 86 |
| Female | 1 | 14 |
| *Age* | | |
| 35–44years old | 3 | 43 |
| 45 years + | 4 | 57 |
| *Experience* | | |
| Less than 5 years | 3 | 43 |
| Less than 10 years | 4 | 57 |
| *Role* | | |
| Executive | 3 | 44 |
| Management | 2 | 28 |
| Technical | 2 | 28 |
| *Industry* | | |
| Legal | 2 | 28 |
| Networking | 2 | 28 |
| Telecommunications | 3 | 44 |

**Table 2. Interview demographic profile**

## Emerging Technologies

### *Hackable*

The study shows that over half of the participants reported they believe that emerging technologies are easier to hack. Figure 1 shows that a combined 61% of the respondents found these devices and technologies to be very easy and somewhat easy to be hacked. IoT has been identified as having weaknesses that can be exploited, as some of these devices and technologies have weak security features by default (Harbi et al., 2019; Balaji et al., 2019). An additional 38% found them to have an average risk. Perceived risk of these devices and technologies is high when the results are combined. Reports on data breaches can influence public perception of data controllers and the privacy risks of data breaches (SophosLabs, 2019; Verizon, 2019; Hinchliffe, 2018; Lee & Rotoloni, 2016). This explains why respondents view these devices and technologies as hackable.

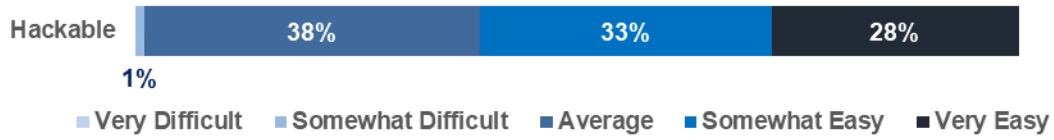


**Figure 1. Hackable**

The most significant part of these results is that risk perceptions do not dissuade users from using these devices, as is highlighted by previous results about their usage patterns. Privacy calculus theory states that users disregard the risks associated with a technology if its perceived benefits outweigh the risks. Perceived benefits motivate users when the risks of using new technologies are perceived to be lower than the benefit (Bhatia & Breaux, 2018). The use of the service is more valuable than its risks and this is a challenge to privacy. The users are a source of risk or threat to privacy due to their willingness to ignore obvious risks to personal data.

As one participant stated:

> *"Yes. As emerging technologies tend to be focused more towards machine learning and AI which needs baseline information, a lot of it private, which makes regulation tricky."*
> *(Participant Comment 33)*

The baseline of the devices requires personal data to operate, which is risky. How the data gets stored and processed should be regulated to lower such privacy risk to users' data.

### *Vulnerability of New Technologies*

The general perspective from the respondents was that emerging technologies can be used in negative ways. Five respondents (71%) expressed this view in relation to a few botnet examples employed in hacking IoT devices using malware installed on mobile devices. If someone has the intention to track and profile users, then they can use the different sensors that are embedded in a mobile device. From a technical standpoint, mobile devices automatically detect Wi-Fi signals and install Bluetooth devices. This represents the smart nature of the technology, as it can learn about the user's movements automatically. A typical example is the following response from one of the respondents:

> *"I mean my watch is busy trying to do that from time to time it says speak and I say I don't want to speak to you and I swipe it off."*
> *(Respondent Comment 6)*

This highlights the intrusiveness of some of these devices. Users can reconfigure their devices to disable these features; unfortunately, by default, devices are set to capture as much information as is necessary. New technologies are collecting user personal data constantly and processing it in terms of online behavior in order to profile users. There have been cases where smartphones auto-recorded users without their knowledge and permission. In addition, personalized advertisements are displayed and collect data about users as they browse websites (Lau et al., 2018). The "secret" recording of users by smart devices has caused legal issues in America where Amazon's Alexa Home Assistant has been found to store recordings of users and relay the information to Amazon (Lau et al., 2018).

At least two (29%) of the respondents took a more neutral stance, highlighting that they believed technology was neutral.

> *"The Internet makes committing crimes easier, it makes combating crime easier to some extent it also makes it adds complexity in terms of jurisdiction and where people are."*
> *(Respondent Comment 1)*

Furthermore:

> *"Emerging technologies yes they may enable it but only in the sense that they are new but they are neutral in terms of . . . they have a positive function but bad players can always take that and misuse it."*
> *(Respondent Comment 3)*

These respondents believe that it is not possible for a technology to be inherently bad. For the technology to have a good or bad effect on society depends on how users use it. Misuse leads to undesirable effects.

## Privacy

### *Threats*

Figure 2 highlights how the participants felt about the fact that data breaches are currently the highest risk to privacy. About 62% reported that breaches are a privacy risk and the literature does confirm this. A sharp rise in breaches has made users perceive their data as being important and changed their attitudes towards how it should be handled by data controllers (Corones & Davis, 2017). Hackers were the next highest privacy risk, at 34%. Hackers are responsible for several data breaches; therefore, it makes sense that they were identified as a threat to privacy. Hackers can also steal data directly from individual users if they are motivated to do so.

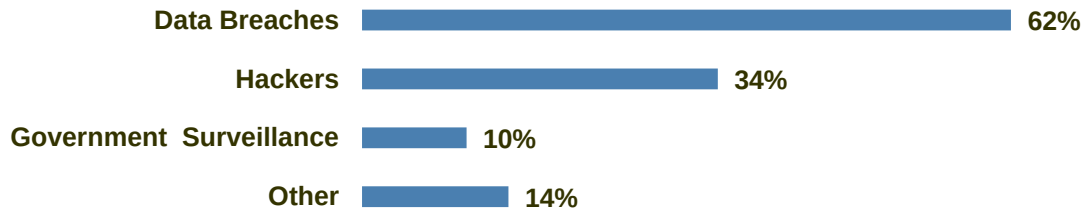


**Figure 2. Threats**

Some participants view surveillance as a privacy risk (10%). For example, a government that conducts surveillance on citizens is considered as a threat to users' privacy (Klitou, 2014). The governments do so to achieve national security and to preserve order (Fuller, 2019). This however exposes the activities of citizens to the government (Stalla-Bourdillon et al., 2014). The movements of citizens are monitored, including financial transactions and phone messages (Fuller, 2019). In the US, law enforcement has been given special powers to demand citizens to switch on their phones (Donohue, 2019; Khilji, 2019). This can be done without a warrant if an officer is suspicious of an individual.

The results show that 14% of the participants stated other privacy threats in their responses such as:

> *"The weakest link in my experience is always the human factor. You can train people etc, but as long as their risk perception remains low, their attitudes towards adopting and sticking to secure habits and practices suffers."*
> *(Participant Comment 16)*

The human factor was identified by one participant as affecting risk perception. While participants in the previous section understand that the devices are hackable, this does not influence the security awareness of users. Users hold the view that they are unlikely to be targets of potential hacking, hence, they are safe. This attitude towards security is a threat, as individual attitudes can compromise a security strategy.

### *Threats: Mobile*

All the respondents stated that mobile devices are a threat to user privacy in one way or another. This finding is supported by a number of researchers who highlighted the dangers of personal data stored on mobile devices (Crossler & Bélanger, 2017; Au & Choo, 2016; Kadir et al., 2016; Marques et al., 2016). Mobile devices are the main gadgets through which users browse the Internet, especially in the developing world (ITU, 2017). They are relatively inexpensive compared to desktop or laptop computers and have embedded Internet-access capabilities. The ITU estimates that about 56% of the population in South Africa has Internet access (ITU, 2017). It is also estimated that approximately 29 million of these users are active mobile Internet users. These users with Internet access may not have the same level of education and awareness of the privacy risks posed by these devices (Tamò-Larrieux, 2018).

