Measuring the implications of Vicarious Liability under the Protection of Personal Information Act in Small, Medium and Micro Enterprises in South Africa

Kimberly Beth Watson

WTSKIM004

Supervisor: Richard Higgs

Minor Dissertation presented in partial fulfilment of the requirements for the degree of Master of Philosophy specialising in Digital Curation

Library and Information Studies Centre

University of Cape Town

2018

Plagiarism Declaration

I understand the meaning of plagiarism and declare that all of the work in this document, save for that which is properly acknowledged, is my own.

Signed by candidate

Kimberly Beth Watson

Acknowledgements

Special thanks to my supervisor Richard Higgs for his guidance and patience throughout this process. I would also like to thank Dr Peter Tobin for helping me contact suitable interview candidates, as well as the interviewees themselves for their willingness to participate in this study.

Thank you to my colleagues Sarah Schäfer and Lindsay Callaghan, who were always ready to discuss strategy. Last my family, Donia, for taking the time to edit. To Rilke, Kate, Lauren, Kathryn, Kathleen, Marge, Maryann, Lisa, Carmomma, Regina, Jim, Eyal, and Collin. Without you I do not know where I would be.

This work is dedicated to my husband Robin for his grace, compassion, and unfailing love.

Abstract

Protecting personal information has become of utmost importance in the digital age. The South African Protection of Personal Information Act has in some ways given the customer more control over how companies can contact them or sell their information to third parties. While this Act is in the best interests of both consumers and businesses in South Africa, there has been concern about how it is to be implemented, and many businesses have not yet introduced procedures to ensure compliance. Particular aspects of the Act make it unlike other legislation that inspired it. The vicarious liability clause specifies the employer as the party responsible should any breach be made by an employee within the company. Many researchers and those who work with the law find this clause particularly divisive, leaving little room for employers to prove they have made adequate changes and educate colleagues on new processes. Those who lack resources, specifically small, medium, and micro enterprises (SMMEs), are particularly at risk. This study surveys a sample of attitudes towards vicarious liability, and investigates processes that have been changed as a result of the Act within an SMME workplace in the Western Cape region.

The results of the study demonstrate that while some employees claimed their colleagues were educated thoroughly, many were not aware of the consequences of vicarious liability, nor did they understand how it worked. There were clear apprehensions regarding general awareness of the Act on the part of both businesses and the general public. Many SMMEs are in the process of developing new standard operating procedures in the wake of this legislation, but there is still notable concern that there will not be enough time or resources to effect these changes.

Further research needs to be done to recognise the challenges that smaller companies face as privacy policies continue to develop in South Africa. The country faces a unique set of challenges that cannot be compared to the socio-economic situation of the developing world.

Abbreviations and acronyms

AT: Accountability Theory

HOA: Homeowners' association

HOO: Head of Operations

IP: Information privacy

PBD: Privacy by design

POPIA/PoPI: Protection of Personal Information Act

PI: Personal information

PIVC: Personal Information Value Chains: the use of big data to form personal information chains about individuals. This forms patterns and becomes a series of predictions about a specific customer.

SA: South Africa

SMMEs: Small, Medium and Micro-Enterprises

UCT: University of Cape Town

Table of Contents

CHAPTER 1

Introduction

1. Background

The Protection of Personal Information Act (Act 4 of 2013) (South Africa. PoPI) was promulgated by the Parliament of the Republic of South Africa in November 2013 and signed into law by President Jacob Zuma on 19 November 2013 (Swartz & Da Veiga, 2016:9). New legislation effectively regulates the ways in which personal information (PI) may be processed. According to the Act, such information includes common data regularly collected by companies, for example, medical, financial and biometric information (Swartz & Da Veiga, 2016:10). The PoPI Act and other legislation regarding information privacy and the protection of citizens from cybercrime in Africa have been developed in the wake of similar legislation in European countries and the United States. The PoPI Act aims to protect South African consumers by giving them more control over how and when their information is shared, who has access to this information, and why. Furthermore, it demands that companies and organisations use responsible methods for storing and collecting this sensitive data. The bill was signed into law on 19 November 2017, giving all relevant institutions a one-year grace period.

There appear to be cultural issues specific to Africa regarding information privacy (IP). It is noteworthy that the African Union Charter “fails to mention privacy, [which indicates] that privacy is not considered a necessary right for Africans,” and instead focuses on Ubuntu ethics and moral values (Borena, Belanger & Ejigu, 2015:493). Alex B. Makulilo alludes to the fact that “privacy is a value that has its roots in the Western world” and so the “push by the West for such countries to adopt privacy laws”

is challenged “on account of ‘cultural imperialism’ or ‘one size fits all’ arguments” (2015:78). African countries and other developing areas in the world are affected by Western privacy laws because of the “powerful … desire to engage in global e-Commerce,” while recognising “trust as … a fundamental component of the new economy” (Makulilo, 2015:79). This research is therefore sensitive to the reality of how IP has developed on the continent.

Data privacy policies in Africa began to evolve during the era of the African struggle for independence during the 1950s, and the constitutions of the newly independent countries “had many influences from the West, allegedly because they were made by … colonial powers [and thus protected] the minority White settlers and foreign companies in the colonies after independence” (Makulilo, 2015:79). Dennis Ocholla points out aspects of privacy that belong to and easily fit into the narrative of Western understandings of privacy. Ocholla discusses four main theories of privacy and their implications when they are extrapolated beyond the geographical location where they were created. He suggests that in most instances, “equality and human rights as experienced and perceived by these groups are utopian in nature, what is naturally right to them is often decided not by themselves, but by some superior body” – such as those at the top in a given social hierarchy by virtue of politics, culture, traditions and/or the religion of the community (2009:80). Consequently, the tradition of information ethics needs to be re-examined when transferred to new or different contexts. It is irrational to transplant information management practices and ethics blueprints into a context within which they did not evolve, at least without close examination of the consequences. Additionally, the lack of internet penetration in

many parts of the continent hinders the creation of a clear picture of individual consumers (Nadasen, Pilkington & Da Veiga, 2016:6).

Despite its Western ethical foundations, information privacy was nevertheless deemed sufficiently important in the South African context for the creation of the PoPI Act, which seeks to align South African with European best practices for sensitive data management. The legislation will to an extent affect all SMMEs because the information life cycle, as well as the manner in which information is created and processed, must comply with the legislation at every stage (Hinde, 2014:29).

PoPI aligns South Africa with progressive Western ideas regarding IP, and positions the country to become a more economically sustainable country, while supporting the privacy of its citizens. On 2 December 2016, the South African government created an Information Regulation body, whose objective is to independently monitor and enforce compliance with the Act. The body is comprised of Pansy Tlakula, Lebogang Cordilia Stroom, and Johannes Collen Weapond, as well as Tana Pistorius and Sizwe Snail Ka Mutze as part-time members (South Africa. Department of Justice, 2016). The body is financed by the Minister of Justice and the Treasury, and the members will hold their positions for a 5-year term.

1.2 POPI Act and privacy within South Africa

It may be suggested that human behaviour is affected and influenced by Big Data, an assertion supported by John Gilliom's observation that "surveillance of human behaviour is in place to control human behaviour," as it can lead to self-censorship and inhibition (Kang & Gilliom as quoted in Solove, 2009:493). Governance models for Big Data and the protection that currently exists to manage PI are meagre in

comparison to the number of algorithms that can create more knowledge about data subjects (people or variables that are being studied) than the data subjects care to reveal. A study conducted for a European Commission defines Big Data in terms of volume (amount), velocity (speed at which the data grows), variety (its nature; numeric, free text, audio, video), complexity (how the data links with other data) and value (how much it is worth when exploited) (Barbero et al., 2016:13). Richards and King note that "technologists often use the technical '3-V' definition of big data as 'high volume, high-velocity and high-variety' information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (2014:394). Private or sensitive information is defined as any details that can personally identify an individual such as name, age, race, ID number, email address, location (history online and offline), purchase history or facial recognition (Richards & King, 2014:369).

Personal Information Value Chains (PIVCs) are a method of mining Big Data, and mining data is the practice of examining large pre-existing databases in order to generate new information (Marr, 2016). Developing countries are beginning to use the power of Big Data to form personal PIVCs, which convert individuals into data subjects:

> In developing countries, governments and companies are still in the embryonic stages of harnessing the power of big data to form PIVCs in order to better service their citizens and customers respectively…. Attention is also paid to the privacy of individuals with respect to their PI in this process of creating value chains. (Nadasen, Pilkington & Da Veiga, 2016:3)

PIVCs are "raw data, resulting in valuable information, which gives a company or government organisation an advantage in fulfilling its mission"

(Nadasen, Pilkington & Da Veiga, 2016:3). Because they have the capacity to treat individuals as unique, they can lead to consumer-centric, more efficient marketing schemes (Nadasen, Pilkington & Da Veiga, 2016:1, 11). PVICs allow information to become inform-*action*, becoming a series, pattern or sequence that can generate a series of predictions about a specific individual. However, this process may be hindered by POPI (Nadasen, Pilkington & Da Veiga, 2016:3): "Customers will benefit from (the Act) as they will have more control over who processes their PI, [and] be aware of what purposes it will be is used for." For example, cold calling or unsolicited contact directed towards current or prospective clients will no longer be legal unless the individual has given consent for such contact to be made (Nadasen, Pilkington & Da Veiga, 2016:3).

It is through PIVCs that markets today precisely identify and target their individual customers. The fear is that PoPI may considerably inhibit the potential of South African businesses to use PIVCs for economic growth. This consideration must be balanced against the strong argument that legislation is needed to protect citizens' rights to their privacy and having a say in how data is used to understand and market to them.

The implications of PoPI are numerous. The legislation impacts organisational policies, employees, information technology infrastructure, third party service providers, and responsible parties that collect, process and store personal data (Swartz & Da Veiga, 2016:10-11). Swartz and Da Veiga point out the following positive changes that will be effected, focusing on how the legislation incorporates preventative measures designed to protect the consumer:

1. Preventative measures will be in place as data collectors must be transparent in disclosing their reasons for collecting information and take adequate measurements to prevent leakage;
2. Consent is ensured because the data subject must give permission for their information to be shared with third parties;
3. Individual rights will be protected as data subjects can consequently file lawsuits if their information has been interfered with against their will. (Swartz & Da Veiga, 2016:11-12)

On the other hand, a number of negative predictions have been made concerning the effects of PoPI. Firstly, market losses are anticipated as businesses become individually responsible for costs, including updating information technology systems to flag the opt-in/opt-out options of direct marketing. They are also responsible for reformatting system designs and administration processes (Swartz & Da Veiga, 2016: 12). Secondly, the cost to company infrastructure is a matter of concern to businesses as they will be challenged to meet the deadline of the 1-year grace period. Thirdly, data value chains will be impacted, undermining the previous regulatory practices of information collection that companies have relied on to target individual and potential clients and predict their needs and desires (Swartz & Da Veiga, 2016: 12). The entire system must be re-evaluated as customers are required in terms of PoPI to 'opt in'. Finally, the use of IP for marketing purposes affects how companies may legally reach out to their customer base, as customers may now opt out of all communication and advertising (South Africa. POPIA, Section 69, 2013).

1.3 Research problem

This dissertation examines how South African SMMEs understand the impact of PoPI and how they are preparing for its implementation. This study is situated in Digital

Curation as it concerns the management of information, the legislations that concern South African businesses and addresses the specific issues regarding storing, processing, and sharing this data. Swartz and Da Veiga's 2016 research discovered that 12% of SMMEs were in the process of complying with PoPI, 16% believed they were already compliant, 56% were still unaware of the conditions and therefore at risk of non-compliance by the end of the grace period, leaving 16% not compliant (2016:10). These statistics provide the basis for this study: a staggering 56% of SMMEs were unaware the conditions that they were required to meet to become compliant and therefore were at high risk of non-compliance. Although this statistic dates from 2016 and the percentage might now be somewhat lower, there is a very high probability that the situation is ongoing. The consequences of non-compliance include losing customers, pay-outs for damages or lawsuits, fines of up to R10 million, and 10 years in jail (Botha, Eloff & Swart, 2015:4-5). What is more, Section 99 (2) of PoPI lists the very limited defences "which an employer may raise against action" against the terms of the Act in order to evade responsibility and liability (Millard & Basceranco, 2016:3). The conditions of PoPI make SMMEs particularly vulnerable. Large or multinational companies are more likely to already be compliant with the international regulations that PoPI is based upon, and if this is not the case, they are much more likely than SMMEs to have adequate resources to facilitate the necessary changes.

SMMEs possess fewer financial, managerial and structural resources (Le Fleur et al., 2014:8), which make them more vulnerable to the impact of PoPI and this is why they have been chosen as the subject of this study. Certain issues brought to light through close examination of PoPI are critical for SMMEs; specifically, that the term

“responsible party” in the legislation is synonymous with the employer. As indicated above, the Act makes provision for severe consequences if businesses are non-compliant or if breaches are discovered, consequences that SMMEs will typically be unable to survive.

