IST-Africa 2017 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2017
ISBN: 978-1-905824-56-

Do Users Know or Care About What is Done with their Personal Data: A South African Study

Ntsako BALOYI[1], Paula KOTZÉ[1,2]
[1]CSIR Meraka Institute, PO Box 395, Pretoria, 0001, South Africa
Tel: +27 12 8412594, Fax: +27 12 8414270 Email: NBaloyi1@csir.co.za
Tel: +27 12 8412268, Fax: +27 12 8414270, Email: paula.kotze@meraka.org.za
[2]Department of Informatics, University of Pretoria,
Private Bag X20, Hatfield, 0028, South Africa

Abstract: People engage with various technologies in their daily lives and become data subjects when they share personal information with software, devices, services or organisations. Sometimes individuals may be oblivious to the fact that their personal data is being captured, or of the possible ramifications, once their personal information is outside their control. Data protection has become an area of great interest across the globe as it directly affects fundamental human rights and particularly the right to privacy. The objective of this paper is to explore the extent to which individuals within South Africa are knowledgeable or concerned about the collection, use, transfer, etc. of their personal data. Based on the information collected using a survey, it was found that individuals in South Africa do care about their personal data privacy, although they are not always familiar with legal regulations governing personal data protection or legal rights related to their personal data.

Keywords: Personal data, data protection, POPI Act, PAI Act.

1. Introduction

Data is the basis for information and consequently for decision-making. Information is very important in everyday life [1], and drives the way we live and operate in today's digital-driven world. However, data collected by digital devices nowadays often concerns private affairs or personal information that may be sensitive. People tend to expose information or have information about them exposed consciously and/or unconsciously [2, 3]. Can people still have private lives and sacred spaces in the digital world, and do they care to preserve that sanctity of their private lives?

A 2002 South African study to determine consumer perceptions about information privacy from a marketing perspective, found that 69% of the participants had been victims of invasion of personal information [4]. This paper seeks to examine the issue of data privacy further and explores whether South African residents and citizens in 2016 are conscious of the implications of sharing personal data, are aware of the risks associated with personal data collection and processing, and if they care at all what happens with their personal data.

1.1 Technological Developments and the Collection of Personal Data

The past few decades have brought about substantial technological developments. The trend of technological advancement continues on an upward trajectory at a rapid rate. This inarguably much needed progress within the technology space has brought unparalleled benefits to individuals, governments and businesses [1]. The flip site of the coin is that the

same development has brought with it many challenges, one of which relates to the processing of personal data and the invasion of what previously was considered private [1].

A few years ago the words 'information age' were very popular. There can hardly be any argument against the assertion that data or information runs today's world. Data plays a significant role in various aspects of life, public and private. The use of personal data can bring both social and economic benefits and these benefits must be juxtaposed against data privacy risks [1]. Personal data combined with data collected on online behaviour can be used to personalise services, provide targeted solutions and improved experiences, although not all would agree that such is desirable [5]. Personal data can be both sensitive and non-sensitive [6]. This distinction comes out in most data protection instruments.

More and more technologies and applications collect and process increasing amounts of personal data [1]. On the other hand it appears that people are becoming more and more generous when it comes to sharing their personal information [3]. Technological solutions, like the internet of things, big data, cloud computing, smart systems, etc. [7], are built around data, some of which may involve sensitive personal information. Personal data has become a commodity; an object of trade [5]. Some of the ways in which personal information is collected include the use of cars, smart phones, software applications, wearables, websites and even through sales organisations [3, 8].

1.2 Personal Data Protection

Voltaire is credited for being the first to craft the phrase 'with great power comes great responsibility' [9]. It can be said that with great data comes great responsibility and furthermore, with personal data comes even greater responsibility. The level with which personal data is collected, shared and processed staggers belief [1, 2, 5]. The risk to people's privacy is apparent. Furthermore people's data is sometimes collected without the knowledge or consent of the data subject [10]. Human life today is characterised by traceable digital footprints, which can be detrimental to ones' safety and privacy [1].

The handling and safeguarding of personal data by both the subject of the personal data and users of such data, may not always be an easy task, but it has become a necessity. There often has to be a trade-off between convenience and data protection. Whether people vote for convenience or simplicity over privacy is one of the aspects covered in this paper.