Younger users own Internet-enabled mobile devices in South Africa as compared to other countries on the continent (Lannoy, 2018). It has been shown in previous studies that these groups of users tend to self-disclose at a higher rate than users who have been on the network for a longer period. One respondent made the following observation:

> *"Our cyber-security awareness is so low we have so many new people coming onto the Internet all the time who don't have any experience who've got a new machine which doesn't have anti-virus or anything. It's quite easy to compromise those machines and to create that botnet and a lot of that is in South Africa."*
> *(Respondent Comment 3)*

The respondent expanded on this comment by highlighting that in the early days of the Internet, machines would be managed by Internet-cafe owners who would be responsible for the security of the devices. This is in direct contrast with the devices' security being the responsibility of a given user.

One of the challenges of using mobile devices is that they can be infected by malware (Au & Choo, 2016). The installation and management of applications on smartphones can be a challenge for users who are not knowledgeable, which may lead to their security being compromised (Au & Choo, 2016). The respondents observed that attackers make use of different strategies to access users' data. One such strategy is to lure users into downloading and installing an application that has a simple function, such as editing photographs. The user then gets a notification that the application needs to be updated and that the update should be approved. The update can include a request for more permissions which the application does not need. This ordinarily would raise a red flag or concern from a more knowledgeable user, but novice users simply agree and accept the offered option so that they can continue to use the application.

A study was done to explore different users' comfort levels with mobile applications that request permissions that run in the background. The participants believed that for them to be comfortable, they

need to understand when and why a mobile resource is requested (Votipka et al. 2018). They do not view background resources to be of equal importance as other applications' requests (Votipka et al. 2018). These findings highlight the importance of user education and that users must be informed as they install new applications.

There are internal checks within application stores for the most popular smartphone operating systems, such as Android and Apple (Cruz et al., 2019). In the case of Android-based phones, hosted by the Google Play Store, applications are tested via Play Protect to see if they have any potentially dangerous code. A respondent observed that attackers, however, use other ways to bypass the testing strategies. One way is to link their malicious code to operate with the mobile device's gyroscope sensor when it is active. This represents the challenge of detecting malicious applications and that users should not just trust an application simply because it is hosted and downloaded from an official source (Cruz et al., 2019).

One respondent observed that in certain cases, malwares are pre-installed on the devices. The spyware is known as Pegasus spyware, which has been developed by NSO, an Israeli company, to be sold to governments only (Marczak et al., 2018). It is used by governments to spy on journalists and human rights activists (Marczak et al., 2018). According to a 2018 report, this spyware was found to have infected numerous phones in South Africa (Marczak et al., 2018). This is the reason why the respondents argue that mobile technology violates one's privacy.

### *IoT Threats*

Two respondents (29%) reported that other devices, such as IoT devices, can be a threat to privacy. Every manufacturer is creating unique products, which makes compatibility difficult, thereby affecting the design of secure IoT. Devices such as pacemakers were identified as an example of a threat:

> *"Your off-the-shelf pacemaker today has an IP stack in it and the hospital updates what your pacemaker is doing by making it update so the potential for someone to hack my pacemaker and get it to do something dodgy is not insignificant."*
> *(Respondent Comment 1)*

Medical personal data has strict regulations governing how organizations should store it. These regulations need to reflect the changing technologies that can store patients' information which can be hacked (Eggers et al., 2018). Another technology mentioned by a respondent was self-driving cars which have been shown to be hackable. This may lead to undesirable outcomes such as accidents being caused by a car that has been hacked. The issue of voice-activated assistants came up in one of the interviews. The interview respondent mentioned that:

> *"Yes, I've disabled Siri. I have disabled her but it's because it picks up certain phrases whenever you have done your Google search because Siri is competing with Google."*
> *(Respondent Comment 6)*

The threat of a live microphone which activates itself and records users' conversations is understood to be a privacy risk by one of the respondents. They went on to say the technology reflects the smart nature of mobile devices which are constantly learning about their users by monitoring them (Lau et al., 2018).

### *User Created Risks*

The respondents noted that users are a source of privacy risks. Users are willing to disclose personal data which makes them more vulnerable to attacks. Personal data that is stored on smart devices has the

potential to be stolen by hackers (Moore, 2017). Users may also have the personal data of their family members, friends, or work colleagues stored on devices which may have a severe impact in the event of a breach. The devices have minimum privacy settings which can be a threat to users' privacy (Kshetri, 2016). Data is not encrypted by default which makes these devices more vulnerable.

A study was done to understand the different behaviors of users regarding the use of smartphones. The users showed moderately secure behavior when using smartphones (Nowrin & Bawden, 2018). Their behavior varies depending on gender. More awareness training may help to improve secure behavior (Nowrin & Bawden, 2018). Another study was done to investigate the security behavior of smartphone users in China. It was found that users have poor awareness of potential malware when installing or updating mobile applications (Zhang et al., 2017). The different groups of users had different levels of knowledge based on their age and income levels (Zhang et al., 2017).

Another risk that users face is when they give permissions to applications on their mobile devices. Users are not always aware of how their data is used when personal data is shared on new technologies (Au & Choo, 2016). In the past, data controllers have been found guilty of data misuse also, which also affects even the large companies (Taddeo & Floridi, 2017). An interview respondent mentioned that while large data controllers have improved how they inform users, it must be noted that in the past, they would hide that information in the End User Agreement.

Malicious applications were discussed at the beginning of this section; however, the user aspect of risk results when users unknowingly agree to use a technology without being informed of the risks. Applications that are designed for one player, such as games or camera applications, should not request permissions from a users' contact list, messages, or pictures on devices. One respondent commented that:

> *"You have no idea who wrote that up, no idea if you've given it permission to share your contacts and your pictures and you don't know what or who that application is sending your personal data."*
>
> *(Respondent Comment 1)*

The permissions given to these applications mean that they can read the users' sensitive data and share it with the developers of the applications who then sell it to third parties (Garcia-Rivadulla, 2016). Data stored in text format can be read on the device, including passwords to online banking applications. The respondent emphasized that when users install applications without reviewing permissions requests, it can lead to undesirable outcomes.

When asked why, the respondent made an interesting explanation:

> *"Let's face it 90% of all users are far too lazy to fiddle with the settings on any program they use."*
> *(*Respondent *Comment 1)*

Inaction by users can be a threat to privacy, as some users do not want to learn how to improve their own privacy. It may not be a good strategy to place the responsibility for data protection on the users, as they are more interested in using a technology than in learning how to protect their privacy as they use it.