The study is structured around the eight principles of the Act: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.

1.4 Objectives of the study

PoPI will to some extent affect all roles within the SMME workplace. This research aims to conduct interviews using one or more companies, utilising these objectives to investigate by means of case study. This research interrogates this issue via the following questions:

1) How concerned are SMMEs with vicarious liability in the context of their specific workplace?

2) Does the SMME studied believe that it will be compliant with PoPI within the grace period?

3) Does the SMME currently have adequate resources to educate employees on new protocols; i.e. does it have the financial ability to employ suitably knowledgeable personnel, give workshops and training courses and other training tools?

1.5 Rationale for and objectives of the study

Before the advent of PoPI in South Africa, the concept of vicarious liability, borrowed from English law (Botha & Millard, 2012:227), was well established. An employer could "be held vicariously liable for delicts committed by employees", but "for an employer to be held liable… the person committing the delict must [be employed] and… have acted in the scope of [their] employment" (Botha & Millard, 2012:329-30). The definition of delict law within South African law is concerned with "the circumstances in which one person can claim compensation from another for harm that has been suffered" (Loubser et al, 2009:4). There are thus three requirements for vicarious liability to be invoked: 1) an employee / employer relationship should exist at the time when the delict is committed; 2) the employee must commit a delict, and 3) the employee must have been acting within the scope of their employment when the delict is committed (Murray, 2012:5). When deciding whether or not the actions of an employee are the fault of the employer, it must be considered whether or not the employee was acting in accordance with what is expected of them as an employee.

For example, in the case of Bezuidenhout versus Eskom it was demonstrated that the employer was not liable. An employee gave a ride to a hitchhiker and proceeded to have an accident which severely injured the passenger (*Bezuidenhout v Eskom* 2003 SA: 3-4). The judge determined that the driver had not been "acting within the scope of his employment at the time of committing the delict" (*Bezuidenhout v Eskom* 2003 SA: 5). This case is thus an example of how the concept of vicarious liability has been applied in South African case law.

Additionally, prior to PoPI, South African employers could prove that they had taken reasonably practicable action to avoid absorbing full responsibility for the actions of

employees, especially when employees may have acted against legislative terms in the context of common law, for instance, even though there were adequate measures taken on behalf of the employer to educate employees on new or revised best practices and measures (EEA, Section 60 (4) as cited in Millard & Basceranco, 2016:225). Training is important in terms of vicarious liability because, in order "to fully avoid liability, the employer must prove that the plaintiff reasonably failed to avoid all harm; otherwise, the doctrine of avoidable consequences allows imposition of liability subject only to 'mitigation' of damages … the plaintiff unreasonably failed to avoid" (Marks, 2002: 1420). Compared to other similar data protection laws around the world, PoPI's understanding of the liability of employers for the actions of employees is severe, and has been criticised by some as unreasonable.

This research investigates the significance of vicarious liability within the PoPI. Although, as indicated above, there is legal recognition of vicarious liability outside of the PoPI, this is a fundamental component within the legislation that will affect SMMEs and leave them vulnerable to potential penalties, even though they may have taken all measures possible to comply. The vicarious liability clause has caused much concern for the evolving local economies within South Africa because "PoPI specifically assigns accountability for lawful data processing to the employer (as the responsible party) and holds an employer accountable for non-compliance with PoPI" (Millard & Basceranco, 2016:9). The problem is that "employees are responsible for nearly half of all security violations and system intrusions" (Crossler et al. 2003, as cited in Vance, Lowry & Eggett, 2015:346). The data collected from the interviews identifies major concerns within the SMME workplace. It also contextualises the business's specific

approaches to these concerns and how they expect each employee to mitigate risk within the scope of individual responsibility.

1.6 Research design and methods

This research was conducted as a qualitative study, using interviews to generate a dataset to systematically analyse the perspectives of a specific SMME. Ethical clearance was obtained from UCT prior to interviewing the data subjects. Interviewees were made aware of their rights within the interview process and were asked to sign a consent form. They were made aware that they could refuse to answer any questions in the interview or withdraw from the process completely at any time. Furthermore, their personal identities as well as the names of their companies were kept confidential so as not to compromise the reputation of the individual or company. Details pertaining to the SMME which might have threatened to expose its identity were restricted or redacted and made anonymous in the record. The dataset aimed to include interviews with incumbents of specific roles, including compliance officer, human resource manager, actuary, data manager, information technology manager, employee and external compliance officer. The process aimed to gather within one SMME as much data as possible from potentially opposing perspectives regarding compliance. It intended to uncover possibly divergent views on key issues within one industry that might well be applicable to other SMMEs facing similar issues. Interviewing employees in various roles also tested how they perceived the responsibility of those working with them or under them in the hierarchy of the workplace which is a key consideration in Accountability Theory.

This research is based on Accountability Theory (AT), which helps us to understand how people make independent decisions and rationalise their actions. This is relevant

to the dissertation because the researcher is concerned with the decision-making process of the individual in the workplace. AT explains how one may need to justify decisions, judgements, and actions to someone else (Vance, Lowry & Eggett, 2015: 346). It allows for two understandings of accountability: as a virtue, and as a mechanism; as a quality that encourages someone to accept responsibility, or as a felt obligation to explain oneself and be subjected to consequences for one's actions by another person (Vance, Lowry & Eggett, 2015: 346). AT also functions as a method of assessing vicarious liability within PoPI legislation, because accountability is completely the responsibility of the employer. The data collected from the interviews also serves as a basis for discerning employees' opinions as to whether or not the Act's severe conception of responsibility is realistic, warranted, and justifiably appropriate. The interviews will also potentially provide insight into South African views about information ethics in general, apart from the PoPI legislation. Questions were designed to open a conversation about the proliferation of Western legislative views regarding PI privacy. This allowed the data subjects to comment personally on whether they thought PoPI was hurting South African industry.

1.7 Limitations

This study focuses only on PoPI compliance issues and ethics in SMMEs, targeting specific employee positions and an external compliance officer. The researcher had control over the size of the population and the scope of the topic coverage. The research was constrained by limitations of time, which permitted only one company to be investigated and a limited number of data subjects to be interviewed. SMMEs throughout the country face different challenges. For example, businesses in large city centres, such as Cape Town or Johannesburg, generally have access to more

adequate resources, staff education systems and funding, than those in smaller cities or towns. Study of the SMME in question will give feedback on its business demographic in relation to its geographic location. The research cannot therefore claim to extend beyond the scope of the data subjects to address the situations of other SMME elsewhere in the country. Although results will not be generalisable, they can still provide insight that may be useful for further research on SMMEs and PoPI compliance.

1.8 Summary

Concepts of Information Privacy (PI) in the African context are criticised for having been heavily influenced by Western ideals of ownership. The African Union Charter does not enshrine IP but rather focuses on Ubuntu ethics that contradict certain Western values upon which many pervasive technologies have been developed. PoPI aims to move South Africa towards becoming more economically competitive in the global market and protect individuals as data subjects who often do not know the best measures to protect themselves from IP and PI infringements. The Act also hopes to protect customers from the many PI infringements that are currently overlooked, and to hold employers accountable for the actions of their employees. Now that the Act has been signed into law, companies are prevented from distributing customers' PI without the customers specifically giving permission to do so.

The research questions aim to enable a close look at vicarious liability in the workplace, how seriously people take this clause and how they identify their risk. They also aim to examine how employers see PoPI's timeframe with regard to their chances of successfully and timeously implementing new best practices. Furthermore, this

study aims to assess how SMMEs view resource management and whether they are adequately prepared to implement and assess the changes.

One of the most problematic issues with the Act is that it equates “responsible party” with employer. Employers are completely liable for all actions of their employees, even if they can make a plausible case for having educated them in accordance with new best practices. This leaves employers vulnerable and risks South Africans being obliged to use the services of multinational companies as SMMEs are due to suffer great financial losses and be forced to close their doors if infringement occurs. Eloff, et al. warn that “South Africans’ personal information … processed outside South Africa by multinational organisations and through the internet … renders the information vulnerable” to the agendas of global markets (2016:2). However, in contrast to other, similar privacy acts around the world, vicarious liability makes PoPI very severe. Furthermore, employees can plausibly pursue their own interests for short-term benefit by selling sensitive information, with the limited risk of employment termination, while the company could suffer long-term potentially irreparable losses, and masses of clients’ sensitive PI could be compromised. In a general sense, this research aims to uncover what measures South African SMMEs are taking to protect their business from penalty, whether they can, and how they see themselves implementing the steps to establish new best practices. The research is based on AT so as to assess how employees are accountable for their actions as well as how employers are accountable to the legislature.

Additionally, the research questions are designed to collect broader insights regarding IP and PI in South Africa and how this legislation may prove to positively or negatively impact the local economy.

CHAPTER 2

Literature Review

2.1 Introduction

A literature review aims to give a coherent account of the existing state of knowledge regarding a topic and provide an introduction to it (Steward, 2002:495). The process involves drawing upon research collected in books, papers, journal articles, theses and other documents, to achieve a comprehensive understanding of the subject and identify various pertinent debates so as to support the specific argument made (Steward, 2002: 495). Successful literature reviews are inclusive, fully referenced, selective, relevant, synthesised, balanced, critical and analytical (Steward, 2002: 496).

This literature review was developed using the following databases and e-resources: UCT libraries, Google Scholar, Science Direct, and Cape Library Consortium (CALICO). Further information was gathered from websites and blogs. Internet database search terms included: vicarious liability, case law, PoPI, POPIA South Africa, PoPI compliance, African data compliance, African information privacy, South Africa personal information standards, data ethics, African data policy, international data policy, big data ethics, and big data management. Additionally, two UCT lecturers were consulted: Jacques Ophoff, Senior Lecturer in Information Systems in the UCT Commerce Department, who suggested some specific reading and recommended the second authority, Tobias Schonwetter, Senior Lecturer in the UCT Faculty of Law.

In accordance with the limitations and delimitations of the study, only the latest findings and research (post-2013) were considered relevant to PoPIA (PoPI). Some earlier historical information on the development of PI (Personal Information) and IP (Information Privacy) was also considered relevant and therefore included.

This chapter is divided into 5 sections, including a summary and introduction. After the introduction, the first section discusses the ways in which Accountability Theory (AT) can be applied to understand issues relating to the implementation of new policies in the data-access workplace. The second part discusses the theoretical framework of the research, privacy ethics and personal information as well as anonymity and the right to be forgotten. It also touches upon the historical development of IP tactics and theory in Africa and globally, and considers cultural issues and consequences as well as issues with legislative compliance. The third section develops an understanding of PoPI implementation by South African SMMEs and also discusses vicarious liability and potentially useful compliance measures. The final sections predict the future of information privacy in Africa and summarise the literature review. This includes similar studies; their scope, theory, methodology and findings.

2.2 Accountability theory and access policies

Accountability theory (AT) hinges on the perceived need to justify one's behaviour to another person or party because one feels accountable for one's decision-making processes and judgements used in this process (Vance, Lowry, & Eggett, 2015: 347). Vance, Lowry and Eggett propose four core components of AT: identifiability within a group or workplace, expectation of evaluation, awareness of monitoring, and social presence. Identifiability in the context of the workplace "is a person's 'knowledge that

his outputs could be linked to him' and thus reveal his/her true identity" (Williams et al., 1981:309, as quoted in Vance, Lowry & Eggett, 2015). This kind of surveillance is also at play in the context of large-scale Big Data, which leads people to attempt to hide their identity and therefore their connection with data output, such as search histories. In the workplace, identifiability aids accountability, as it deters anti-social behaviour and making decisions contrary to the established code of conduct or procedures. These might be implemented through server logs, applications that require specific logins, or record digital signatures upon access.

Expectation of evaluation is the belief that one's performance will be assessed by someone else who will make sure their actions are in accordance with the rules; this also increases socially desirable behaviour and discourages rule-breaking (Vance, Lowry & Eggett, 2015:349). Expectation of evaluation is probably already in place in some SMMEs and companies that deal with sensitive data. It would be beneficial to use evaluation-based web logs, transaction auditing, real-time reports of access logs, and visual dashboards for user activities to monitor implementation of PoPI. These could be used to track the progress toward key results regarding performance in adhering to new procedures alongside key performance indicators within each business. The work of Frink and Klimoski (2004) examines the phenomenon of accountability in matters relating to human resource management, which is quite relevant to applying new PoPI procedures in SMMEs. Their analysis covers a spectrum of perspectives on accountability theory in practice (Frink & Klimoski, 2004:1). They point out how accountability may lead to undesirable actions within the workplace such as breeding cynicism because the person held responsible may not have control over all variables, but can also be used to predict the behaviours of

individuals, which can be beneficial in a multi-level organisation (Frink & Klimoski, 2004: 11-12). Predicting behaviours might be used to understand how employees might approach compliance to PoPI or give insight as to how to mitigate or prepare for different kinds of employee reactions.