1.3 Data Protection Laws

The focal point of data protection laws is a person, or better put: the data subject. A data subject is a person whose identifying data is the subject of collection or processing [11]. Personal data is thus defined as information about an identified or identifiable individual [12]. Data subjects may sometimes not even be familiar with implications attached to their sharing of personal data or the processing thereof by organisations. Data protection laws seek to protect vulnerable people from excessive or abusive collection and use of their personal data, especially sensitive personal data. This is not surprising as people are vulnerable to abuse of power by governments and businesses. It is an entrenched principle in law that private individuals are not on equal footing with government and businesses and hence they need a greater level of protection [13].

Personal data protection is a subject of interest for many legislative bodies and data protection authorities around the world [14]. Many countries take a human rights approach to data protection premised on the right to privacy. Consumer protection laws and other similar laws around the world, take a similar approach to the protection of individuals as that followed by most data protection legislation when it comes to treating ordinary individuals as being in a position of vulnerability. The European Union (EU) has gone further to include data protection as a fundamental right alongside the right to privacy [15]. It however appears that many countries which follow a human rights approach to data

protection, especially those that have data protection laws, or have recently enacted such laws, are actually pressured to do so by economic or commercial interests with foreign countries that already have such laws and prohibit transfers of information to countries without 'adequate data protection' laws [11]. This trend could stem from the bias of the initial international organisations that have been involved in the data protection space, starting with the Organisation for Economic Co-operation and Development (OECD), a trade or economic focused international organisation, followed by the Council of Europe, a human rights organisation, and the EU, which is both a political and economic partnership [3]. The data protection laws seem to want to balance economic, human rights and political interests.

Two primary legislation have been promulgated in South Africa regulating personal information, namely the Protection of Personal Information Act (POPI Act) [11] and the Promotion of Access to Information Act (PAI Act) [16]. South Africa enacted the POPI Act, which regulates the protection of personal information, on 26 November 2013. Certain sections of the POPI Act are already in effect, whilst some are still suspended pending the appointment and functioning of the information regulator [3]. The information regulator was appointed on 7 September 2016, but has at the time of writing this paper not yet release any regulations on the two Acts [17]. The POPI Act [11] applies to both electronic and non-electronic personal information, as well as to both natural and juristic persons. It sets out the rights and remedies for data subjects in relation to their personal information, as well as the responsibilities of responsible parties (data controllers) and operators (processors) to be regulated by the information regulator. The PAI Act does also regulate the right to access to, and the correction of information, including personal information held by public institutions and other persons, which is needed to protect or exercise any rights subject to justifiable limitations.

2. Objectives

This paper reports on a study of current perceptions, knowledge and practices of individuals concerning the supply, sharing and use of their personal information in South Africa. In general, the study seeks to determine people's concerns with their personal data collection, usage or processing, knowledge of their legal rights related to personal data protection, risks associated with sharing personal data and types of personal data collection methods.

This paper does not address the issue of organisations' compliance with personal data protection or privacy legislation. This issue is addressed in a separate paper [18].

Section 3 of the paper addresses the methodology followed to collect and process the data for the study. Section 4 presents the results of the survey. Section 5 concludes by discussing the findings and business benefits or the value that could be derived from the results of the survey.

3. Methodology

The study was quantitative in nature. As part of a wider research project, a survey was conducted to collect information on the perceptions and knowledge of current practices related to personal data protection in South Africa. The purpose of the survey was to identify and highlight individuals' attitudes and practices towards the sharing and protection of personal data.

The survey consisted of 12 questions requiring 'yes' or 'no' answers. A statement accompanied the questionnaire on what the survey is about, that participation is confidential and voluntary, and that responses would be used for research purposes only. In line with the theme or spirit of the research, no personal identifying information was collected and

participants completed the questionnaire anonymously without an option to include their demographic information.

The survey questions mainly addressed four key areas.

1. How individuals share personal data and their familiarity with privacy statements.
2. Individuals' knowledge of their legal rights in relation to personal data processing and protection, as well as the consequences attached to the misuse or compromise of personal data.
3. Individuals' reputational risks and trust towards organisations collecting and processing personal data.
4. Individuals' awareness of the personal data collection methods and usage or processing examples.