### *Social Engineering*

Four respondents (57%) mentioned that social engineering was a threat to privacy. This is when attackers attempt to get an individual's personal data to build a profile. Attempts at phishing trick users into giving out their personal data by pretending to be authentic websites (APWG, 2019). The users unknowingly share their data only to be attacked by the hackers. One of the respondents shared an experience they had with a phishing attempt:

> *"Somebody called me yesterday and said to me we've got R9,000 of yours we'd like to transfer it to your account and I said which greenback account then they said Nedbank . . . the first thing that came to my mind was that this person didn't even tell me what their name is or where they were calling me from but now he already knows my information . . . he said give me the expiry date and the number of your card."*
> *(R*espondent *Comment 2)*

The experience ended with the respondent telling the caller to call back after five minutes. When the cybercriminal did not call back, the respondent redialed the number that was used but it was disconnected. Scams can succeed as attackers have a profile of a user and simply need one or two pieces of sensitive information to complete the profile. The more information a user discloses, the more vulnerable they become to attacks (Garcia-Rivadulla, 2016). In an organizational context which has access to someone who provides information, this can help an attacker to collect enough details to launch an eventual attack.

## DISCUSSION

This Section discusses the findings in the context of literature and theory. This Section is organized according to research questions based on the aims presented in the introduction. The most relevant results have been selected to answer each of the research questions. This has been done to determine if the collected data adequately answers these questions. Under each heading, a summary of the findings is embedded within a discussion of the wider context of the results.

*RQ1. To what extent are emerging technologies vulnerable to privacy and security attacks/breaches?*

More than half of the respondents indicated that emerging technologies are vulnerable to potential attacks. This may be due to press reports of data breaches and the growing calls for more privacy (Hinchliffe, 2018; Lee & Rotoloni, 2016). A previous study was done to determine how security and behavioral tendencies of users impact the views of companies in light of past security breaches. The presence or absence of breaches influences users' views (Curtis et al., 2018). It has a lesser effect on the intentions of users to be more secure (Curtis et al., 2018).

This does not influence their willingness to use these technologies. Research indicates that convenience is the main reason why users adopt new technology over any perceptions they have on privacy (Gashami et al., 2016). These finding explain why users continue to use emerging technologies despite their reservations concerning privacy (Gashami et al., 2016). They use technologies to store their data in the cloud in either email form or through uploading files. They also use banking applications on their mobile devices as they offer convenience which appeals to smartphone users.

There is theoretical support why users continue to use these devices. Privacy calculus states that users are likely to decide whether to use a new technology based on rational processes of cost-benefit analysis (Ching et al., 2016). This is because if users see that the perceived value outweighs the risks, they ignore the privacy challenges of a given technology (Moller, 2012). When a new technology is viewed as

valuable, its adoption increases exponentially (Plangger & Montecchi, 2020). Some users may believe that they can control the risks better than others and this gives them confidence as they use the technology. The use of the service is more valuable to the user than the potential danger it poses to privacy.

A study on user privacy concerns found that 40% of South African users were worried about privacy (Hootsuite, 2019). This shows that a significant number of users are concerned about the misuse of data. The findings in this study found that most participants believed that emerging technologies have made hacking simpler. This supports the view of users who consider technology as having privacy risks. A potential influence on user risk perceptions are the numerous reports of data breaches (IBM Security, 2019).

IoT was singled out as having internal weaknesses that can be exploited, as these devices lack basic security features. The probability of a data breach increases if the device has no internal security features or they are not configured for security. This is because as personal data is stored and shared on these devices, it can be affected potentially by a data breach. These new technologies are equipped with sensors that are Internet-based and attackers can access these devices and use them to create botnets that can be used to launch other attacks. The participants shared instances of botnets created as a result of hacking IoT hardware and malware deployed on mobile devices which depict the vulnerability of these devices (Fruhlinger, 2018). Users can decide to turn off some features if they wish; unfortunately, the devices are configured to gather as much data as possible by default. New technologies can access and process users' private data to profile them.

*RQ2. What threatens privacy and security in emerging technologies today?*

Regulators identified mobile devices as the major threat to user privacy. Malicious applications threaten privacy as well as users' lack of cybersecurity literacy (Tamò-Larrieux, 2018; Neisse et al., 2016). Infected applications or malware that are installed on mobile devices pose a risk. Installing and managing smartphone applications can be a challenge for users who do not have cyber expertise (Neisse et al., 2016). One approach used to obtain information from users is to entice users to download and install an application then update it. When they give permissions to applications on their mobile devices, they are not always aware of how their data is used (Neisse et al., 2016). The problem with this is that users are not always well informed on the risks involved in this process. A study was done to explore users' views on updating mobile applications. This study revealed that users who do not update their applications are likely to have had negative experiences with the updating process (Mathur & Chetty, 2017). This has a negative impact on application security, leaving them more vulnerable to attacks if the applications are not patched or updated appropriately (Mathur & Chetty, 2017).

Some websites use online trackers to advertise to users as they browse the web (Razaghpanah et al., 2018). When an application is launched, data is sent to third party trackers. This data can be in the form of what device is being used or which sites are visited (Razaghpanah et al., 2018). These tracers violate users' privacy, as they share user data with third parties without the consent and knowledge of users.

Regulators noted that users are responsible for the privacy attacks they experience. Users are willing to disclose personal data which makes them more vulnerable to attacks (Choi et al., 2019). Data controllers have in the past been found guilty of data misuse, showing that this issue affects even the large companies (Taddeo & Floridi, 2017).

As mobile device usage increases so does the exposure to attacks (Au & Choo, 2016). A higher adoption of the technology can create more chances for attackers to hack the devices. This raises the risk to

personal data being misused by the data controllers. Certain factors affect perceived risk, such as uncertainty over the new technology, regulatory uncertainty, and the unavailability of information (Yang et al., 2015). Potential risks can be found in new mobile applications which have been shown to contain malware (Neisse et al., 2016). Users can connect to unsecured Wi-Fi which can be used as an attack vector. New users are also a threat as they can be tricked into installing malware that they should not install (Au & Choo, 2016).

Different privacy threats are growing as new technologies are being released into society (Leenes, 2019). Devices such as the IoT have created a new way for large botnets to be created (Urquhart, 2018). These new technologies are equipped with sensors and are connected to the Internet (Peppet, 2014). Some of these devices lack basic security features and are not configured for security. Attackers can get access to these devices and use them to create botnets, such as the Mirai virus that can be used in other attacks (Fruhlinger, 2018). In 2019, a variant of the Mirai virus was found to be selecting new architectures to attack such as new IoT devices (Gatlan, 2019). This shows that the malware threat on new devices is still growing and needs to be solved. Unsecured IoT devices can be a threat to privacy as every manufacturer is making different IoT products (Harbi et al., 2019). There is no universal agreement on low-level protocols or frameworks to guide the development of IoT devices and this is a challenge data protection. As mentioned before, Mirai virus variants can be used to attack these devices (Gatlan, 2019). This shows how a lack of standards threatens privacy.

## Conceptual Framework

Privacy research is by nature multidisciplinary as it covers both legal and technological dimensions. These dimensions provided the concepts presented in the conceptual framework illustrated in Figure 1. Through a process of inductively theorizing from the literature and the collected data, we arrived at the integrated framework. The theory-development approach used in this study was to review relevant literature on regulation and emerging technologies, integrate the key concepts identified with insights provided by the collected data to build a theory or pattern of meaning (Tracy, 2019). This was an iterative process of moving from identifying relevant categories, refining them, and assessing their value until the final theory was developed (Corbin & Strauss, 2014). Figure 3 outlines the conceptual framework and introduces six new propositions that emerged from the collected data.