They delve further into the psychology of accountability, which works well for A-Type personalities, who intrinsically self-monitor. But human resource managers must recalibrate their expectations and approaches to suit a variety of employee personalities (Frink & Klimoski, 2004:12). Tetlock et al. explain that it is rare that workplaces can attribute either process or outcome forms of accountability with complete confidence: “Under pure process accountability, employees expect to justify efforts and strategies to generate results. The focus is on inputs, not outcomes” (Tetlock et al., 2013: 22). The outcome form of accountability expects employees to deliver end results without explaining how they got there. Both have their strengths and weaknesses, and Tetlock et al. (2013) conclude their case studies of workplaces by observing that managers rely on ideologies of accountability and exaggerate its actual power (Tetlock et al., 2013:33). Whichever accountability system a manager decides to use exposes their workplace and results in a certain set of risks which they should be prepared to navigate, specifically when sharing private information.

Working with sensitive data gives rise to numerous issues and complexities in management. This is one of the most common human relations issues, as humans are subject to error and can accidentally, or purposefully, divulge sensitive information for personal gain. The challenge is to secure processing procedures between employee and processing system. Ann Cavoukian and Jeff Jonas suggest guidelines

that reflect how PoPI explicates best practices for handling sensitive information. Their recommendations include the following:

1) that personally identifiable information should be collected only when the use of it and its limitations are specified before collection;

2) the use of PI should be explicitly explained to the individual and not violate its use as authorised by law;

3) transparency of participation should empower individuals to play a significant "role in the lifecycle of their own personal data"; and

4) there are adequate safeguards to protect the integrity of the information (Cavoukian & Jonas, 2012:7-8).

To resist the threats to privacy posed by technologies such as those employing location-based services, privacy by design (PbD) has come to revolutionise how systems operationally collect information (Cavoukian & Jonas, 2012:9). Cavoukian and Jonas consider the following measures as crucial to transforming data operations. In some cases, these principles will be contrasted with PoPI clauses.

1) Full attribution: this means that every record's source should be evident, and its metadata (the set of data that gives information about other data) must ensure it can be traceable. This allows for easy transfer and reconciliation of data.

2) Data tethering: additions, changes, and dates must be recorded in real time.

3) Analytics on anonymised data (encrypted data or data that has personally identifiable information removed to protect privacy): performing advanced analytics over cryptographically altered data (protects data from theft or alteration) means organisations can anonymise more data before sharing. Every copy of data increases the risk of unintended disclosure, so it should be anonymised before transfer and anonymised upon receipt.

4) Tamper-resistant (this means no one can change the data) audit logs: every user search should be logged in a tamper-resistant manner, which means they cannot be changed, thus decreasing the possibility of policy violations.

5) False negative favouring methods: capability to strongly favour false negatives is critically important in systems that could affect civil liberties. It is usually favourable to miss a few details (false negatives) than to inadvertently make claims that are not true (false positives), as sometimes a single part of data can lead to multiple conclusions. Section 103 (a) of PoPI states that failure to comply includes a situation wherein the company "makes a statement knowing it to be false" (PoPI, 2013:97). If the employee or compliance officer fails to interrogate statements or data, this negligence can be read as overlooking potentially crucial and misleading information.

6) Self-correcting false positives (a data system that can correct itself from presenting misleading results): every new data point presented prior to assertions is re-evaluated to ensure that it is still correct and if not, repaired in real time. This should be a compulsory feature within data sets to make sure the information is as accurate as possible. As stated in Section 103 (b) of PoPI, a company that "recklessly makes a statement which is false, in a material respect, is guilty of an offense" (PoPI, 2013: 98)

7) Information transfer accounting (this accounts for how and where information is shared) monitors information flows, and ideally displays who is responsible for opening data and its movement. This makes it easier to find those responsible for data leaks. (Cavoukian & Jonas, 2012:10-12).

Such methods aim to ensure the tightest monitoring to both guarantee accountability in data management by employees and establish protocol for data to correct itself

when new data is introduced into the system. These elements are quite similar if not identical to PoPI's outline of how sensitive data should be handled.

2.3 Research relevance and similar studies

Compliance has not been studied within the framework of the PoPI; no academic work was found after thorough research. One of the most relevant sources found was the 2014 work of UCT master's student Charles Hinde in the Department of Information Systems, who proposed a model to assess organisational IP matters in relation to PoPI. Hinde specified areas wherein information was likely to be compromised in the workplace, resulting in losses and liability for employers, while also proposing methods for organisations to evaluate their IP maturity – which can be understood as how internal IP systems develop and how successful they are (Hinde, 2014:9-10). Hinde's work includes a broad definition of privacy and discusses what PoPI means for South African organisations, but it differs fundamentally from this study in that its aim is to create a functional tool with a user-friendly interface (2014:14), a data organisation tool to protect businesses and organisations. This study is focussed more upon the resources to which SMMEs have access at the present time. There is no current research specifically devoted to SMMEs and compliance issues.

Millard and Bascerano (2016) write in depth about vicarious liability for employers in many of the contexts affected by PoPI, but their work does not deal directly with personal information. It is concerned rather with South African case law and instances in which the notion of vicarious liability was critical. The current study is therefore important because it offers some insight into crucial issues that employers must face and deal with in the face of PoPI: for example, managing the risks of vicarious liability in the workplace while ensuring that employees follow new regulations. It should be

noted that there are as yet no other case studies that address vicarious liability and PoPI because the Act had not yet come into effect at the time that this research commenced.

Other studies that consider privacy compliance issues include the work of Borena, Belanger, and Ejigu (2015), who examine how Africa at large attempts to protect itself from the vulnerabilities of the internet world, acknowledging its vulnerability to external factors due to limited skill sets and technology. They use critical social theory to determine how the right to privacy might be implemented (Borena, Belanger and Ejigu, 2015:3491). The study is relevant because it addresses issues that are pervasive on the continent and highlights government efforts to address them. However, they only consider privacy issues at the macro level, and their work does not explore the implementation of PoPI specifically.

Nadasen, Pilkington and Da Veiga's work regarding information flows in South Africa investigates what PoPI means for South Africa in comparison with other international privacy laws, exploring how the Act impacts value chains, specifically for the insurance industry (Nadasen, Pilkington & Da Veiga, 2016:1). They determine where South African insurance companies are defective "in the areas of privacy and personal information value chains", and highlight where a lack of privacy is still evident in respect of individuals' personal information (Nadasen, Pilkington & Da Veiga, 2016:11).

Other relevant studies that are made use of include the work of Botha, Eloff and Swart (2015), who discuss PoPI in the context of evaluating online resources and

implementing the legislation. Botha, Eloff & Swart (2015) describe how PoPI will affect small and medium enterprises in South Africa but do not consider micro-enterprises. Their research discusses how the legislation may affect marketing and growth, a question they address using an online survey (Botha, Eloff & Swart, 2015:1). The questions asked determined if the enterprise responding qualified as a Small or Medium Enterprise, gathered information about how much they understood about PoPI, then investigated where the specific enterprise was in the process of complying with the legislation (Botha, Eloff & Swart, 2015:1-2). Their last question "determined the feeling of [these businesses] towards the PoPI Act and how [they understood] how it would affect their business once fully implemented" (Botha, Eloff & Swart, 2015:2). Their paper focussed on proactive marketing, while this research is more concerned with how organisations understand the matter of protecting themselves from vicarious liability. If organisations cannot protect themselves or do not know how to, marketing is the least of their worries.

Finally, the work of Skolmen and Gerber (2015) discusses how cloud computing as an option for South African organisations deals with various factors regarding security. The study considers PoPI as an ideal opportunity to address information security-related concerns and prepare the way for potential cloud users and providers, while re-examining how the cloud typically regulates, stores and secures information (Skolmen & Gerber, 2015: 1). It proposes a framework for how cloud adoption might be regarded as the best way of approaching compliance with PoPI and become the most widely-adopted method of information processing and storage. However, their work doesn't touch upon HR issues and how employees will tackle information processing without this technological framework. What it does do is develop an

understanding of how the PoPI Act and the IT establishment understand compliance with the legislation, and how the two might find a way to develop and maintain a symbiotic relationship if built on trust and while promoting national adoption of the cloud computing method (Skolmen & Gerber, 2015:9). This study is important because it posits a solution to complex compliance issues while using existing technologies that may prove to be useful for many South African companies, should the Act and the cloud framework be able to negotiate reciprocal demands. While this may be a solution for some businesses, it does not seem like a practical solution for smaller companies, nor does it address micro-enterprises specifically. Furthermore, it does not recognise how adoption of this framework might be problematic.

2.3.1 Contextual framework of privacy

This section details the theories and historical developments that have fed into and led up to PoPI and this research. It gives an account of the worldwide progressive understanding and acceptance of privacy and personal information as having significant political meaning in the context of individual rights.

2.3.2 What is privacy?

Privacy would seem too broad a concept to fit into a simple definition: it is not sufficient to define it in terms of the protection or control of biometric, financial, and social information. The world appears currently to be in something of a crisis about privacy: every day there are headlines using emotive trigger language such as “warning”, “security breach”, “tracking”, “violation”, and “threatened”. Defining privacy is a constant struggle. American legal scholar Lillian BeVier writes, “privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate

interests… [used] to generate goodwill on behalf of whatever interest is being asserted in its name". Others understand privacy as "protean", or suffering "an embarrassment of meanings" (BeVier, Gerety & Scheppele, cited by Solove, 2009:7). In a South African context, the right to privacy is technically protected in terms of common law and within the Constitution (Hinde & Ophoff, 2014:3). "However, the right to privacy is not absolute and consideration is given to competing interests such as maintaining law and order, protecting commercial interests, and the administration of national social programs" (Hinde & Ophoff, 2014:3). The definition of privacy seems to change depending on the context and whom it is working for, which is problematic for several reasons, but mainly because it can justify invading the privacy of others. Furthermore, if the meaning of privacy can be constructed through fine print and legislation, anyone can form their own idea of what is entailed by privacy to protect business interests. The objective of PoPI is to bring some order to this situation in the public domain and "regulate the processing of PI by public and private bodies while working with international standards" (Hinde & Ophoff, 2014: 3).

The right to privacy should be recognised as having both negative and positive connotations in the context of a well-balanced society. It allows individuals to be free *from* exposures that threaten safety and be free *to* protect all kinds of personal information, while it defends individuals from unwarranted policing on various levels, on- and offline. Here Isaiah Berlin's "Two Concepts of Liberty," positive and negative freedom (Berlin, 1969), can be invoked. Freedom-*to* and freedom-*from* are co-dependent variables designed to offer the most benefit to the citizen. Positive freedom "is involved in the answer to the question 'What, or who, is the source of control or interference that can determine someone to do, or be, this rather than that?' The two

questions are clearly different, even though the answers to them may overlap" (Berlin, 1969: 122). Berlin explains that the freedom to do something is a matter of measuring the absence of interference in the process of acting independently on free will. Meanwhile “liberty in the negative sense involves an answer to the question: 'What is the area within which the subject — a person or group of persons — is or should be left to do or be what he is able to do or be, without interference by other persons’” (Berlin, 1969: 122). Negative freedom considers how that interference takes place and to what end. Berlin’s distinction offers a clear conceptual understanding of how privacy and corresponding legislation may be conceived. However, it is not particularly useful to understand privacy in the abstract; instead it should “be worked out contextually” and accepted as a collection “of many distinct yet related things”. There must also “widespread applicability” in the way it is managed (Solove, 2009:40, 41).

2.3.3 The development of privacy ethics and personal information protections

As a Western concept, the right to privacy developed from early philosophical foundations such as Aristotle’s distinction between the two spheres of life: the *polis*, political life, and *oikos*, domestic life (Roy, 1999:4). This distinction is also recognised as the difference between the sphere in which the government regulates life and that in which life is self-regulated, as explained in John Stuart Mill’s essay ’On Liberty’ *(*DeCew, 2002). The earliest recorded legislation concerning privacy was the English Justices and Peace Act of 1361, which threatened consequences against eavesdroppers and Peeping Toms (cited in Hinde, 2014:15) The earliest acknowledgement of the concept of IP in a modern legal context was *The Right to Privacy* by Samuel Warren and Louis Brandeis in 1890, which emphasised “the right to be let alone” and understood the right to privacy as being based on the “general

right of immunity of the person" (DeCew, 2002). The concept of privacy protections was further developed in the Fourth Amendment of the United States Constitution, which entrenches privacy protection in the United States, and understands privacy as "control over information about oneself [including protection] against unwarranted searches, eavesdropping, surveillance, and appropriation and misuses of one's communications" (DeCew, 2002). The Fifth Amendment is also important in this context as it "affords individuals a privilege against being compelled to testify about incriminating information" (Solove, 2004:188).