Snowball sampling was used, where the participants directly targeted were requested to further disseminate the survey to any community of individuals. The first group of participants approached to complete the survey included individuals with a wide spectrum of professional backgrounds, for example, individuals working in the pharmaceutical, healthcare, banking, telecommunications and information and communications technology (ICT) industries, individuals from government, ICT research organisations and academia, as well as students and friends. The survey was distributed via email and various social media platforms. Google Forms was used to capture the responses of individuals. The survey was run for a period of six weeks, from the last week of October 2016 to the second week of December 2016. In total 138 responses were received, mainly from participants within South Africa.

A Pearson correlation coefficient analysis [19] was performed on the results for the various questions to determine whether a relationship exists between responses to any two questions. For a data set of n=138, any coefficient value ($|r|$) equal or above 0.17 indicates a significant relationship. The Evans' guide [20] is used to classify the relationship strength (0.00-0.19 – very weak; 0.20-0.39 – weak; 0.40-0.59 - moderate; 0.60-0.79 – strong; 0.80-1.00 - very strong).

This study does not claim to be exhaustive of personal data protection related issues or to be a fully representative sample.

4. Findings

This section presents the results of the survey and a brief discussion of the findings.

4.1 How Users Share Their Personal Data

4.1.1 Use of Devices or Electronic Applications

Participants were asked whether they use a smart phone or any device that collect, process or use their personal information (e.g. email, cell phone, health data, location data, etc.). One hundred and thirty two participants responded to this question. As per Figure 1, only 2.9% said they did not have or use a device or application that collects or process personal information. The authors are of the view that the 2.9% participants that responded in the negative might be ignorant of some of the methods of collecting personal information like cookies, cell phone tower triangulation, etc. [3]. This view is based on the fact that all these participants captured their responses electronically via Google Forms, which is an electronic medium with the ability to collect information on users. There is thus a high probability that these participants also do use other applications, devices or services that collect personal information, albeit unawares.

4.1.2 Reading of Privacy Statements

As depicted in Figure 1, when asked whether participants thoroughly read privacy statements or notices of websites, devices and applications that collect or process personal information, 79% said that they did not, whilst only 21% said they do. In this case, it seems that people choose convenience over privacy and brush off the reading of privacy statements to determine the level of protection provided by the policies.

These results confirm the Brazilian study on the use of social media [21], which found that users generally do not carefully read privacy statements. This could be an indicator that more needs to be done to raise people's consciousness about data privacy and protect them from such inadvertent but yet detrimental actions. The findings somewhat contradict the 2002 South African study [4], in which participants expressed an interest in companies having privacy policies and government regulating the processing of personal information, since they hardly read those privacy statements.

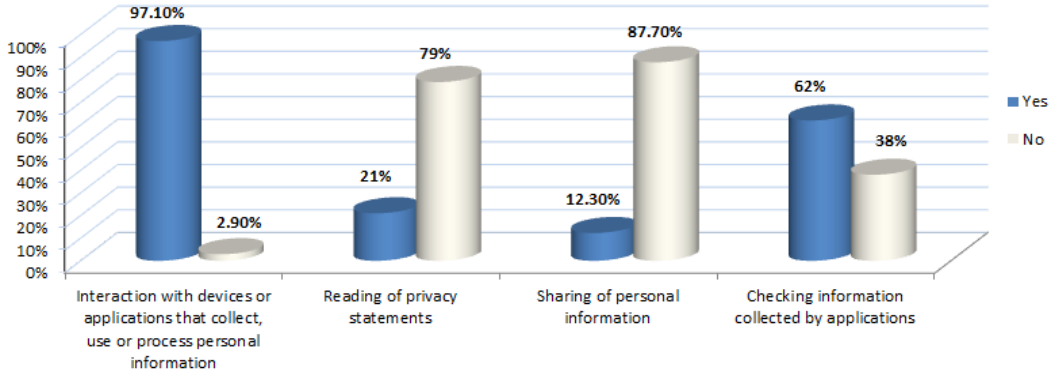

Figure 1: User sharing and checking of personal data

4.1.3 Sharing of Personal Information

Participants were asked whether they allow the sharing of their personal information collected by organisations through devices, applications, etc., with other organisations. In this regard, 87.7% of participants, as illustrated in Figure 1, indicated that they prohibit the further sharing of their personal information. The authors are of the view that the 12.3%, which do allow the further sharing of their personal information, might be a further indication of the need to educate people about their personal privacy as it relates to the sharing of personal information. In this regard, Ghana has already engaged in public awareness campaigns [22] and South Africa should follow suit in future. The findings correspond with the 2002 South African study [4] that found that 90% of participants were uncomfortable with companies sharing their personal information.