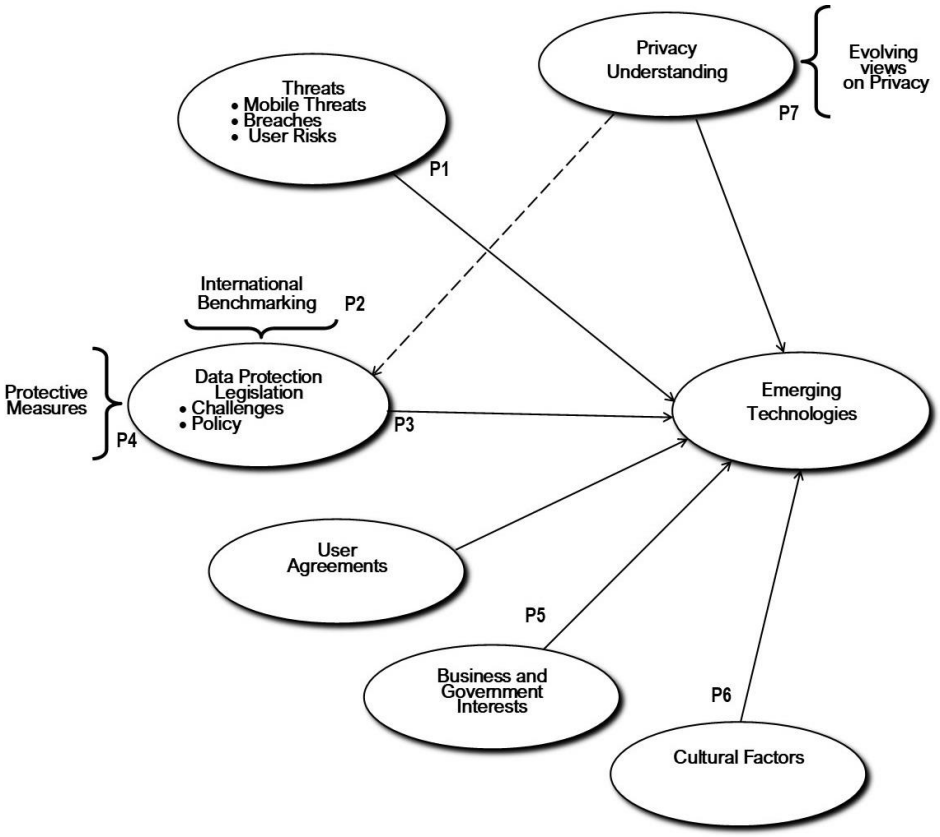


**Figure 3. An integrative framework for regulating privacy in emerging technologies**

The framework shows that it is important to have a current understanding of cyber-security and privacy when dealing with new technologies. A lack of understanding how privacy affects data protection can lead to ineffectual privacy laws. Companies and governments that do not value privacy will fail to protect user data or misuse it for their own gain. This is how privacy can be observed by policymakers as they investigate violations. These two concepts are interlinked, as has been shown by this study. A lack of security often leads to privacy violations (Conger & Landry, 2008).

The propositions were formulated in interaction with the literature and the results (data) collected in this study. These propositions are part of the theory-building process, as they are part of explaining what is occurring (Maxwell, 2014). They serve as tentative answers to the research questions. Based on the findings, some of the propositions were found to be supported. New propositions also emerged from the data which we present in the next Section.

## Privacy Threats

As new devices become more embedded within our daily lives, they generate and store personal data about us (Conger et al., 2013; Solove, 2011). Devices, such as smartphones, send out personal data on users to many other companies that are unknown to the users (Bunnik et al., 2016). The devices give data trackers enough information to profile users and this is a privacy risk. Cyber-attacks have taken place where hackers have stolen users' personal data. Governments who use surveillance systems that spy on citizens' online activity can access personal data (Sarat, 2015).

When companies use predictive analytics, it affects user privacy as their private data is collected or shared with online advertisers (Bunnik et al., 2016). A data breach which leads to hackers possessing users' personal data can lead to cyber-crimes being committed against them, such as identity theft or ransoms (Federal Trade Commission, 2018; Lee & Rotoloni, 2016). These findings lead to the following proposition:

Proposition 1: There are multiple threats facing emerging technologies which are in the form of mobile devices, data breaches, and user created risks.

## International Benchmarking

Best practices should be incorporated alongside local approaches and benchmarked against international standards (Subrahmanian et al., 2015). This can help users to appreciate that privacy standards are being maintained. Certain technologies, such as the IoT, have the potential to be misused and this requires a pro-privacy approach to regulating them. Ruggiu (2018) implores governments to be more specific and less permissive. This is due to overlapping roles human rights and ethical standards are experiencing (Reins, 2019). The more impact new technologies have the more regulators should actively monitor their usage (Reins, 2019).

The following proposition is observed:

Proposition 2: Benchmarking against international privacy approaches can help the development of local data protection laws.

## Data Protection Legislation

Governments must provide some form of oversight on corporate activities (Sethi & Sethi, 2016). The government, through public law regulatory infrastructure, must also oversee the implementation of prevailing legal theories on how privacy is enforced within their jurisdiction. Companies view privacy regulation as preventing them from maximizing profits (Cohen, 2012). To deal with this, the government often consults with other stakeholders in the industry, such as advocacy groups, to provide insights. These can be used to address any shortcomings in legislation. This cooperation seeks to provide higher levels of privacy protection for users and to manage the risks and liability involved in such. It is also necessary, as policymakers are often not technically aware of the specifics of new technologies and how they affect society at large (Ludlow et al., 2015). This is a common challenge which is known as the "pacing problem" (Ludlow et al., 2015).

Governments must develop regulatory approaches that are fair and promote a multi-stakeholder approach (Sethi & Sethi, 2016). The governments may seek to motivate the industry to adopt self-regulation (Tropina & Callanan, 2015; Hirsch, 2013). This allows industries and governments to come together in implementing voluntary codes of conduct through partnerships (DTPS, 2017).

A new revised proposition has been formulated based on the findings:

Proposition 3: Effective legislation along with other strategies can improve users' data privacy and security as they use emerging technologies.

## Protective Measures

Users should take a proactive approach towards privacy by learning how to protect their data (Beigi et al., 2019). Users should not use the default settings offered by emerging technologies or online services. They must take advantage of maximum privacy settings; otherwise, their data remains vulnerable.

Privacy-enhancing technologies are useful in this regard. They range from browsing the Internet in a browser that masks a user's IP address or using cryptocurrencies, such as Bitcoin, to pay for online transactions (Tamò-Larrieux, 2018). It must be noted that open-source developments are not guided by a central authority. There has been some controversy over the anonymity they create and how they empower individuals to commit crimes without being traceable (Tamò-Larrieux, 2018).

The following proposition about protective measures is observed:

Proposition 4: Protective measures may accompany legislation for them to manage new threats effectively.

## Business and Government Interests

Views on privacy continue to be affected by national interests regarding security and business interests on profit, while users require trusted computing (Cavoukian, 2012). The increase in awareness of data breaches causes users to advocate for privacy protection. Online services that cannot assure data protection may force users to consider whether it is worthwhile to continue using those services (Lee & Rotoloni, 2016). The following proposition about the interests that affect privacy is observed:

Proposition 5: The different interests of groups, such as companies and governments, will continue to influence how emerging technologies are used in society.

## Cultural Factors

Privacy is affected by cultural aspects as well (Tropina & Callanan, 2015). The ways society's views about privacy evolve is affected by the new technology and its capabilities (Peppet, 2014). Privacy is seen through the prism of cultural context, which is shown in the framework. The different approaches to privacy reflect cultural differences across the world, which must be observed by international data controllers.