The notion of privacy enshrined in the US Constitution and advanced by Warren and Brandeis has in recent decades expanded to the domain of digital life behaviours. Collecting personal information about all online behaviours can make way for third parties to create a personal narrative that may influence individual experience offline. Contemporary violations of privacy tend to subject individuals to mental pain and distress rather than physical pain (Solove, 2006:477). An example of this is the anxiety-inducing phenomenon of doxing, publishing personal information about an individual on the internet with malicious intent (*Merriam-Webster Dictionary*).

Foucault conceives a power that involves constraint and enablement: "who has influence versus who has authority is a critical distinction" (as cited in Domanski, 2015:7). There has been a direct correlation between the evolution and increasing influence of mass media and concern for the privacy of personal life for citizens in both Europe and North America (Mantelero, 2013:2). There are significant differences between European and US standards of privacy, although they share similar sentiments toward protecting liberal values such as freedom of speech. The most

notable development from the EU was the right to be forgotten, implemented by the Directive of 95/46/EC, originating from *droit à l'oubli* that succeeded in forbidding the press and TV from making personal life public (Mantelero, 2013:1). A similar sentiment appeared later in US law, as the "right to pursue and obtain happiness" under which every individual has "the right to live free from the unwarranted attack of others upon one's liberty, property, and reputation" (*Melvin v. Reid*, 1940:91).

One of the most recent developments in internet privacy legislation has emerged from the Trump administration in the United States. The president repealed internet privacy rules that were passed by the Federal Communications Commission under the Obama Administration (Neidig, 2017). Although the Fourth Amendment in the US constitution prohibits unreasonable searches and seisures without a warrant of probable cause, US privacy legislation has differed from many other developed nations' protective data policies because when Americans "leave the home – virtually or physically – the right to privacy dissipates" (Sullivan, 2006). The patchwork of legislation in the US has been anything but all-encompassing (Sullivan, 2006). The Trump-era rules are set to overturn the Obama-era privacy regulations that require broadband providers to obtain explicit consent from an opt-in signal before selling customers' web-browsing data, app-usage data and other personal information that advertisers and third parties might want access to (Dunn, 2017). Such sensitive information includes geolocation, and financial and health data. The result of such legislation is a more open market for user data, especially for those companies who are aiming to become more present online in the context of the near-monopolies of Google and Facebook.

Internationally, privacy was recognised as a human right in the United Nations Declaration of Human Rights in 1948: “No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation” (United Nations Declaration of Human Rights, Article 12). Numerous privacy laws around the world, including multinational privacy guidelines, directives, and frameworks have subsequently influenced how information moves across borders and oceans (Solove, 2009:3). In 1980, the Organisation for Economic Cooperation and Development created Privacy Guidelines, followed by the EU’s Directive on Data Protection in 1995. Protection policies emerged in many of the most powerful nations worldwide, including Canada’s Personal Information Protection and Electronic Documents Act of 2000, Japan’s Personal Protection Law of 2003, and Argentina’s Law for the Protection of Personal Data in 2000 (Solove, 2009: 3).

In South Africa, citizens have been “protected by the common-law principles of the law of delict”, and essentially any “delict would be ‘an intentional and wrongful interference with another’s right to seclusion [within their] private life’” (Millard & Basceranco, 2016:6). Prior to PoPI, “scholars [believed] information privacy was a sub-category of the right to privacy”; it was unclear what was worthy of being protected and which information about a person might be considered private (Millard & Basceranco, 2016:6).

2.3.4 Privacy in the age of the internet

The internet is an interface in which much personal information is disclosed by individuals signing up for goods, services, and quotes from companies that measure personal information factors and consider them as significant variables. In the context

of the internet, policymaking decisions often have political consequences, and therefore changes to privacy regulations online are political actions in themselves (Domanski, 2015:14). Domanski explains that the internet is dictated by a series of "single controlling points" where internet users' behaviour is controlled or constrained (2015:8). The singular reputation of an individual online has a lasting effect in real life. On a basic level, employers regularly make use of the widespread willingness of many to divulge a plethora of personal life details online. It is common practice to mine data about potential employees online through social media and other popular search engines that might uncover questionable histories. However, these are arguably superficial investigations, to the extent that they uncover what an individual willingly divulges to a specific audience.

Meanwhile, algorithms developed by internet-user search histories create profiles for marketing-related products and services attuned to their preferences and behaviours. There are measures internet users can take to prevent this kind of data collection, including specific browser add-ons for private surfing, and opting out of certain settings that are normally enabled. Other digital services on smartphones and tablets can provide even more information, amounting to a "digital dossier" on individuals (Solove, 2009:119). The ways in which people can be monitored are becoming more numerous, especially with location-based services. In their podcast, Zomorodi and Donohue explain even offline technologies of retail genius track shoppers' movements in shopping malls, collate individuals' data before they get into a specific store, calculate how much they are likely to spend, how much time they are likely to spend at that location, and know each shopper's income (Zomorodi & Donohue, 2017).

Furthermore, according to Frick and O'Neill's podcast, there tends to be too much trust on the part of users of algorithms, and developers must be audited by an unbiased third party for fairness and legality (Frick & O'Neill, 2016). Often the defined success of using these algorithms is machine-learned and filters out women and minorities because they were not "successful" according to past datasets (Frick & O'Neill, 2016). Instead the algorithm applies previously unfair and currently incorrect biases, and bad data equals biased results. People are largely unaware of these scoring systems, and moreover they are unable to find their scores or change them. Simple demographic data may lead to discriminating assumptions about an individual, such as a postal code, which is a social determinant in many societies (Frick & O'Neill, 2016). Situations that involve HR and employment are certainly affected by this kind of data, but more concerning is the reality that these statistics may unfairly indicate an individual's predisposition to criminal activity and predict their illegal activities. A more positive outlook is to recognise that once these algorithms are calibrated fairly, they will be able to do their job extremely well (Frick & O'Neill, 2016).

Information held by a third party is not protected by the collectors of this information (Richards & King, 2014:396). As Richards and King explain, "Big data predictions and interferences risk compromising identity by allowing institutional surveillance to identify, categorise, modulate, and even determine who we are before we make up our own minds" (2014:396). Furthermore, the more the data is analysed the greater is the potential for its suggestions about an individual's behaviour to be wrong, owing to the accumulation of false positives; anonymisation becomes increasingly difficult because advanced data combinations reveal identities (Cumbley & Church, 2013:604). For example, RFID devices and biometrically enabled CCTV enable

tracking. “Law enforcement monitors traffic upstream” using search terms across internet servers to find subject terms that might lead to criminal activity, thus using general warrants for investigation. This was what the Fourth Amendment to the US Constitution intended to prohibit (Zomorodi & Donohue, 2017) and demonstrates how weaker standards in national security are allowing individuals’ information to be taken out of context (Zomorodi & Donohue, 2017). On the other hand, the internet is undeniably a culture-changing development because of its adhocratic (flexible, adaptable, unofficial organisation, lacking formal structure) nature and its ability to “cut across normal bureaucratic lines, to capture opportunities, solve problems, and get results” (Domanski, 2015:7).

2.3.1. Defining compliance

Compliance is defined as the state or fact of according with or meeting rules or standards (*Oxford English Dictionary*). PoPI compliance is based on a series of principles embedded within the legislation, specifically: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. These principles will be imposed on company data structures. Significant changes to existing business processes will have to be enacted with regard to how the company approaches personal data; it cannot make assumptions based on information about a client, but must inquire if, how and when the client or perspective client wishes to be contacted (Swartz & Da Veiga, 2016: 12). Furthermore, the new “opt-in” system, which requires that individuals be asked for permission for their data to be shared with sources other than the primary, must consider client approaches based on the information they are willing to give. The benefit in terms of consumer protection is clear as PoPI allows for much more individual control over personal data (Eloff, 2018).

2.4 Implementation on the African continent

The early constitutions of countries on the African continent often featured a European-based Bill of Rights even though there were little technological advances to warrant consciousness of privacy issues (Makulilo, 2015:79). Legislation regarding privacy has developed slowly through courts in South Africa and Kenya, whose constitutions include similar sections that protect individuals from having their homes searched without a warrant, or having their property seized or their communications trespassed upon (Makulilo, 2015:80). Other privacy policies have developed through sectoral legislation with ad hoc privacy protection provisions (Makulilo, 2015:80). Further laws have been enacted in the context of globally impacting events, including large-scale terrorist activities like the September 11th attacks in the United States and various incidences of terrorism in Europe. These have triggered an acute awareness of vulnerability and resulted in laws being created to intercept and monitor private communications (Makulilo, 2015: 80). In South Africa, the Constitution also protects a person's right to decide what he or she discloses to the public, and protects individual interests or autonomy; however, it does "not at present reflect the basic principles of data protection" (Makulilo, 2015: 80).

African data policies evolved in the 2000s, under the direct influence of the EU Data Protection Directive 95/46/EC. Botha, Eloff and Swart's comparison of South Africa's PoPI and other similar legislation demonstrates the attempt by the legislature to adapt and adopt similar policies from elsewhere. Botha, Eloff and Swart's work offers a close examination of how this legislation differs and why. PoPI was inspired by the EU's Data Protection Directive and other models of privacy from the United States, Canada, Australia, and the UK (Botha, Eloff & Swart, 2016:3). By 2015, sixteen African

countries had enacted data protection legislation: Angola, Benin, Burkina Faso, Cape Verde, Comoros, Gabon, Ghana, Ivory Coast, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, and Tunisia (Fichet, 2015). Another 14 countries have bills or rumoured bills in the pipeline (Botha et al, 2016: 5).

2.5 Vicarious liability and potential compliance measures under PoPI implementation

Arguably, the biggest issue with this legislation is the holding of employers accountable for the acts of employees. PoPI specifically assigns obligation for lawful data processing to the "responsible party", a phrase synonymous with employer; furthermore, the responsible party is entirely responsible for correctly processing that data (Millard & Basceranco, 2016: 9). Holding employers accountable is certainly a great incentive for companies to educate and administer the relevant changes and ensure that those responsible are aware of new best practices. On the other hand, it does not reckon with employees pursuing their own interests. While an employee in breach may have their employment terminated, they may not be held individually responsible for their actions. There is no room for reasonable practicable measures for the employer to prove that they have taken measures to prevent innapropriate use of information under this legislation (EEA, Section 60 (4), as cited in Millard & Basceranco, 2016:225).

The vicarious liability clause also runs the risk of consolidating the power and resources of multinational companies, which have significantly greater access to resources, financial and otherwise. The risk of vicarious liability is that it magnifies these differences, leaving SMME's even more vulnerable to competition with companies that often already comply with legislation elsewhere upon which PoPI is based, such as European legislations. An extreme view would see these risks as

potentially leading to a largely outsourced South Africa, where local companies cannot compete and cater to the specificities, complications, and sensitivities of the South African customer experience. Prioritising the local economy has an important patriotic motive, to protect home-grown businesses and ensure that they have the potential to eventually compete in the national or international context.

2.6 Summary

Implementing new privacy strategies comes with many challenges, especially when the legislation stipulates severe penalties for non-compliance. These challenges are not only budgetary, but also pertain to human resources because of vicarious liability. The problem with vicarious liability is that it does not recognise that employees, regardless of technological training, may consciously decide to go against the new best practices for their own personal gain. Many approaches to foster new best practices within SMME operations involve educating staff members, employing or hiring a third party as a compliance officer, and considering the possibility of surveillance within the workplace as a precautionary measure.

Accountability theory has many facets, as demonstrated in this chapter. In the light of PoPI, managers and human relations personnel must scrutinise the employees they have, as well as what results they desire from the work of these employees. Sometimes the goals and the personality types of these employees may contradict the kind of accountability a manager wants to invoke in the workplace. The manager or human relations personnel must be aware or these risks and be prepared to navigate them effectively.

As suggested in Chapter 1, the understanding of privacy in the African context is different from that in the West, but modernising African countries are increasingly adopting Western-inspired PI legislation. In common with these countries, the rights of individuals in South African communities are not uniform: there are still many who are disadvantaged and lack the resources and knowledge to adopt new technologies, or to use them with caution.

Among the risks engendered by the inception of PoPI is that local, home-grown smaller businesses will not be able to compete in terms of compliant data management with their international competitors.

CHAPTER 3

Research Methods

3.1 Introduction

Accountability theory (AT) has been applied as a framework for this research because it considers the complexity of working relationships between employee and employer, especially in the current context. AT is defined by Vance et al. as a need to justify one's behaviour to another party and thus feel accountable for decision-making processes and judgements (2015:345). This was greatly considered when drafting interview questions because the questions aimed to understand individual's understanding of their own responsibility within the workplace. Thematically AT was taken into account in the analysis stage of the research. AT suggests that active participation in changing standard operating procedures is critical for both the employer and employee. In the context of AT, the workplace hierarchy makes for an environment that fosters people's feeling accountable for their actions, for instance, having to explain why certain decisions were made (Vance, Lowry & Eggett, 2015:345). Therefore, in the ideal context of PoPI compliance in the workplace, an employee who is collecting personal data should have input into the procedures that define this operation. AT is a facet of management that employers should be made aware of because many employees' digital user interfaces can enable privacy breaches and access-privacy violations (Vance, Lowry & Eggett, 2015:345). It is often difficult to monitor all employees' activities in respect of clients' personal data (Vance, Lowry & Eggett, 2015:346), as efforts to do so may entail constraints on workflows and prove to be costly. In sum, AT can be used to assess the effectiveness of

technological implementation within the workplace by making use of certain control and monitoring methods as explained above.