It is also noteworthy that some of the participants were young adults (students) who may not have yet suffered more serious personal data related crimes like identity theft, unauthorised debit orders and the likes. Peoples' socio-political status may also influence their view of what they consider to be in their best interest as relates to transactions with privacy implications.

4.1.4 Checking Information Collected by Applications

When asked whether participants checked the kind of information collected by applications before installing software applications, the majority of participants (62%), as illustrated in Figure 1, indicated that they do check, whilst 38% indicated that they do not. Only one participant did not answer this question, bringing the total number of responses to this question to 137.

It appears that users find a summary view of the type of collected information, as displayed by most services, sufficient to determine their decision to install or not to install a

particular application. This could also explain why 79% of people do not read privacy statements, as discussed in 4.1.2. The correlation between responses for the two questions is significant but very weak (r=0.17). Previous studies (e.g. [5, 15]) have shown that knowledge of the type of information collected does not necessarily imply that users act rationally when installing applications.

4.2 Individuals' Knowledge of Their Legal Rights, the Law and Consequences of Personal Data Compromise or Misuse

4.2.1 Dangers Attached to Loss/Misuse of Data

When asked whether participants knew of the dangers attached to the loss or misuse of their personal information in the hands of those collecting or processing it, only 79.7%, as presented in Figure 2, indicated that they were aware of the dangers related to such loss or abuse of the processing of personal information. The 20.3% respondents that stated that they were not aware of the dangers, is of concern as there can be serious financial, reputational and identity related problems associated with the loss or misuse of personal information [23]. This finding confirms the assertion made above concerning the need to educate people about data privacy.

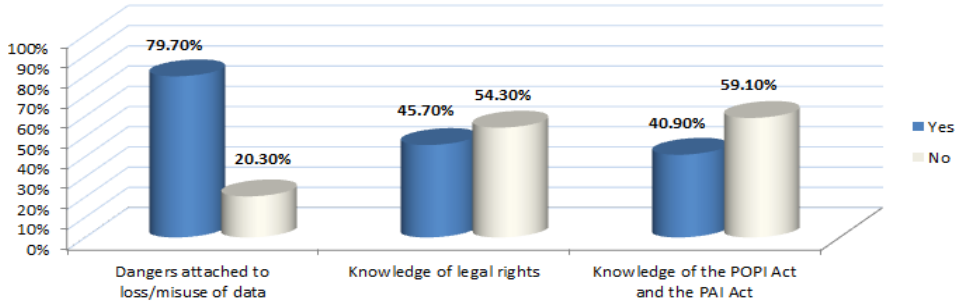

Figure 2: Knowledge of rights, law and consequences

4.2.2 Knowledge of Legal Rights

When participants were asked whether they are aware of their legal rights as it relates to the collection and processing of personal information, only 45.7% indicated that they are, as illustrated in Figure 2. This number is quite low compared to those that do not know their rights (54.3%).

Since such a large proportion of people do not know their legal rights, it is not surprising that 12.3% of participants did not mind their personal information being shared with other organisations and that as much as 20.3% do not even know the dangers associated with personal data compromises. A weak but significant relationship (r=0.32) was indeed found to exist between responses to the question under discussion and the ones on the sharing of personal information. The findings corroborate the 2002 South African study [4] in which 70% of the participants were not aware of how to exercise their right to have personal information deleted.

4.2.3 Knowledge of Current Legislation

As a follow up to the question on knowledge of legal rights, participants were asked whether they were familiar with their rights under two primary legislations in South Africa regulating personal information, namely the POPI Act [11] and the PAI Act [16]. Only 137 participants answered this question. As illustrated in Figure 2, only 40.9% of the participants were familiar with their rights under the two Acts, whilst the majority (59.1%) were not. This is in line with the results on the knowledge of an individual's legal rights with regard personal information, where the majority of individuals indicated that they are

not familiar with their legal rights. Using a Pearson correlation coefficient analysis [19], it was determined that there is a indeed a strong relationship (r=0.67) between the responses to the legal rights and POPI Act and PAI Act questions. A campaign like the Ghanaian 'Know Your Rights' campaign [22] to educate citizens on their legal rights might be a way to go for South Africa.