Privacy must be viewed as contextual, depending on factors that influence it in each region (Ahituv et al., 2014). According to Edmundson (2008), "Cultural and temporal variation is seen as a feature of the norm of informational privacy." Privacy may be less respected and upheld in various cultures, which is a concern (Wilk, 2018). This leads to privacy regulation being subject to "wide variation across jurisdictions as well as subject to enlargement, qualification, and repeal by ordinary legislation" (Edmundson, 2008).

Due to cultural complexity, different approaches to privacy exist (Wilk, 2018). In relation to privacy, self-regulation would entail businesses taking responsibility for the safety of users' personal data which they store on their servers or cloud storage architecture (Sethi & Sethi, 2016). This requires the companies to operate in the public interest as they self-regulate, which is one of the ideals which this study suggests. These factors led to the proposition that:

Proposition 6: Culture influences how society's ability to combat new threats that emerge from emerging technologies.

## Evolving Views on Privacy

As the general understanding of privacy continues to evolve due to innovations and new legislation, an opportunity exists for new theories to transform how society views privacy. This is represented in the integrated framework by adding an element that allows for new ideas to inform a theory-based approach to privacy, thus allowing for a form of feedback to exist.

Previous studies on innovation have highlighted the need to acknowledge the potential impact new technologies have on users, corporations, and governments (Leenes, 2019). There is a need for the responsible usage of these technologies (Leenes, 2019). This is called the engagement approach to innovation and has the aim of ensuring that all stakeholders remain informed (Konrad et al., 2013). An instrument that would guide them as they deploy their products or services may be able to assist them to adhere to legal requirements (Konrad et al., 2013).

After examining the findings, this study proposes that:

Proposition 7: Privacy is not a static concept and continues to evolve as new technologies are developed.

### Implications

Consistent and reliable protective measures are needed; more policies should be introduced to protect user privacy. A scheme of various interventions is more efficient in coping with long-term privacy breaches (Mandel, 2013). This scheme should limit data controllers' actions. If a data controller breaks the constraints, the policy scheme should alert the public.

User Education; digital literacy must emphasize security skills to equip users when using new technologies. The use of tools, such as private tabs when browsing, VPNs, ad blockers and anti-trackers, must be included in digital courses. Educational programs can help as well and the government should make information widely available. Presenting successful case studies of data controllers implementing local data protection standards can help improve confidence in them. The formation of user groups who advocate for secure online practices can also help to achieve this digital literacy. Peer education can have a positive impact in spreading awareness among users who do not have access to formal learning channels.

Changing technological landscape; previous approaches may not be enough due to new technologies and the increasing number of data breaches. Some participants stated that security is an ongoing process which needs to be managed properly. Effective awareness and training programs can also help (DTPS, 2017). It is important that security programs are developed and maintained by data controllers, as they are responsible for how users' data is held and processed.

## LIMITATIONS AND FUTURE RESEARCH

This study does not examine in depth the technical solutions that are available for privacy protection. Some of these solutions include encryption with hash algorithms or fragmentation of data. Instead, the study mentions them as solutions used by developers of the technologies. This study is aimed at helping the policy formulation for data protection laws.

In this study, the response rate for the survey was not as high as it could have been. Certain organizations which could have distributed the survey did not find the survey to be linked with their goals or interests. The response rate affected the ability to produce more sophisticated statistical tests. This led to triangulating the results by cross-checking them with interview data.

The challenge identified in this study merits further investigation, as new threats to privacy exist. As the scope of the study was focused on a few emerging technologies, further research is required on more technologies not investigated in this study. Technologies such as 5G wireless networks, block chain, and smart cities present an opportunity for future research. Personal data is valuable and data breaches must be prevented as new technologies process this information. It is necessary to protect privacy on

technologies with more capabilities to keep policymakers informed as they make decisions on what to regulate.

### What This Study Is Not

This research is framed for the policy design and formulation to regulate emerging technologies. It seeks to bring a technological perspective to policymaking, and it does not seek to provide a detailed comparative analysis of current regulations and frameworks in South Africa. Previous studies by Ntsaluba (2018) and London (2013) have covered that ground. Instead, it seeks to provide guidelines for regulators as they conceptualize privacy regulation and improve current data protection standards.

## CONCLUSION

Privacy threats affect new technologies and there is a need to be aware of this possibility. New technologies, such as the IoT, need to be monitored from a regulatory perspective to enforce security principles when they are being developed. An anticipatory approach to regulating new technologies is necessary to mitigate threats. This research highlighted that privacy risks can harm users and they have to be addressed. This study argues that new technologies fall under the types of threat categories that should be regulated to ensure that the country or continent can enhance its data protection laws. Regulating these technologies can help to mitigate the risks associated with using the technologies.

## ACKNOWLEDGEMENTS

We thank North-West University for its financial and institutional support in carrying out this research. We also thank the organizations which distributed the survey links during data collection and participated in the survey. We also appreciate all the participants.

## REFERENCES

Ahituv, N., Bach, N., Birnhack, M., Soffer, T., & Luoto, L. (2014). New challenges to privacy due to emerging technologies and different privacy perceptions of younger generations: The EU PRACTIS Project. *Proceedings of the 2014 InSITE Conference* (pp. 1–23). https://doi.org/10.28945/1995

APWG. (2019). Phishing activity trends report. APWG. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q1_(2019)pdf

Au, M.-H., & Choo, R. (2016). *Mobile security and privacy: Advances, challenges and future research directions*. Syngress.

Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with layered approach to Internet of Things security. *Measurement and Control*. https://doi.org/10.1177/0020294019837991

Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT Technology, applications and challenges: A contemporary survey. *Wireless Personal Communications*, *5*(7), 3758.

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation*: *Theory, strategy, and practice* (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001

Beigi, G., Guo, R., Nou, A., Zhang, Y., & Liu, H. (2019). Protecting user urivacy. In J. S. Culpepper, A. Moffat, P. N. Bennett, & K. Lerman (Eds.), *Proceedings of the twelfth ACM international conference on web search and data mining* (pp.213–221). https://doi.org/10.1145/3289600.3291026

Belmas, G. I., Shepard, J. M., & Overbeck, W. (2017). *Major principles of media law*. Cengage Learning.

Bhatia, J., & Breaux, T. D. (2018). Empirical measurement of perceived privacy risk. *ACM Transactions on Computer-Human Interaction*, *25*(6), 1–47. https://doi.org/10.1145/3267808

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 1-25. https://doi.org/10.1177/0093650218800915

Bowman, D., Stokes, E., & Rip, A., eds. (2017). *Embedding new technologies into society: A regulatory, ethical and societal perspective.* Pan Stanford Publishing. https://doi.org/10.1201/9781315379593

Brodkin, J. (2019). *FTC investigates whether ISPs sell your browsing history and location data*. ArsTechnica. Retrieved from https://arstechnica.com/tech-policy/2019/03/ftc-investigates-whether-isps-sell-your-browsing-history-and-location-data

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Bunnik, A., Cawley, A., Mulqueen, M., & Zwitter, A. (2016). *Big data challenges: Society, security, innovation and ethics.* Palgrave Macmillan. https://doi.org/10.1057/978-1-349-94885-7

Butenko, A., & Larouche, P. (2015). Regulation for innovativeness or regulation of innovation*? Law, Innovation and Technology*, *7*(1), 52–82. https://doi.org/10.1080/17579961.2015.1052643

Cavoukian, A. (2012). Operationalizing privacy by design: A guide to implementing strong privacy practices. Information and Privacy Commissioner of Ontario Information and Privacy Commissioner of Ontario. Retrieved from https://pdfs.semanticscholar.org/5fa7/dc89181d199fea322c550a631191c4c1c09f.pdf

Ching-Yi Lin, Jen-Yin Yeh, & Yi-Ting Yu. (2016). The influence of privacy calculus, user interface quality and perceived value on mobile shopping. *Journal of Economics, Business and Management*, *4*(10), 567-573. https://doi.org/10.18178/joebm.2016.4.10.453

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, *173*, 113–124. https://doi.org/10.1016/j.jpubeco.2019.02.001

Cohen, J. E. (2012). What privacy is for. *Journal of Harvard Law Review*, *126*, 1904.