3.2 Research design

This research involved a qualitative case study approach. Qualitative research goes beyond describing a sample in terms of numbers and figures to consider also observations, descriptions, and accounts of study subjects (Anyan, 2013:1). The qualitative method aims to discover the complexity behind occurrences by delving into the relevant personal experiences of the research population.

A case study can involve data sources such as documentation, archival records, interviews, physical artefacts, direct observations, and participant observation (Kvale, 1994:147). Often, “case study” and “qualitative study” are used interchangeably, but case studies can also involve only quantitative data. Case methodology focuses on understanding the dynamics within a specific setting (Eisenhardt, 1989:534). The case study research method allows the researcher to explore a specific subject in depth and interpret the collected data flexibly (Stake, 1978:7). Gathering valid data samples for this research method enables the researcher to create meaning from even small samples. As a research method it differs greatly from quantitative studies, which often demand large samples (or at least significantly larger than qualitative studies) (Eisenhardt, 1989:536). Given the scale, the data collected in a case study can be influenced by the variable of personal observation and the biases that come with it (Stake, 1978:7). Case studies may proverbially “miss the big picture” if they focus too narrowly on a specific variable. If the researcher relies too much on archival research and previous studies, s/he runs the risk of imitating similar previously completed research on the same subject. AT is used in this case study to apply a wider

investigation into human behavioural management within the workplace in efforts to curtail the larger, more serious consequences of non-compliance to PoPI.

3.3 Population and sampling

A population sample is defined as a selected number of participants who are deemed adequately to represent the issues that affect the population at large. An adequate case sample can be understood to represent the issues at large, while not generalising the experience of individuals within the population (Stake, 1978:1). One of the benefits of qualitative research is that the sample itself can be relatively small and still yield a rich dataset. The researcher acknowledges that this method would have to have been applied to a much larger sample to provide really trustworthy and meaningful data. Nevertheless, the interviews provided some rich information that reflected the complexity of the issue at hand.

The research population in this study comprised all SMMEs in South Africa. For the sake of convenience, this study identified companies within one of the predominant metropolises in the country: Cape Town. The purpose was to reach individuals in specific positions related to compliance, if and where these existed. The purposively selected sample comprised 6 people in relevant positions, who were interviewed for their views on the issues at hand. The sample was selected by reaching out to contacts in the business of aiding companies and businesses with PoPI compliance. Larger consultancy companies did not prove to be helpful, but individual consultants successfully connected the researcher with willing participants who fit the desired sample requirements.The researcher explained their specific interest in SMMEs, and was then directed towards this specific home owner's association. This association fit the mould as South African SMMEs are defined by the Wholesale and Retail Sector

Education and Training Authority as employing between < 20 (micro) and 100-200 people (Le Fleur et al, 2014:8). The final interviewee sample differed from the intended sample in that it was smaller and did not include an external PoPI compliance person.

3.4 Research instruments

Research instruments were carefully designed to collect the data needed within the study. Research of this kind typically involves methods such as interviews, observations, and archival investigations (Eisenhardt, 1989: 537). These instruments needed to be created in a way that avoided bias as much as possible and delivered results that could be used to answer the research questions. This research study used face-to-face interviews, telephone interviews, and e-mail correspondence. The interview schedule (Appendix B) was designed to measure the understanding of POPI within the workplace and determine how each employee understood personal responsibility under this legislation. The research instrument was also designed to investigate how accountability was understood within the specific workplace by interrogating the hierarchical structure and the interviewee's place within it. The interview questions can be found at Appendix B. The research questions were influenced by AT in that they attempted to measure how individual's perceived personal responsibility to changing workplace protocol. The questions were also influenced by the research as they aimed to investigate the depth to which the interviewees were aware of the PoPI Act and what it meant for the business at large.

3.4.1 Interview correspondence

Prior to the interviews, the interview questions were reviewed by the UCT Research Ethics Committee. During the approval process, the researcher searched for an

organisation or organisations that would be open to answering these questions. The search for these companies began prior to receiving feedback on the interview questions. The researcher had to reach out to several organisations before finding any that were open to having their staff contacted for this purpose.

Face-to-face and telephonic interviews aimed to be conversational yet guided by a series of questions distributed to the interviewees prior to the interview. Strictly casual or non-structured interviews may lead to difficulty when it comes to data analysis (Turner, 2010:755). The interview questions were nevertheless open-ended, to gather as much information as possible. They allowed participants to fully explain their personal experiences and views on a subject (Turner, 2010: 755). The interviews were recorded, notes were taken, and a candid approach was adopted so as to foster an open atmosphere and encourage the sharing of as much information as possible. After the interviews, the data gathered was analysed.

3.5 Validity and reliability

The validity of case studies is determined by the researcher's success in writing a clear research question, designing the research method appropriately, appropriately sampling the research population, systematically managing the collected data and analysing it effectively (Baxter & Jack, 2008:556). Reliability generally relates to how accurate the researcher's instrument is, and the extent to which it renders the results of the experiment or case study repeatable (Golafshani, 2003:599). However, the subjective nature of qualitative research can make this conceptualisation of reliability problematic. Instead, reliability can be supported by the researcher's "purpose of explaining" and "generating understanding" from the material gathered (Golafshani, 2003:601). Stenbacka (2001:552) suggests that "the concept of reliability [in

qualitative research] is misleading", and should a qualitative study be deemed reliable when measured by standard means, "the consequence is rather that the study is no good".

Among the criticisms of qualitative interviews as the data-gathering instrument in a research study is the view that inherently the interviewee and interviewer can never be considered as possessing equal power (Kvale, 1996:1). Interviews are also criticised as not being a 'scientific method', but in fact the interview method's validity, or worth for research purposes, is determined by the specific discipline and purpose for which it is being employed (Kvale, 1994:150).

Qualitative data can be used to understand an applied theory in depth and within the context of the sampled population; it may also be able to suggest a theory which can then be strengthened by this kind of research (Eisenhardt, 1989:538). Often novice research falls short because the findings are not related back to the issue at large and instead focus only on its "granularity" or specificity (Baxter & Jack, 2008: 550). This kind of research can also make serendipitous discoveries and enable drastic leaps into the theoretical, enabling the researcher to avoid narrow or biased findings (Miles, 1979:592). In Chapter 5 the researcher will consider the outcomes of the data analysis in light of the issues raised in Chapter 2 to contextualise the findings in a broader context to avoid Baxter and Jack's warning about granular qualitative data analysis.

The practicality of the single case study must also be considered when assessing the utility of the project's capacity. The intention was that interviews would not necessarily be limited to one organisation, because the scope of the research would then be

confined to a small sample. However, the sample did result in interviewing within only one organisation. This means that the results were clearly limited when compared to more expansive research. Qualitative research is often criticised because its findings do not yield generalisable results – because there are too few subjects, the instruments are too person-dependent, are only explorative, rest upon leading questions, are subjective, and ultimately rely upon the interpretation of the interviewer (Kvale, 1994:147-48). The conceptualisation of such projects often exhibits a palpable tension, to the extent that the researcher wants to have clarity and focus while still coming to gather data without harbouring assumptions (Miles, 1979:591). The present study made efforts to avoid these pitfalls, since the interviews were designed with these criticisms in mind by leaving questions open-ended and allowing for the interviews to be more conversational than interrogative.

3.6 Ethics

The research deals with human subjects and companies, so it was important that interviewees and their organisations remained anonymous. Anonymity has become conflated with confidentiality, which defines what information is hidden from everyone but the researcher (Saunders, Kitzinger & Kitzinger, 2015:618). Although research of this nature does not always ensure confidentiality, the researcher committed herself to the full anonymisation of the data for analysis and for dataset publishing, according to standard practice. When the dataset is detailed in Chapter 4, the employee's position will be specified, but their name will not be revealed. Likewise, a summary of the kind of company used for this case study was provided, but nothing that might clearly identify the organisation, such as its location or the service it provideds. This was made clear in the statement that was given (Appendix A), before the interview, and which the interviewee was asked to sign. This statement clarified the intention of

the interviews and detailed the study and general scope of the research. Interviewees were free to act in any way or make any decision that might affect the progress of data collection (such as withdrawing altogether). The statement can be found in Appendix A.

3.7 Data collection

Data was collected through interviews, by telephone, email, or face-to-face meetings. The interviews were concentrated on one specific business entity and were held subject to their staff's availability; there researcher did not divulge what one interviewee had said in their interview to another to interviewee to seek potentially missing information. Interviews were recorded with the participants' signed consent and transcribed afterwards. Meetings were organised with interviewees according to their personal availability, within or outside of business hours at a location of their choice.

The interviewees were employed by a small homeowner's association. This association was considered a SMME because it employed under 20 people and had an annual revenue of under R150 000 (categorisation according to Le Fleur et al., 2014:8). The interview pool was smaller than the researcher (or research design) had anticipated, but those available were occupied positions that were relevant to the study. The limited number of participants certainly affects the research's impact because it is smaller in scope and yielded less data, but relevant information was still gathered. These interviews were conducted between October 17th, 2017 and November 1st, 2017. The researcher contacted the head operating officer (HOO) to gauge openness to participation in the study. The data from the interviews was initially examined vertically so as to record the content of each sample clearly. Secondly, a

cross-interview analysis was applied to demonstrate how the questions were answered differently by each interviewee. The cross-interview analysis allowed for the clear identification of themes and indicated how each employee understood PoPI compliance in the workplace, and their role in maintaining data integrity and other relevant processes.

After permission was granted to conduct the study, the contact details of three other employees were provided to the researcher. Subjects were contacted via email and supplied with full information about the research project, along with the ethical clearance letter from the UCT Research Ethics Committee. Each subject was requested to sign and return the requisite form and to suggest a time that would be convenient for their participation. The researcher then contacted the interviewees telephonically. This interview method was useful for gathering relevant information in an open-ended fashion.

Interviewee subjects were part of a private established homeowners' association (HOA) within the Western Cape. The organization was small and there were only 4 relevant staff members available to interview. Interviews were conducted with the head of operations, information technologist, finance manager, and personal assistant/environmental officer.

All of the selected subjects consented to being recorded. Sometimes more than one interview question was answered at the same time, and because of this overlap, some of the later questions were redundant. They were nevertheless asked again to reiterate the importance of gathering this information as well as for clarity.

3.8 Organization of data for analysis and presentation

The data collected was audio-recorded so that it could be analysed later. Subsequently, all of the interviews were transcribed as accurately as possible. This was done so that explanations of the interview could be referenced accurately. This referencing technique makes data analysis easier for readers to follow. The interviews were presented systematically, referencing the interview questions. Sometimes questions were slightly rephrased as the interviews were conducted in a colloquial manner, and, as explained previously, sometimes questions were ignored. One participant did not know the answers to specific questions and so they were left completely unanswered. For the sake of maintaining the anonymity this research, interviewees' gender was anonymised, and a plural pronoun is used. This is in line with the researcher's intention to protect all participants and prevent any potential biases. The data is first presented vertically and then a cross-sectional analysis is performed on the case studies. The researcher gathered themes from the data and defined these themes within the analysis. The interview questions had previously been themed, and the answers also answered to the same themes; at times there was some overlap.

The interview data obtained was linked to existing propositions by returning to the research questions. The researcher also focussed on the core issues for mirco enterprises that face steep competition from large international organisations already compliant with PoPI standards. Analysing materials gathered from research is the part of the process that demands the most organization, which potentially makes it the most difficult (Eisenhardt, 1989:539). To prevent disorder, there was a comprehensive explanation of each interviewee's position, goals, and how they faced the issue of

compliance within their post. Analysis was conducted to measure in what way these companies struggle to comply, what resources were available to them, and what issues they continued to face. This overall aim was to dispel any confusion about the cause and effect of this legislation, and identify the effectiveness of the methods the company chooses to employ. The analytical procedures included lateral and bi-lateral examining to thematically dissect the answers given by the various interviewees. Lateral examination gives a general narrative of each interview, and later bi-lateral analysis is applied so themes can be more closely examined.

CHAPTER 4

Data Analysis and Presentation

4.1 The case study

In the first section of this chapter, the interviews will be analysed vertically. The researcher will narrate the interviews individually in their entirety. Later, the analysis will be conducted cross-sectionally to explore themes present in all of the interviews and explore how the given answers can be understood in relation to AT and contrast existing research.