4.3 Individuals' Reputational Risks and Trust Towards Organisations Collecting and Processing Personal Data

4.3.1 Trust in Organisations that Collect Personal Data

In order to check user confidence towards organisations that collect and process personal information, participants were asked whether they trust organisations that collect their personal information to protect it accordingly. As illustrated in Figure 3, the majority of participants (71.9%) indicated that they do not trust such organisations to safeguard their information, whilst only 28.1% showed confidence towards such organisation's safety measures. Only 135 participants answered this question.

It is interesting to compare this result with the 79% of the participants that said they do not thoroughly ready privacy policies, and yet 71.9% do not trust that their personal information will be kept safe. This lack of trust could be fuelled by prevalent media reports of information technology system and network security breaches, both locally and internationally [1].

A 2012 study conducted in the United States of America (USA) indicated that 34% of participants did not trust any organisation with their personal data [21]. Whilst the USA study might be a bit outdated and indicative of the trust culture in the USA, the result of our study confirmed the USA study, with an even greater pessimistic perspective or attitude towards organisations that collect personal information. This shows that organisations should work hard to win back people's trust and avoid further reputational damage, which could even lead to loss of customers and sanctions where organisations fail to comply with data protection laws [23]. The 2002 South African study [4] also indicated concerns about trust in organisations that collect personal data.

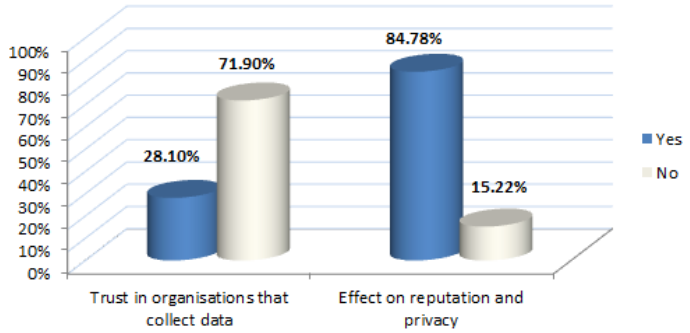

Figure 3: Reputational risks and organisational trust

4.3.2 Effect on Reputation and Privacy

Participants were also asked whether they thought that their reputation or privacy might be impacted by the loss or compromise to their personal information shared with, or collected by organisations, applications or devices. As illustrated in Figure 3, 84.78% of participants are concerned about reputational and/or privacy effects that can stem from their shared or collected personal data. Only 15.22% responded in the negative, some of whom might think that they have nothing to hide, thereby downplaying their own privacy interests.

4.4 Unsolicited Collection, Use and Transfer of Personal Data

4.4.1 Passive Collection of Information

Over and above mobile phone and computer applications, certain other devices/equipment such as cars, IoT devices, etc. might collect certain information about individuals or their activities without the individual's knowledge. Participants were asked whether they were aware of such passive collection of personal information by devices and applications without their knowledge. As illustrated in Figure 4, 76.5% of participants confirmed that they are aware of such unsolicited collection of their personal information. The remaining 23.5% said they were not aware of such collection. Only 136 responses were recorded on this question.

Although individuals may be aware of the passive collection of their personal information, by for example cars, there is sometimes very little that they can do about it.