Conger, S., & Landry, B. J. L. (2008). The intersection of privacy and security. *All Sprouts Content*, 243.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x

Corbin, J. M., & Strauss, A. L. (2014). *Basics of qualitative research. Techniques and procedures for developing grounded theory* (4th ed.). SAGE.

Corones, S., & Davis, J. (2017). Protecting consumer privacy and data security: Regulatory challenges and potential future directions. *Federal Law Review*, *45*(1), 65–95. https://doi.org/10.1177/0067205X1704500104

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Crossler, R. E., & Bélanger, F. (Eds.). (2017). The mobile privacy-security knowledge gap model: Understanding behaviours. *Proceedings of the Hawaii international conference on system sciences*. https://doi.org/10.24251/HICSS.2017.491

Cruz, L., Abreu, R., & Lo, D. (2019). To the attention of mobile software developers: Guess what, test your app! *Empirical Software Engineering*, *125*(6), 1–31.

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviours and trust following a data breach *Managerial Auditing Journal*, *33*(4), 425–435. https://doi.org/10.1108/MAJ-11-2017-1692

Department of Justice. (2013). Protection of Personal Information Act 4 of 2013. Department of Justice, Pretoria.

Department of Justice. (2017). Cybersecurity and Cybercrimes Bill of 2017. Department of Justice, Pretoria.

Department of Telecommunications and Postal Services. (2017). Cyber Readiness Report. Department of Telecommunications and Postal Services, Pretoria.

Dewri, R., & Thurimella, R. (2015). *Privacy in mobile devices: Privacy in a digital, networked world.* Springer. https://doi.org/10.1007/978-3-319-08470-1_10

DLA Piper. (2019). *Global data protection laws of the world*. World Map DLA Piper. Retrieved from https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all

Donohue, L. K. (2018). Customs, immigration, and rights: Constitutional limits on electronic border searches. Yale LJF, *128*, 961.

Edmundson, W. A. (2008). Privacy. In M. P. Golding & W. A. Edmundson (Eds.), *The Blackwell Guide to the Philosophy of Law and Legal Theory*. John Wiley and Sons. https://doi.org/10.1002/9780470690116.ch19

Eggers, W. D., Turley, M., & Kishnani, P. (2018). *The future of regulation: Principles of regulating emerging technologies*. Deloitte Insights. Retrieved from https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation.html

Federal Trade Commission. (2018). Privacy and data security. Retrieved from https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf

Fruhlinger, J. (2018). *The Mirai botnet explained: How IoT devices almost brought down the Internet*. CSO Online. Retrieved from https://www.csoonline.com/article/3258748/the-mirai-botnet-explainedhow-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Fuller, C. S. (2019). Is the market for digital privacy a failure? *Public Choice*, *180*(3), 353–381. https://doi.org/10.1007/s11127-019-00642-2

Garcia-Rivadulla, S. (2016). Personalization vs. privacy. *IFLA Journal*, *42*(3), 227–238. https://doi.org/10.1177/0340035216662890

Gashami, J. P. G., Chang, Y., Rho, J. J., & Park, M.-C. (2016). Privacy concerns and benefits in SaaS adoption by individual users. *Information Development*, *32*(4), 837–852. https://doi.org/10.1177/0266666915571428

Gatlan, S. (2019, April 9). Mirai botnet variants targeting new processors and architectures. Bleeping Computer. Retrieved from https://www.bleepingcomputer.com/news/security/mirai-botnet-variantstargeting-new-processors-and-architectures

Gcaza, N., & Solms, R. von. (2017). A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Hansson, S. O. (2012). A panorama of the philosophy of risk. In *Handbook of risk theory: Epistemology, decision theory, ethics, and social implications of risk* (pp. 27–54). Springer. https://doi.org/10.1007/978-94-007-1433-5_2

Harbi, Y., Aliouat, Z., Harous, S., Bentaleb, A., & Refoufi, A. (2019). A review of security in Internet of Things. *Wireless Personal Communications*, *29*(7), 1–20. https://doi.org/10.1007/s11277-019-06405-y

Herkert, J. R. (2011). Ethical challenges in emerging technologies. In G. E. Marchant, B. R. Allenby, & J. R. Herkert (Eds.), *Growing gap between emerging technologies and legal-ethical oversight: The pacing problem*. *International Library of Ethics, Law and Technology*, *7*, 35-47. https://doi.org/10.1007/978-94-007-1356-7_3

Hijmans, H. (2016). *European Union as guardian of Internet privacy*. Springer. https://doi.org/10.1007/978-3-319-34090-6

Hinchliffe, T. (2018, November 15). A look into big tech user data requests from governments worldwide. The Sociable. Retrieved from https://sociable.co/business/big-tech-user-data-requests-governments

Hirsch, D. D. (2013). In search of the Holy Grail: Achieving global privacy rules through sector-based codes of conduct. *Ohio State Law Journal*, *74*(6), 1029–1070.

Hootsuite. (2019). *The global state of digital in 2019*. Hootsuite Media Inc. Retrieved from https://hootsuite.com/resources/digital-in-2019

IBM Security. (2019). 2019 cost of a data breach report. IBM Security. Retrieved from https://www.allaboutsecurity.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

International Telecommunications Union. (2017). ICT facts and figures 2017. International Telecommunications Union. Retrieved from https://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures(2017)pdf

Inukollu, V. N., Arsi, S., & Ravuri, S. R. (2014). Security issues associated with big data in cloud computing. *International Journal of Network Security and Its Applications*, *6*(3), 45. https://doi.org/10.5121/ijnsa.2014.6304

ITNewsAfrica. (2017, October 26). South Africa ranks as third most exposed country to cyber risks. ITNewsAfrica. Retrieved from https://www.itnewsafrica.com/2017/10/south-africa-ranks-as-third-mostexposed-country-to-cyber-risks

Johnson, G. (2019). Privacy and the Internet of Things: Why changing expectations demand heightened standards. *Washington University Jurisprudence Review*, *11*(2), 345–374.

Kadir, A. F. A., Stakhanova, N., & Ghorbani, A. A. (2016). An empirical analysis of Android banking malware. In W. Meng, X. Luo, S. Furnell, & J. Zhou, *Protecting mobile networks and devices: Challenges and solutions* (pp. 209–234). Taylor & Francis Group.