4.1.1 Estate Manager Interview (Interviewee 1)

Interviewee 1 confirmed that they knew a substantial amount regarding the PoPI Act because they had led a project to implement its principles at the estate. They stated that they had specifically implemented appropriate policy and procedure, so that they would comply with the Act (line 25). It did not change the way they dealt with information because they already had "proper systems in place for basic protection of information" (line 28-29). Furthermore, they explained that the business already operated under the ISO14001 management system, which required that all processes ensure sensitivity to information in general (line 31-32).

They understood vicarious liability within sections 99 (1) and 99 (2) of PoPI as implying that more responsibility was to rest on the employee alone, rather than the employer (lines 42-43). These sections are widely criticised as being "too limited" because the list of defences that employers can use to defend themselves is short, thus leaving the employer "extremely vulnerable" (Millard & Basceranco, 2016:3-4). In addition, the

data subject can “base his or her claim against the employer either on the common law or on PoPI” (Millard & Basceranco, 2016:4). This means that the employer can be held accountable to either common law or on PoPI, whichever gives the data subject more traction in a court of law. According to this interviewee, “the fact that an employee who [was] appointed or not appointed [could] be held liable [for misconduct] and not necessarily the employer” was “a bit harsh” (line 45). They expressed they their concern about this specific clause because “normally accountability starts at the top and in this case, it sits a few levels down” (line 50).

The researcher realised that this interpretation of the clause was wrong. The interview continued, and the researcher interrogated how Interviewee 1 understood mitigating this risk.

Interviewee 1 explained that in the light of this, it would be best to hire people they understood to be trustworthy and continuously monitor their activities so as to proactively try to prevent breaches of PI (line 55-56). The Estate Manager (EM) explained that implementing these changes involved hiring an external specialist as a consultant to assist in the process of compliance (line 69). This process of compliance took a period of a year, after which the organisation was granted a certificate of official PoPI compliance (line 75). The EM claimed that this HOA was the first homeowners’ association in South Africa to receive this certificate (line 76). Reportedly, this certificate states that the company has undergone the necessary processes of due diligence for PoPI compliance (lines 82-83). Interviewee 1 noted that this status would need to be re-examined every six months to maintain its integrity (lines 85-87).

Interviewee 1 resisted stating whether or not they found the vicarious liability act fair or unfair because it “doesn’t matter ... it’s coming into effect as law, we will just have to live with what is in the Act” (line 92). In relation to the most important changes made in the workplace, they noted that more control over information was of the utmost importance, especially sensitive information. Sometimes “homeowners ask for information, and we say, sorry, we cannot supply this to you” (lines 103-104). These situations often arise when a new homeowner is attempting to contact a previous tenant in search of information about the specifics of home maintenance, for example. Sometimes the information is not deemed relevant for current homeowners to know, “for instance, access control records” (lines 112-113). Employees are sensitised to these issues in meetings. If a current homeowner wants to contact a previous homeowner, Interviewee 1 first contacts the previous owner for consent to release their contact information (lines 119-120). This interviewee explained that records of all such communication are kept, although this is not strictly necessary. Their mention of keeping information although they understand that they are not explicitly required to is demonstrative of an overlap between PAIA (Promotion of Access to Information Act) and PoPI regulations.

Interviewee 1 declared that the HOA was fully compliant at the time of the interview. They then reverted to question 6, regarding the employer's liability for the conduct of its employees. The EM told the researcher that the question about “employer as responsible party” should read “as the employee accountable” (lines 139-140). The researcher noticed that the interviewee clearly thought that PoPI essentially made employees liable for their actions, and not the employer, but was hesitant to correct them lest it affect the overall content of the interview. The EM later again queried the phrasing of the question, at which point the researcher felt obliged to explain that in

fact the Act specifies the employer as the party responsible for all employee actions, which was the main reason for this research. The researcher explained that this Act differed from similar legislation around the world in that it lacks the flexibility for employers to prove they have trained and educated staff (lines 145-148).

In terms of educating staff, Interviewee 1 explained the HOA had more than one session with an external consultant to explain the best way forward. All the department heads were in those sessions and “they were involved from the start” (lines 155-158). Afterwards, a PoPI procedure was formalised. With regard to changing technological procedures, the interviewee stated that not many things had to be changed, but basics including computer passwords were implemented (lines 165-167).

Interviewee 1 said the biggest challenge for them was compliance with PAIA, in that they understood that in certain cases information could be demanded from them, whereas in other cases, as per the PoPI Act, providing such information would not be allowed (lines 170-173). They also stated that it was problematic when homeowners privately shared their information as this is completely outside of the HOA’s control (lines 176-178).

With regard to the financial outlay of hiring a contractor to help with PoPI compliance, the cost was not an issue as the HOA follows a service level agreement, meaning that staff are hired on a need basis and there are very few full-time employees (lines 186-188). A further challenge the EM mentioned stemmed from the “clean desk” initiative, where all documents are to be protected and nothing left behind after the day’s work is finished (line 203-204).

Finally, the EM stated that not much information regarding the Act was in the public domain, that there was a "lack of understanding of the Act" and that it would prove a "big challenge" for "many, many [small and medium] companies" (line 214).

4.1.2 Information Technologist Interview (Interviewee 2)

The IT person understood fully that the HOA would be liable for prosecution should personal or sensitive information be leaked (Interviewee 2, lines 50-52). They were very well aware that vicarious liability meant that in certain unspecified circumstances, management can be liable for the actions of another more junior employee (lines 55-58). Furthermore, they expressed some concern about this clause because overseeing the actions of all one's employees seemed like a daunting if not impossible task. They felt that they did not have adequate control over the actions of all their employees (line 60-63).

At the time of the interview, no working procedures were being changed because, as Interviewee 1 had stated, the HOA was PoPI compliant (Interviewee 2, line 70). However, there were changes that had to be made in the process of complying. These changes were minor, such as enabling passwords on computers, organising training for personnel, and ensuring no documents were left behind after the work day (lines 76-78).

They thought the vicarious liability clause was "a bit unfair" because they did not have control over the actions of all employees, even though one-on-one training was given to all employees (lines 93-95). They explained that employees are not monitored daily, and only "every now and then" (later qualified as "monthly") is the workflow looked over. There was no official monitoring system (lines 103-106).

They identified their biggest personal challenge as ensuring that the changes were implemented, especially mitigating the vulnerability of the office as a public space with private information readily available as “anyone could just walk in and have access” (lines 111-113). They explained that although employees could not take information home, all the data was readily accessible to them at any time, meaning they could technically give it out at any time. However, confidentiality clauses had been signed throughout the office to protect the company (lines 119-121).

The IT person expressed concern that the broader public lacks an adequate understanding of the PoPI act in general, and customers do not know their rights (lines 128-129). They thought the public should be made aware of such laws regarding the privacy of information, although they didn’t know who would be responsible for such education (lines 135-138).

4.1.3 Finance Manager Interview (Interviewee 3)

Interviewee 3 understood PoPI as legislation meant to ensure that personal information is handled in a responsible manner (Interviewee 3, lines 11-12). They were unclear about what the vicarious liability clause meant (line 24), and referred instead to what the protection of privacy meant, viz. acting responsibly when handling or processing any data or personal information (lines 19-21).

In terms of how work procedures were affected within the compliance processes, they reported that nothing much had changed. They had always worked “in a very personal and private” way, as they deal with salaries and financial information. They were also a Commissioner of Oaths, so they understand the value of confidentiality (lines 30-32).

They reported no changes in work procedures, “I haven’t really changed anything of mine … we always comply with everything” (lines 36-38). They did not go through any training with regard to PoPI, nor were they aware of anyone else below them going through training (lines 40, 47). However, later they recalled that an external training team had visited the office and provided two training sessions (lines 49-52).

In terms of personally complying, they only mentioned that their computer had to be kept locked, although they claimed that this had always been the case (lines 65, 67).

Interviewee 3 did not have any further comments or observations, other than to reiterate that the HOA was compliant (lines 68-70).

4.1.4 Environmental Officer Interview (Interviewee 4)

Interviewee 4 did not answer directly when asked what the PoPI Act meant but observed that their organisation had always had a policy in place that information is personal and “shouldn’t be given out” without permission (Interviewee 4, lines 21-22). Furthermore no one should have access to this information. Their understanding of vicarious liability was that the HOA would be responsible should an employee give out this information and thus not comply with the Act (lines 26-27).

They did not express any concern with regard to the vicarious liability clause as they felt the HOA had “an obligation to train the staff” and ensure that employees’ actions were monitored on a daily basis. They thought it was fair that employees would be responsive to the employer’s requests and demands within the work environment, and that accepted that the employer would be the party responsible for any infraction (lines 29-32).

Interviewee 4 explained that little change was made to the HOA's operations before compliance was reached because they had "always had a policy of keeping homeowners' information private" (lines 35-36). The small changes that were made included the "clean desk policy" (lines 38-39). They did not find vicarious liability to be unfair because "everyone has a right to have their information protected".

They reported that accountability was monitored through the Head of Department and at regular meetings. They explained that there was an ongoing in-house training programme because the HOA is "ISO compliant" (line 50-52). This training happened every month but did not necessarily include PoPI training. However, new employees are trained regarding PoPI and regular employees are given PoPI training once a year (lines 54-55). They explained there were no technological changes made before or after compliance, nor did compliance change the way in which the HOA stores data (line 60, line 62).

Interviewee 4 believed that their organisation was at the forefront of PoPI compliance. There was a lot of resistance to it because "it's another system" and "any systems with regard to legislation… people tend to have issues with" (lines 69-71). The reason for this resistance to adopting policies was unclear to the researcher, but she inferred that it meant working to gather enough resources to make the changes required.

4.2 Cross-Interview Analysis

Themes across the interviews were identified using close reading to detect word frequencies. The themes to be identified loosely correspond to the eight core specifications of the PoPI act, which will be expanded upon and located in the context of the research. These principles are: accountability, processing limitation, purpose

specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. The interview questions were designed to measure compliance with these principles and also answer the research questions:

1. How concerned are SMMEs with vicarious liability in the context of their specific workplace?

2. Does the SMME believe that compliance will be reached within the grace period?

3. Does the SMME currently have adequate resources to educate employers on new protocols and the financial ability to employ suitably knowledgeable personnel, give workshops, training courses, etc.?

The themes will be concentrated into the following categories that are identified as significant in the larger scope of the study;

A) understanding PoPI and what vicarious liability means

B) education on the Act and important security practices, and

C) general concerns about PoPI compliance for South African SMME's

These issues will be explored in depth in the following sections by comparing and contrasting interviewees' attitudes towards them.

4.2.1 Theme A: Understanding of PoPI and the Vicarious Liability Clause

The question of understanding vicarious liability is paramount in this research and the interviews were designed to highlight this aspect. All four interviewees understood the concept of privacy to be of utmost importance, but their understanding differed in terms of how they understood it should be treated in the workplace. For example, with regard to training and knowledge of PoPI and the vicarious liability clause, only one of the interviewees demonstrated a clear understanding of what implementing these

changes meant for the workplace. There was a lack of consistency in the interviewees' understanding of what vicarious liability was in the application of their workplace processes.

Interviewee 3 was not able to explain what the vicarious liability clause within the legislation meant and reported only that the company always had a policy that personal information should not be given out (Interviewee 3, lines 22-23). In another instance, Interviewee 1 explained they understood the PoPI act "well, because [they had done] a project to implement the PoPI Act principles" (Interviewee 1, lines 22-23). Interviewee 1 reported that they were concerned about the clause because "normally accountability stops at the top" and in this case accountability "sits a few levels down" (lines 48-50). Interviewee 3 said that vicarious liability meant "the company is responsible if [an] employee gives out information [or if they do not] comply with the Act" (lines 26-27). They understood simply that information should not be made freely available but did not mention further details. While Interviewee 3 admitted understanding little about the clause, Interviewee 1's interpretation of it – that employees rather than employers would be held responsible for their wrongdoing – was simply incorrect.

Interviewee 4 appeared to share a similar point of view, and rephrased the vicarious liability question back to the researcher as follows: "isn't it that you must be responsible … when you're handling or proceeding on any data or personal information?" (lines 19-21). When asked for clarification on vicarious liability, they said they did not know. It was obvious that this interviewee did not understand that employers could be held responsible for the actions of others in certain circumstances pertaining to the

processing, sharing and storing of information. The researcher chose to give this information to the Interviewee because they had asked for it. In contrast, Interviewee 2 understood the Act to "protect all personal information" the company had access to, explaining that they "could also be liable for another person's actions", although "in South African laws, [it] actually says we can't be liable … [but] in certain circumstances, we can [be]" (lines 56-58). This interviewee demonstrated that the definition of vicarious liability was unclear for their organisation and their specific role within the company, especially with regard to those working under them. "Inevitably, in any organisation that consists of an employer and employees, the employer will be held liable for contraventions of PoPI by its employees because PoPI regards the employer as the responsible party" (Millard & Basceranco, 2016:3). To the same question, Interviewee 4 responded curtly that the purpose of PoPI was "just to ensure [employees] conduct themselves in a responsible manner when handling personal information" (lines 11-12). In the context of PoPI, none of the interviewees understood that the affected party, who would traditionally have sued the employer for infringement of privacy based on the common-law vicarious liability doctrine, could now sue them in terms of this legislation: "there is the possibility to litigate based on the stipulations of PoPI" (Millard & Basceranco, 2016:3). The analysis of this theme therefore concludes that none of the interviewees understood exactly what vicarious liability meant with respect to the Act.