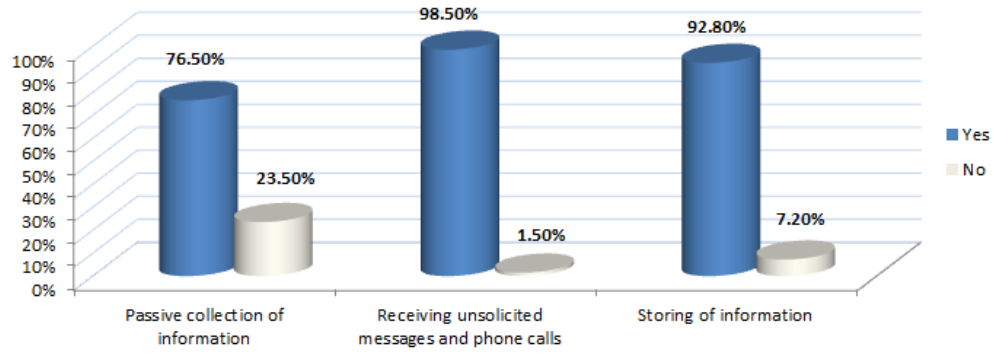

Figure 4: Unsolicited collection, use and transfer of personal data

4.4.2 Receiving Unsolicited Messages and Phone Calls

Participants were asked whether they have ever received any unsolicited communication in the form of calls, text messages (SMSs) and emails from organisations/individuals to which they were not connected. As indicated in Figure 4, 98.5% of participants confirmed that they did receive such communication. Only 1.5% of participants said that they have never been on the receiving end of such targeted communication. This outcome is a clear indication of the sharing of individual's personal information by people or organisations already in possession of such information, whether with or without the data subject's prior approval or consent. Even though the extent of receiving unsolicited messages was lower in comparison, the 2002 South African study already indicated that 74% of participants were bothered by receiving unsolicited advertisements [4].

4.4.3 Transborder Transfer, Storage and Processing

When asked if they were concerned that sensitive information about themselves might be stored somewhere, possibly outside South Africa, and that such information may be exposed or misused, 92.8% of the participants indicated that they were concerned, as illustrated on the far right of Figure 4.

Using a Pearson correlation coefficient analysis [19], indicated that there is a moderate relationship (r=0.43) between responses to this question and the one on reputational or privacy effects due to information compromise. This may indicate the level to which people want to feel in control of their information as both questions relate to an element of data exposure.

These results clearly indicate that many people are not comfortable with transborder transfers of their personal information. This is quite intriguing as most software applications and devices that people use in South Africa actually belong to, or are

manufactured by, international organisations, which may in turn store the information that they collect beyond the borders of South Africa.

4.5 Additional Analysis

In addition to the Pearson correlation results mentioned in the discussions above, several other weak but significant relationships were found between data sets:

- There is a very weak correlation (r=0.17) between knowledge of ones' legal rights as they pertain to the protection of personal information and reception of unsolicited communications.
- There is a weak correlation (r=0.21) between knowledge of ones' legal rights as they pertain to the protection of personal information and checking information collected by applications, as well as with reading privacy statements.
- There seems to be a weak correlation (r=0.20) between knowledge of the Acts on personal information and knowledge of dangers associated to the loss or misuse of personal data, as well as with thoroughly reading privacy statements.
- There is a weak correlation (r=0.24) between trust in organisations collecting personal data and allowing them to share it.
- A weak correlation (r=-0.21) was found between concerns about reputation and passive collection of personal data. This means that a concern with the loss of reputation is correlated to the knowledge about the passive collection of information by cars and other devices.
- A weak correlation (r=-0.21) between concerns about reputation or privacy and allowing organisations to share personal data. This means that a concern with the loss of reputation is correlated to not allowing personal information to be shared with other organisations, etc.
- A very weak correlation (r=-0.19) exist between knowledge of the dangers relating to and allowing organisations not to share personal information with other organisations, etc.

5. Conclusions

From the results of the survey, it appears that many South Africans do care about their personal data privacy although they may not always be familiar with legal regulations governing personal data protection or their data protection related rights. These results confirm the results of the Brazilian survey [21], which found that Brazilians, and indeed people in general, do care about their privacy.

A generalisation with regards to people's concern about their data privacy is justified. Whilst many people do not thoroughly read privacy statements, they do not easily allow organisations to share their personal data, when prompted, and do check the kind of personal information collected by software applications before installation. Many people appear to be aware of the dangers that can emanate from misused or compromised personal information and are anxious that their privacy or reputation may be affected as a result. Caution should be taken in this regard, as people from different socio-political backgrounds may have different perceptions about personal data protection and privacy.

It is also clear that many people use software or devices that collect personal information and are aware that most such software and devices may collect their personal data without their consent or knowledge. Confidence in organisations that collect and process personal data to safeguard it is very low and people are largely not comfortable with organisations transferring or storing their personal information outside South Africa.