Khilji, A. (2019). Warrantless searches of electronic devices at US borders: Securing the nation or violating digital liberty? *Catholic University Journal of Law and Technology*, *27*(2), 173–206.

Klitou, D. (2014) *Privacy-invading technologies and privacy by design: Safeguarding privacy, liberty and security in the 21st Century*. Asser Press.

Konrad, K., van Lente, H., Coenen, C., Dijkstra, A., & Milburn, C. (2014). *Shaping emerging technologies: Governance, innovation, discourse*. IOS Press. https://doi.org/10.1007/978-94-6265-026-8_2

Kshetri, N. (2016). *The quest to cyber superiority*. Springer International Publishing. https://doi.org/10.1007/978-3-319-40554-4

Lannoy, A. de. (2018). *Youth, deprivation and the Internet in Africa*. Retrieved from https://researchictafrica.net/after-access-survey-papers/2018/After_Access:_youth_and_digital_inequality_in_Africa.pdf

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? In *Proceedings of the ACM on Human-Computer Interaction*, *2*, 1–31. https://doi.org/10.1145/3274371

Law Society of South Africa. (2017). Comments by the Law Society of South Africa on the Cybercrimes and Cybersecurity Bill. Retrieved from https://www.lssa.org.za/wp-content/uploads/2020/01/LSSA-CYBERCRIMES-AND-CYBERSECURITY-BILL-Comment-30-Novemeber-2015.pdf

Lee, W, & Rotoloni, B. (2016). *The 2016 Emerging cyber threats, trends and technologies report*. Georgia Institute of Technology. Retrieved from http://www.iisp.gatech.edu/sites/default/files/documents/2016_threats_report_finalblu-web.pdf

Leenes, R. (2019). Regulating new technologies in times of change. In L, Reins (Ed.), *Regulating new technologies in uncertain times* (pp. 1570-2782). Asser Press. https://doi.org/10.1007/978-94-6265-279-8_1

London, R. (2013). *Comparative data protection and security law: A critical evaluation of legal standards*. University of South Africa,.

Lucivero, F. (2016). E*thical assessments of emerging technologies: Appraising the moral plausibility of technological visions*. Springer.

Ludlow, K., Bowman, D. M., Gatof, J., & Bennett, M. G. (2015). Regulating emerging and future technologies in the present. *NanoEthics*, *9*(2), 151–163. https://doi.org/10.1007/s11569-015-0223-4

Makulilo, A. B. (2016). *African data privacy laws*. Springer. https://doi.org/10.1007/978-3-319-47317-8

Mandel, G. N. (2013). Emerging technology governance. In G. E. Marchant, K. W. Abbott, & B. Allenby (Eds.), *Innovative governance models for emerging technologies* (pp. 44-62). Edward Elgar. https://doi.org/10.4337/9781782545644.00009

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. The Citizen Lab. Retrieved from https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

Marques, D., Muslukhov, I., Guerreiro, T., Carriço, L., & Beznosov, K. (2016). Snooping on mobile phones: Prevalence and trends. *In SOUPS 2016: Twelfth symposium on usable privacy and security* (pp. 159-174). USENIX. Retrieved from https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-marques.pdf

Mathur, A., & Chetty, M., (2017). Impact of user characteristics on attitudes towards automatic mobile application updates. In *Thirteenth symposium on usable privacy and security* (pp. 175-193).

Maxwell, J. A. (2014). *Qualitative research design: An interactive approach* (3rd ed.). Sage.

Moller, N. (2012). The Concepts of Risk and Safety. In S. Roeser (Ed.), *Handbook of risk theory: Epistemology, decision theory, ethics, and social implications of risk* (pp. 56–82). Springer. https://doi.org/10.1007/978-94-007-1433-5_3

Moore, A. D. (2017). Privacy, neuroscience, and neuro-surveillance. *Res Publica*, *23*(2), 159–177. https://doi.org/10.1007/s11158-016-9341-2

Moosa, I. A. (2015). *Good regulation, bad regulation. The anatomy of financial regulation*. Palgrave Macmillan. https://doi.org/10.1057/9781137447104

Morgan, B., & Yeung, K. (2007). *An introduction to law and regulation: Text and materials*. Cambridge University Press. https://doi.org/10.1017/CBO9780511801112

Narayanan, V. K., & O'Connor, G. C. (2015). What are emerging technologies? In *Wiley Encyclopedia of Management* (pp. 1-4). Wiley Online Library. https://doi.org/10.1002/9781118785317.weom130058

Neisse, R., Geneiatakis, D., Steri, G., Kambourakis, G., Fovino, I. N., & Satta, R. (2016). Dealing with User Privacy in Mobile Applications: Issues and Mitigation. In *Protecting mobile networks and devices* (pp. 81-106). Taylor & Francis.

Nowrin, S., & Bawden, D. (2018). Information security behaviour of smartphone users. *Information and Learning Science*, *119*(7), 444–455. https://doi.org/10.1108/ILS-04-2018-0029

Ntsaluba, N. (2018). *The cyber security legislative and policy framework in South Africa*. University of Pretoria.

Ogus, A. I. (2004). *Regulation: Legal form and economic theory*. Hart Publishing.

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

Peppet, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review*, *93*(85), 85-176.

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, *50*, 32–44. https://doi.org/10.1016/j.intmar.2019.10.004

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). Applications, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In P. Traynor & A. Oprea (Eds.), *Proceedings of the 2018 network and distributed system security symposium* (pp. 1-15). International Computer Science Institute. https://doi.org/10.14722/ndss.2018.23353

Reins, L. (Ed.). (2019). *Regulating new technologies in uncertain times*. Asser Press. https://doi.org/10.1007/978-94-6265-279-8

Roos, A. (2016). *Data protection law in South Africa*. Springer. https://doi.org/10.1007/978-3-319-47317-8_9

Ruggiu, D. (2018). *Human rights and emerging technologies: Analysis and perspectives in Europe*. Pan Stanford Publishing. https://doi.org/10.1201/9780429490590

SABRIC. (2019). Digital Banking Crime Statistics. SABRIC. Retrieved from https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics

Sarat, A. (2015). *A world without privacy: What law can and should do?* Cambridge University Press. https://doi.org/10.1017/CBO9781139962964

Sethi, S., & Sethi, S. P. (2016). *Globalization and self-regulation: The crucial role that corporate codes of conduct play in global business*. Palgrave Macmillan.

Solove, D. J. (2011). *Nothing to hide: The false trade-off between privacy and security*. Yale University Press.

Sophoslabs. (2019). Sophoslabs 2019 Threat Report. Retrieved from https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

Stalla-Bourdillon, S., Phillips, J., & Ryan, M. (2014). *Privacy vs. security*. Springer. https://doi.org/10.1007/978-1-4471-6530-9

State Security Agency (SSA). (2015, December 4). The National Cybersecurity Policy Framework (NCPF). Government Gazette No. 39475. Retrieved from https://www.gov.za/sites/www.gov.za/ files/39475_gon609.pdf

Subrahmanian, V. S., Ovelgonne, M., Dumitras, T., & Prakash, B. A. (2015). *The global cyber-vulnerability report*. Springer. https://doi.org/10.1007/978-3-319-25760-0

Sutherland, E. (2017). Governance of cybersecurity: The Case of South Africa. *The African Journal of Information and Communication, 20*, 83–112. https://doi.org/10.23962/10539/23574

Taddeo, M., & Floridi, L. (2017). *The responsibilities of online service providers*. Springer. https://doi.org/10.1007/978-3-319-47852-4

Tamò-Larrieux, A. (2018). *Designing for privacy and its legal framework: Data protection by design and default for the Internet of Things*. Springer. https://doi.org/10.1007/978-3-319-98624-1

Tracy, S. J. (2019). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (2nd edition). Wiley Blackwell.