4.2.2 Theme B: Education on the Act and Important Security Practices

This second theme is considered a sub-theme of the first because it relates to processes and changes that occur or need to occur during PoPI compliance. Security was a prominent theme in all of the interviews, which suggests that it was highly valued

by all the respondents in their various roles in the HOA. It is important that all employees be made aware of the provisions of the Act and how each role affects the overall performance of the company in compliance. Only adequate training of staff would ensure the effectiveness of the HOA's compliance certification.

Each interviewee was questioned on the education processes in the training they had received and the security practices that resulted from it. Interviewee 1 explained that an external staff member had conducted "more than one session … going through the do's and don'ts" of the Act, its history, and what needed to be done going forward. "All of the department heads [participated] in those sessions" (Interviewee 1, lines 155-158). This interviewee implied that there had been some information passed down to those underneath the department heads, yet each of them had to determine what information it was necessary to convey. Interviewee 3 was non-specific about the details of this training and mentioned that training happened throughout the year: "we have ongoing monitoring through our HOO's and through our regular meetings…. We have a training programme, because we're ISO compliant, so we have a continuous training programme, and that's included in our training" (Interviewee 3, lines 50-52). However, it was unclear whether or not this training included PoPI or if it was simply an update on security practices in general. Later, they clarified that once a year PoPI training is given to staff and all new staff members (Interviewee 3, lines 54-55).

In contrast, Interviewee 4 reported not having had any training on PoPI at all and replied "No" when asked if they or anyone they knew of had gone through training (Interviewee 4, lines 40, 45). However, they mentioned "we've got people that came to our office and you know, were telling us … there were two [training sessions] ... So, I mean, we had that with the PoPI Act people twice" (Interviewee 4, lines 49-51). A

different answer was given by Interviewee 2, who claimed that there was no workshop but rather something “like a one-on-one training, just to bring them up to speed… on a one-on-one basis” (Interviewee 2, Line 80-82).

There was a variety of responses when interviewees were questioned about the changes they were instructed to make in these training sessions. These changes included enforcing the clean desk policy, ensuring computers were password protected, and securing the office against the vulnerability of its being used as a public space for clients and others visiting the HOA. Interviewee 2 reported this vulnerability as one of their biggest challenges because “anyone could just walk in and have access to information” (lines 112-113). Interviewee 1 also reported a clean desk means making sure “there’s nothing left that’s of any interest to anyone … and [that if there is something of interest] they cannot access it” (lines 203-204). Interviewee 3 did not see these as big changes. In terms of their security, things “changed … a teeny weeny little… the clean desk policy and stuff like that. But as far as homeowner information … we’ve always had [the] policy [to keep this information private]” (Interviewee 3, lines 38-39). Interviewee 4 suggested that nothing had changed in terms of the best practices of their position, “... mine [are] still the same… nothing is lying around, and people can’t access my computer, or papers… Everything is locked away” (Interviewee 4, lines 59-61).

4.2.3 Theme C: General concerns about PoPI compliance for South African SMMEs

This is also considered a sub-theme of the main theme, understanding PoPI and vicarious liability. The research examined this aspect because the perception of the entire compliance process on the part of those who had already gone through it might

provide insights for companies or organisations still struggling to do so. There were mixed responses to this question.

Interviewee 4 thought there was “a bit of resistance to [the Act] because it’s… another system [and] people tend to have issues with systems” (lines 69-71). This interviewee was talking about generalised resistance to change, perhaps because of the Act’s complexity and conflict with other legislation with which SMME’s are required to comply. Interviewee 1 said, “I just think there’s a lot of information about the PoPI Act that’s still not out in the market”, and observed that this lack of understanding would be a “big challenge for many, many companies” (Interviewee 1, lines 210-211, 214). They also mentioned the possibility of conflict with PAIA (Promotion of Access to Information Act) because “in certain cases, people can demand information from you [and] in other cases, as per PoPI … you cannot supply [that information]” (Interviewee 1, lines 171-173). This spoke to Interviewee 4’s remark about resistance, as companies were obliged to negotiate different, sometimes conflicting legislation. Interviewee 2 also spoke to this complication, noting that “South African laws [actually] state that we can’t be liable for another person’s actions, but in certain circumstances, we can” (Interviewee 2, lines 56-57). These comments demonstrate that the interviewee does not completely understand vicarious liability, nor the reality that the “data subject may elect to base his or her claim against an employer either on the common law or on PoPI” (Millard & Basceranco, 2016: 4). This interviewee also stated that they did not believe the general public was educated about these matters: “I just think the broader public doesn’t understand PoPI, and doesn’t know their rights… People [do not even understand] the signboard [which says] that we’re liable” (Interviewee 2, lines 128-132). It is important to note that Interviewee 3 was not asked

the question because they did not seem to be knowledgeable about vicarious liability or any of the compliance processes.

4.3 Summary

SMMEs are expected to change many of the ways they store, process, and access personal information. This includes training staff, financial support to implement changes, and guidance towards better policies. PoPI aims to give further protection to South African consumers, but consumers also need to be made aware of the rights they have under this legislation. Although a number of insights were generated through the interview process, the researcher acknowledges that the scope was definitely limited because of the number of interviewees and the paucity of information provided by some of the participants. The bi-lateral and vertical analysis proved to be helpful in establishing further information about themes closely related to the initial research questions. The researcher felt that because of the method of data analysis used, it was not necessary to use techniques of data presentation such as word frequency demonstrations or word clouds. Instead, the interviews are attached as appendices, with mark-up highlighting the various themes and the lines numbered (as referenced throughout the analysis).

CHAPTER 5

Discussion and conclusion

5.1 Introduction

This chapter discusses the research findings, important details the researcher noticed within the process. It acknowledges the limitations of the study, makes some recommendations, and uses the findings to draw final conclusions. Appendices include the consent form (Appendix A), the interview questions (Appendix B), and the interview transcripts (Appendix C).

The data collection process did not go easily at first, as there were few companies who were willing to participate in or even communicate about study. The researcher believes this reluctance was potentially due to admitting deficiencies about the processes within the workplace. There also may have been concerns about privacy, or that the researcher might share the identity of the organisation. Because of this, the research began later than anticipated and the sample was much smaller than expected; initially the researcher intended to interview between 6 and 7 people in relevant roles to gain insight into how they were handling the challenges of PoPI compliance. As mentioned in 3.3, although the information gathered was limited, the quality and quantity of data gathered from the interviews was very useful for this research.

This study investigated PoPI compliance for South African SMMEs, many of which will be strongly impacted by the upcoming enforcement of this legislation. Of particular importance and weight is the vicarious liability clause, which, unlike other similar legislation around the world, is seemingly unforgiving to employers whose employees

breach personal data regulations. This study revealed how one SMME in particular handled such vulnerabilities, what their concerns were, and how they attempted to educate staff about the importance of implementing new procedures. The interviews demonstrated that while some employees were very informed, others did not know the legislation in detail and reported nothing had changed regarding the company's standard operating procedures. Meanwhile, some employees seemingly knew little or nothing of what vicarious liability meant for them. It was clear that while some interviewees took a proactive approach to handling this issue, others understood simply that information privacy had always been a priority, even prior to PoPI legislation. In such an instance, AT could be applied to streamline knowledge and monitor changes in the workplace so that they might be adopted evenly. It is unfavourable to have many variations on such an important matter; all employees should know their responsibilities and understand the foundation of changes within the company.

5.2 Discussion

5.2.1 Implementing PoPI and its effects on SMMEs

This legislation presents several challenges, particularly for SMMEs who may not have the resources, knowledge, or know-how to begin the implementation process. This study discovered that the process of compliance includes access to external resources, comprehension of information regarding the Act, and finding new best practices for the workplace. Some of the interviewees reported that they were significantly concerned about the apparently widespread lack of understanding regarding the severity and importance of the legislation. This was demonstrated by the interviewees' imperfect understanding of PoPI. The fact that basic understanding

of PoPI was absent means comprehension of vicarious liability is not known to employers or employees in this context, which is unfavourable. AT might suggest that a streamlined training and congruent follow-up approach on in-house changes regarding PoPI and vicarious liability is something that could be applied in this situation. Analysis of the interviews revealed significant discrepancies, even in an organisation that had been accredited for PoPI compliance. This will be expanded upon in the next section.

5.2.2 Discrepancies in findings

There was noticeable confusion about vicarious liability among the employees who were interviewed for this research. The first interviewee, who seemingly handled most of the overarching processes within the company, was unclear about what vicarious liability meant. They understood vicarious liability to mean that employees would be responsible for their own actions, rather than the "employer" being responsible for the actions of all employees. Since this is one of the most controversial and highly criticised aspects of the Act, the finding was somewhat worrying. Furthermore, although two interviewees reported that there was ongoing training to ensure that all employees were versed in the details of the Act, one interviewee did not know what vicarious liability meant. They were likewise unclear about what PoPI meant and simply equated it with protecting personal information within the workplace, a value that the company had reportedly respected even before the Act. These findings were important because they demonstrated the potential for miscommunication and information concentration that did not necessarily trickle down to subordinates or was unevenly distributed in the organisation. It also proved that although some employees were knowledgeable about information protection laws in South Africa, very important

aspects could be misunderstood. The researcher suggests that some of these discrepancies could be dealt with by using measurable tools such as short tests or quizzes. These could help identify knowledge gaps which could be revisited within the training sessions.

5.3 Findings in the Context of Accountability Theory

AT has proven to be a tool that can be used by human resources personnel and managers to measure how effectively employees adopt specific practices and procedures within the workplace. This research found that there was evidently some confusion about what vicarious liability meant, although all the interview subjects noted that new security procedures were treated as a priority to secure the personal information held within the organisation. The findings suggest that the organisation was unclear how to monitor the actions of its employees and rather relied on some education about the Act as providing them with enough motivation to adhere to new rules and regulations. This was somewhat concerning. Ideally, employees should be made part of the process changes. If they are involved in this, then perhaps this will improve broad adoption and mean less monitoring will be needed by employers.

Accountability theory says that hierarchies are important to establish an internal understanding of who reports to whom. In the context of vicarious liability, employers have options. Making use of quality assurance roles ensures work is performed to standard and within allotted timeframes; it also means metrics are being reported to management about the issues that may arise from quality assurance data analytics. Quality assurance can also be used to educate employees. In the interviews, a

knowledge gap was undeniably present as to what exactly the reason for the new processes were, although the researcher knew that the processes were because of PoPI. Regardless of the gaps in comprehension, there was a shared sense of responsibility from the employees interviewed and each emphasised that security and the protection of privacy remained core objectives of the organisation.

5.4 Concluding remarks

Ensuring successful PoPI compliance is essential for all South African companies, regardless of size. The process requires many of these organisations to take the initiative to research and understand the weight of this new legislation and its effect on policies and procedures. Management must proactively understand the weaknesses within the company and seek to rectify them to ensure they are not at risk or liable for employees' actions, as supported by the premise from AT that "under pure process accountability, employees expect to justify efforts and strategies to generate results. The focus is on inputs, not outcomes" (Tetlock et al., 2013: 22). This entails management's seeking the means to educate employees and see that the foundations of PoPI are truly comprehended. This in turn means active engagement and the monitoring of outcomes. By doing so, organisations can ensure their immunity to risks that may result in great financial and reputational losses. Likewise, it is clear that the general public needs to understand their rights in the new era of South African information protection laws, and what they can do in the event of their personal information being shared without consent.

5.5 Limitations of the study and recommendations for further research

This study was limited to one SMME in the Western Cape, and so cannot be taken as representative of the situations such firms around the country are facing. Furthermore, this particular organisation was non-profit, and had access to funding in order to hire an external compliance specialist to assist with compliance processes. This is a variable that cannot be assumed to apply to other SMMEs, which may not have the same resources. If this organisation had not had the assistance of an external auditor, the answers of the interviewees might have been vastly different.

Further research may look to involve SMMEs from other provinces, particularly those in rural areas. Undoubtedly, the organisation in question was one that presented a best-case-scenario; having already become PoPI compliant, it was routinely regulated and did not face financial strain. In some ways, this was not the kind of case study the researcher had in mind, but the limitations were embraced because of the timeline imposed on the research. It is important to look at the management processes of SMMEs, and perhaps do a comparison with how larger companies tackle the issue. This may generate some constructive insights for smaller companies. Such research will be important for further regulation adoptions and simultaneously produce insight into specifically South African issues within management and the workforce in general. It is in the interest of the national economy to ensure that smaller companies have a fighting chance of competing within the global economic sphere, while at the same time scrupulously protecting the privacy of its citizens.