Software developers, device and car manufactures, as well as businesses and governments can no longer afford to treat data privacy as an afterthought. People are

starting to demand not only online privacy, but also the protection of their offline data. The South African legislature has followed the European model of protecting both online and offline personal data [3, 24], but South Africa goes one step further to provide personal data protection to juristic persons/individuals (e.g. companies).

Things are not all rosy though, as there are people that are still ignorant about privacy implications or do not act in line with their convictions (or rationality). It is recommended that government, business, research institutions and civil society should run programmes to inform and educate people about their rights as it relates to personal information, and train them on personal data protection fundamentals in a digital society. It was indeed also hoped that the survey and the study conducted would nudge participants and the general public to start thinking about personal data privacy issues.

Future work will involve an investigation into personal data protection within organisations, as well various data protection regulations and practices around the world. The study can also be repeated for specific target groups such as high school students, people in specific geographic locations and the likes.

References

[1] OECD, *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)*, in *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 2013, OECD. p. 19 - 37.

[2] Li, Y., et al., *Privacy protection for preventing data over-collection in smart city.* IEEE Transactions on Computers, 2016. **65**(5): p. 1339 - 1349.

[3] Roos, A., *Data privacy law*, in *Information Communications Technology Law*, D. van der Merwe, Editor. 2016, LexisNexis (Pty) Ltd: Johannesburg. p. 363-487.

[4] Jordaan, Y., *South African Consumers' Information Privacy Concerns: An Investigation in a Comercial Environment*, in *Marketing and Communication Management*. 2003, University of Pretoria: Pretoria. p. 395.

[5] Kitchin, R., *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security*. 28 January 2016 ed. 2016, Dublin: Data Protection Unit, Department of the Taoiseach. 82.

[6] Ajigini, O.A., *A Framework to Manage Information During its Migration Between Software Platforms*, in *Information Systems*. 2016, University of South Africa: Pretoria. p. 369.

[7] Edwards, L., *Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective*. 2015, CREATe: Glasgow. p. 1 - 37.

[8] Escribano, B., *Privacy and security in the Internet of Things: Challenge or Opportunity*. 2014, Olswang. p. 1 - 7.

[9] Gleneicki, A.F., *With great power comes great responsibility*, in *FutureLab*. 2014, FutureLab.

[10] Popescul, D. and L.D. Radu, *Data security in smart cities: challenges and solutions.* Informatica Economică, 2016. **20**: p. 29 - 39.

[11] Government of South Africa, *Protection of Personal Information Act*. 2013.

[12] OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 1980.

[13] Beukes, M., *Administrative Law: Only Study Guide for ADL2601*. 2010, Pretoria: University of South Africa.

[14] Tesfachew, T., *Global developments and lessons learned*, in *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. 2016, United Nations: Geneva. p. 23 - 29.

[15] Eskens, S.J., *Profiling the European Consumer in the Internet of Things*, in *Information Law*. 2016, University of Amsterdam.

[16] Government of South Africa, *Promotion of Access to Information Act*. 2000.

[17] Kula, S. *Appointment of the Information Regulator for POPI and PAIA*. 2016.

[18] Baloyi, N. and P. Kotzé, *Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations?*, in *IST-Africa 2017 Conference*. 2017, IEEE: Windhoek.

[19] Krehbiel, T.C., *Correlation coefficient rule of thumb.* Decision Sciences Journal of Innovative Education, 2004. **2**(1): p. 97.

[20] Evans, J., *Staightforward Statistics for the Behavioural Sciences*. 1996, Pacific Grove: Brooks/Cole Publishing.

[21] dos Santos Brito, K., et al., *How people care about their personal data released on social media*, in *2013 Eleventh Annual Conference on Privacy, Security and Trust (PST)*. 2013, IEEE. p. 111 - 118.

[22] Antwi-Boasiako, A., *Implementation of data protection legislation – the case of Ghana*, in *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. 2016, United Nations: Switzerland. p. 117 - 120.
[23] Liquid Telecom, *A law unto themselves*, in *Cybersecurity & Data Protection Africa Report*. 2016, Liquid Telecom. p. 12 - 13.
[24] The European Parliament and the Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council.* Official Journal of the European Communities, 1995. **281**: p. 31 - 50.