Tropina, T., & Callanan, C. (2015). *Self-and co-regulation in cybercrime, cybersecurity and national security*. Springer. https://doi.org/10.1007/978-3-319-16447-2

Urquhart, L. (2018). Exploring cybersecurity and cybercrime: Threats and legal responses. In L. Edwards (Ed.), *Law, policy and the Internet* (pp. 393-416). Hart Publishing.

Votipka, D., Rabin, S. M., Micinski, K., Gilray, T., Mazurek, M. L., & Foster, J. S. (2018). User comfort with Android background resource accesses in different contexts. In *SOUPS 2018: Fourteenth symposium on usable privacy and security* (pp. 235-250). USENIX.

Westin, A. F. (1967). Privacy and freedom. *Washington and Lee Law Review*, *25*(1):166-170.

Wilk, R. (2018). Internet privacy hogwash. *Anthropology News*, *59*(3):153-156. https://doi.org/10.1111/AN.872

Winder, D. (2019, January 27). How WhatsApp merger with Facebook Messenger puts your privacy at risk. Forbes. Retrieved https://www.forbes.com/sites/daveywinder/2019/01/27/how-whatsapp-merger-withfacebook-messenger-puts-your-privacy-at-risk/#270a7d874e57

Wright, D., & Hert, P. de. (Eds.). (2016). *Enforcing privacy: Regulatory, legal and technological approaches*. Springer. https://doi.org/10.1007/978-3-319-25047-2

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. *Industrial Management and Data Systems*, *115*(2), 253–269. https://doi.org/10.1108/IMDS-08-2014-0243

Zeegers, R. (2018) *Privacy and data protection foundation* (1st ed.). Van Haren Publishing.

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviours of smartphone users in China: An empirical analysis. *The Electronic Library*, *35*(6), 1177–1190. https://doi.org/10.1108/EL-09-2016-0183

# APPENDICES

## ANNEXURE A: ONLINE SURVEY QUESTIONNAIRE

### Section A: Demographic Information

Gender:

*Mark only one value*

☐ Female

☐ Male

Age:

*Mark only one value*

☐ Under 18 years old

☐ 18-24 years old

☐ 25-34 years old

☐ 35-44 years old

☐ 45 years +

Level of qualification:

*Mark only one value*

☐ National Certificate

☐ Bachelor's Degree

☐ Honours Degree

☐ Master’s Degree

☐ Doctoral Degree

Role within your Organisation:

*Mark only one value*

☐ Executive

☐ Management

☐ Technical

Level of experience:

*Mark only one value*

☐ Less than 5 years

☐ Less than 10 years

☐ More than 10 years

### Section B: Survey Questions

**Emerging Technologies**

1. Do you store any personal data in the cloud through e-mail or cloud storage

*Mark only one value*

☐ Yes

☐ No

2. Do you use devices that connect to the Internet at home such as smart TVs, watches or any other appliance?

*Mark only one value*

☐ Yes

☐ No

3. Do you use online banking services on your smartphone?

*Mark only one value*

☐ Yes

☐ No

4. How often do you use any of your other smart devices to store your personal information (such as email address or phone number?)

*Mark only one value*

☐ Frequently

☐ Moderately

☐ Rarely

☐ Not at all

☐ Don't Know

5. Are emerging Internet technologies i.e. Internet-of-Things making it easier to hacked or cyber-stalked?

*Mark only one value*

☐ Very Easy

☐ Somewhat Easy

☐ Average

☐ Somewhat Difficult

☐ Very Difficult

**Privacy**

6. Which of these do you perceive to be the biggest threats to users' cyber-security and privacy today?

*Mark all that apply*

☐ Hackers [using key loggers, trojans, etc]

☐ Data Breaches [theft of users' personal data]

☐ Government Surveillance

☐ Social Engineering [in combination with phishing]

☐ Other (please specify)

7. What is your largest concern regarding cybersecurity/privacy

*Mark only one value*

☐ Lack of Regulatory compliance

☐ Costs of implementation

☐ Need for constant updating of systems

☐ Skills/Expertise shortage for system maintenance

☐ Artificial intelligence & machine learning

8. Data controllers such as Google or Amazon store a lot of data on their users. How effective do you believe their protections for consumers' data to be?

*Mark only one value*

☐ Very Effective

☐ Effective

☐ Moderate

☐ Weak

☐ Very Weak

9. Do you read User Agreements with companies before signing up for their services such as cloud storage?

*Mark only one value*

☐ Yes

☐ No

9.1. If you answered No, why?

*Mark all that apply*

☐ I trust they will protect my data

☐ The End-User Agreement is too long

☐ I don't understand the technical language in the contract

☐ Other (please specify)

10. Have you ever personally experienced a loss of private data through your mobile phone or other Internet-enabled device?

Mark only one value

☐ Yes

☐ No

11. What tools do you use to protect your privacy when online?

*Mark all that apply*

☐ Virtual Private Networks, Proxy Services & Onion Routers

☐ Crypto-Currencies i.e. Bitcoin

☐ Encrypted Cloud Services

☐ Password Generators

☐ Ad & Pop-up blockers

☐ None

12. How can developers or innovators of new Internet technologies improve privacy in their products/services?

*Mark all that apply*

☐ Add privacy as a main feature to their products/services

☐ Have better privacy policies

☐ Comply with data protection laws

☐ Use less personal data or allow users to control their own data

☐ Engage users continually for feedback

☐ Other (please specify)

**Regulation**

13. Which region of the world do you believe has the best data protection laws?

*Mark only one value*

☐ North America

☐ European Union

☐ Asia-Pacific

☐ Africa

☐ South America

14. Do you believe competing interests such as national security or the need to make profits pose a challenge for privacy?

*Mark only one value*

☐ Absolutely

☐ Sometimes

☐ Never

15. Which of the following concepts is most relevant to how you view privacy?

*Mark only one value*

☐ Risk

☐ Consent

☐ Trust

Do you have any extra comments to make or issues you would wish to highlight? Thank you for your participation!

## ANNEXURE B: REGULATOR INTERVIEW GUIDE

**Section A: Demographic Information**

Please provide me with a few details about yourself and your role at the organisation.

*Gender:*

*Age:*

*Level of experience:*

*Role within your Organisation:*

*Sector of the Organisation:*

**Section B: Questions based on research objectives.**

**Cyber-security**

1. In your opinion, do data controllers offer sufficient protections for users' data?

2. What are some of the biggest threats to users' security and privacy today?

3. How best can users manage their cyber-security when online?

**Data Protection**

4. Which region of the world do you believe has the strongest data protection laws and why?

5. Do you believe the differences in approaches to data protection laws in the world are a challenge to building a secure Internet?

6. How can current data protection laws be improved?

7. Are competing interests such as national security or profit motive a challenge for privacy today? Why?

**Emerging Internet technologies**

8. Are emerging Internet technologies making it easier to conduct harmful activities such as hacking or stalking in today's world?

9. What challenges do regulators face in regulating emerging technologies?

Are there any other issues you would like to raise? Thank you.