Case References

Bezuidenhout v Eskom 2003 3 SA 83 (SCA)

Melvin v Reid 1931 Cal. App.112 (Cal. App.)

References

Anyan, F. 2013. The influence of power shifts in data collection and analysis stages: a focus on qualitative research interview. *The Qualitative Report*. 18(36):1-9. http://www.nova.edu/ssss/QR/QR18/anyan26.pdf

Barbero, M., Coutuer, J., Jackers, R., Moueddene, K., Renders, E., Stevens, W., Toninato., Y., et al. 2016. *Big Data analytics for policy making*. Deloitte. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2016-07/dg_digit_study_big_data_analytics_for_policy_making.pdf

Baxter, P. & Jack, S. 2008. Qualitative case study methodology: study design and implementation for novice researchers. *The Qualitative Report.* 13(4):544-559. http://nsuworks.nova.edu/tqr/vol13/iss4/2

Berlin, I. 1969. *Four essays on liberty*. Oxford: Oxford University Press.

Borena, B., Belanger, F. & Egiju, D. 2015. Information privacy protection practices in Africa: a review through the lens of critical social theory. *48th Hawaii International Conference on System Sciences*. http://doi.org/10.1109/hicss.2015.420

Botha, J., Eloff, M.M. & Swart, I. 2016. Proactive data breach detection: Examining accuracy and applicability on personal information detected. *International Conference on Cyber Warfare and Security.*

Botha, J., Eloff, M.M. & Swart, I. 2015. Evaluation of online resources and the implementation of the Protection of Personal Information Act in South Africa.

Pretoria: Institute for Corporate Citizenship, UNISA.
https://www.researchgate.net/publication/274390237

Botha, M., Millard, D. 2012 The past, present and future of vicarious liability in South Africa. *De Jure.* 45(2): 225-253. http://www.scielo.org.za/pdf/dejure/v45n2/02.pdf

Cavoukian, A. & Jonas, J. 2012. Privacy by design in the age of big data. *Information and Privacy Commissioner of Ontario, Canada*. www.privacybydesign.ca

Cumbley, R. & Church, P. 2013. Is "Big Data" creepy? *Computer Law & Security Review*. 29(1):601-609. http://dx.doi.org/10.1016/j.clsr.2013.07.007

DeCew, J. 2002. Privacy. *Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/entries/privacy

Domanski, R.J. 2015 Framing the Question "Who Governs the Internet?" *CUNY Graduate Center.* Lexington Books.

Dunn, J. 2017. Trump just killed Obama's internet-privacy rules: here's what that means for you. *Business Insider*. Available at: https://www.businessinsider.com/trump-fcc-privacy-rules-repeal-explained-2017-4?IR=T. June 09, 2018.

Eisenhardt, K.M. 1989. Building theories from case study research. *The Academy of Management Review*. 14(4):532-550.

Eloff, D. 2018. Unscrambling the general data protection regulation. *De Rebus*. Available at: http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/. July 17, 2018.

Frick, W. & O'Neill, C. 2016. When not to trust the algorithm. *Harvard Business Review.* October 06, 2016.

Frink, D. & Klimoski, R. 2004. Advancing accountability theory and practice: introduction to the human resource management review special edition. *Human Resource Management Review.* 14:1-17.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report.* 8(4):597-606.

Hinde, C. 2014. A model to assess organizational information privacy maturity against the Protection of Personal Information Act. BSc Dissertation, Department of Information Systems, University of Cape Town.

Hinde, C. & Ophoff, J. 2014. Privacy: a review of publication trends. Centre for Information Technology and National Development in Africa, University of Cape Town.

Kvale, S. 1994. Ten standard objections to qualitative interviews. *Journal of Phenomenological Psychology.* 25(2): 47-173.

Kvale, S. 1996. *Interviews: an introduction to qualitative research interviewing*. London: Sage.

Le Fleur, H., Koor, J., Chetty, V., Ntshangase, S., Mackenzie, R., & Rawoot, F. (2014). Informal Small Medium and Micro Enterprises (SMME) Retailers in South Africa. Johannesburg: Henley Business School .

Loubster, M., Midgley, R., Mukheibir, A., Niesing, L., Perumal, D. 2009. The Law of Delict in South Africa. *Oxford University Press.*

Makulilo, A.B. 2015. Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review*. http://dx.doi.org/10.1016/j.clsr.2014.11.005

Mantelero, A. 2013. The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*. 29(3): 229-235. http://dx.doi.org/10.1016/j.clsr.2013.03.010

Marr, B. 2016. *How Big Data and Analytics are Transforming Supply Chain Management.* Available: https://www.forbes.com/sites/bernardmarr/2016/04/22/how-big-data-and-analytics-are-transforming-supply-chain-management/#37cdd55639ad. Accessed October 11, 2018.

Merriam-Webster. “dox”. Merriam-Webster. Available at: http://merriam-webster.com/dictionary/dox. Accessed February 02, 2018.

Millard, D. & Bascerano, E.G. 2016. Employers’ statutory vicarious liability in terms of the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad* 19(1). http://doi.org/10.17159/1727-3781/2016/v19i0a555

Miles, M.B. 1979. Qualitative data as an attractive nuisance. *Administrative Science Quarterly.* 24(4): 590-601. http://www.jstor.org/stable/2392365

Murray, S. 2012. The extent of an employer’s vicarious liability when an employee act within the scope of employment. LLM Dissertation, Department of Law, North-West University.

Nadasen, N., Pilkington, C. & Da Veiga, A. 2016. Personal information value chains in the South African insurance industry: an experiment. *International Conference on Information Resources Management (CONF-IRM).* http://aisel.aisnet.org/confirm2016/28

Neidig, H. 2017. Trump signs internet privacy repeal. *The Hill*. Available at: https://thehill.com/homenews/administration/327107-trump-signs-internet-privacy-repeal. Accessed January 27, 2018.

Ocholla, D. 2009. Information ethics education in Africa: where do we stand? *International Information & Library Review* 41(2): 79-88. http://dx.doi.org/10.1080/10572317.2009.10762802

Oxford English Dictionary. “Compliance”. Available at: https://en.oxforddictionaries.com/definition/compliance. Accessed January 27, 2018.

Richards, N.M. & King, J.H. 2014. Big Data and the future for privacy. *SSRN Electronic Journal*. http://doi.org/10.2139/ssrn.2512069

Roy, J. 1999. ‘Polis’ and ‘Oikos’ in Classical Athens. *Greece & Rome.* 46(1):1-18.

Saunders, B., Kitzinger, J. & Kitzinger, C. 2015. Anonymizing interview data: challenges and compromise in practice. *Qualitative Research.* 15(5):616-632. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4582834/

Skolmen, D.E. & Gerber, M. 2015. Protection of personal information in the South African cloud computing environment: a framework for cloud computing adoption. *Information Security for South Africa (ISSA)*. Johannesburg. 1-10. doi: 10.1109/ISSA.2015.7335049

Solove, D.J. 2004. *The digital person*. New York: New York University Press.

Solove, D. J. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review*. 154(3):447-560.

Solove, D. J. 2009. *Understanding privacy*. Cambridge, MA: Harvard University Press.

South Africa. Protection of Personal Information Act (POPIA/ PoPI), 2013. https://www.saica.co.za/Portals/0/Technical/LegalAndGovernance/37067_26_11_Act4of2013ProtectionOfPersonalInfor_correct.pdf

South Africa. Department of Justice. 2016. Government, 2 Dec 2016. http://www.justice.gov.za/inforeg/docs/ms-20161202-inforeg.pdf

Stake, R.E. 1978. The case study method in social inquiry. *Educational Researcher* 7(2):5-8.

Stenbacka, C. 2001. Qualitative research requires quality concepts of its own. *Management Decision.* 39(7):551-556.

Sullivan, B. 2006. 'La difference' is stark in EU, U.S. privacy laws. [online] msnbc.com. Available at: http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.WR2YUBOGPeQ. Accessed 18 May 2017.

Swartz, P. & Da Veiga, A. 2016. POPI Act opt-in and opt-out compliance from data value chain perspective: a South African insurance industry experiment. *Information Security for South Africa* 9-17.

Tetlock, P., Vieider, F., Patil, S. & Grant, A. 2013. Accountability and ideology: when left looks right and right looks left. *Organizational Behaviour and Human Decision Processes.* 122:22-35.

Turner, D.W. 2010. Qualitative interview design: a practical guide for novice investigators. *The Qualitative Report* 15(3): 754-760. http://nsuworks.nova.edu/tqr/vol15/iss3/19

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), available at http://www.refworld.org/docid/3ae6b3712c.html. Accessed June 07 2018.

Vance, A.O., Lowry, P.B. & Eggett, D. 2015. Increasing accountability through user-interface design artefacts: a new approach to addressing the problem of access-policy violations. *MIS Quarterly*. 39(2):345-366.

Zomorodi, M. & Donohue, L. 2017. "Note to self". *The bookie, the phone booth, and the FBI*. N.p., 2017. Web. 8 May 2017.

Appendix A

Investigating PoPI compliance and vicarious liability in the workplace

Informed Consent for Interview at a Small Medium/Micro Enterprise

Purpose

My name is Kimberly Beth Watson. I am an MPhil student specialising in Digital curation in the Library and Information Studies department at the University of Cape Town. I am executing a study on the vicarious liability clause within the Protection of Personal Information Act (PoPI). As part of this study I would like to interview staff from within a small medium or micro enterprise that has, will, or is in the process of complying to PoPI. I would greatly appreciate your participation.

Agreement

By signing this consent form you agree to grant me an interview session with you. This interview will not last more than an hour and will be conducted over the phone and will be recorded with your permission using an audio recorder. I will ask questions related to this particular topic of study. The collected information will be treated as highly confidential and any personally identifying information regarding you or your company will be anonymized during reporting and analyzation. Participation in this study is voluntary and your participation may be withdrawn at any time during the research process.

Contact

You will be given a copy of this consent form for personal record keeping purposes. If you have further questions or concerns regarding this study or require more information, you may contact myself or my thesis supervisor.

Kimberly Beth Watson (researcher)
Email: WTSKIM004@myuct.ac.za
+27659615661

Professor Richard Higgs (supervisor)
Email: Richard.higgs@uct.ac.za
+27836111419

Informed Consent

By signing this form, I consent to be a participant in the research study outlined above. I understand why this study is being conducted and what information will be collected from me. I agree to be involved in this study by participating in this interview**. I agree/do not agree** for this interview to be recorded.

Signature of researcher _____ Date _____

Signature of participant _____ Date _____

Appendix B

Research Questions

[Hello, my name is Kimberly Beth Watson. Thank you for taking the time to participate in this study. I understand that you do/ do not wish to be recorded. I will / will not record this conversation. Do you have any questions or concerns before we start?]

1. What do you know about the Protection of Personal Information Act?

2. What is your understanding of the vicarious liability clause within this legislation?

3. Are you concerned about the vicarious liability clause within the legislation? If so, how?

4. In what ways do you see PoPI affecting your work procedures as they are now?

5. In what ways have you prepared to face these changes?

6. Do you consider some aspects of PoPI to be unfair because accountability of the employer as the responsible party holds the employer accountable for non-compliance, while similar legislation around the world is more lenient?

7. What are some of the most important things you are changing within the workplace to make sure your company is compliant with PoPI?

8. Do you plan to enable or develop monitoring programs to develop accountability for those employees who deal directly with sensitive/private client information?

9. Do you believe your company will reach full compliance within the 1-year grace period?

10. Do you believe you have adequate resources (with regards to human resources, finances, education plans, etc.) to educate staff and make necessary technological changes?

11. What do you understand to be your organization's greatest challenges in attempting to comply with PoPI?

12. How will PoPI change how your process, collect, and store your data?

13. Any other observations?

[Thank you for participating in my research. Let me know if you have any further concerns about the content of this interview. If you wish to retract anything from the record at any time, please feel free to contact me, via email or phone.]

Appendix C

Ethical Clearance

Library and Information Studies Centre
University of Cape Town
Upper Campus

Private Bag X1, RONDEBOSCH, 7701 South Africa
Level 6 Hiddingh, The Chancellor Oppenheimer Library
Tel: +27 (0) 21 650 4546
E-mail: lisc@uct.ac.za
Internet: www.lisc.uct.ac.za

UCTLIS201710-17 15 October 2017

Ms Kimberly Watson
Library and Information Studies Centre
University of Cape Town

Dear Ms Kimberly Watson

I am pleased to inform you that ethical clearance has been granted by the Ethics Review Committee of the Library and Information Studies Centre on behalf of the Humanities Faculty of the University of Cape Town for your Master's study entitled: *Investigating PoPI compliance and vicarious liability in the workplace.*

I wish you the very best with your study.

Yours sincerely,

A/Prof. J. Raju
Chair, Department (LISC) Research Ethics Committee

Appendix D

Here is a link to the archive of interview transcripts: 10.6084/m9.figshare.5896708