Organizational information privacy strategy and the impact of the PoPI Act

Marc Pelteret
Jacques Ophoff

This is the accepted version of a paper published in 2017 Information Security for South Africa: proceedings of the 2017 ISSA conference.
The final, published version is available via DOI: https://doi.org/10.1109/ISSA.2017.8251775

Organizational Information Privacy Strategy and the Impact of the PoPI Act

Marc Pelteret[1] and Jacques Ophoff[2]
Department of Information Systems
University of Cape Town
Cape Town, South Africa
marc@pelteret.net[1], jacques.ophoff@uct.ac.za[2]

***Abstract*—In today's knowledge-centric society, personal information is one of the key resources of most businesses. Because of this, maintaining the privacy of personal information has become an important topic. Many countries have enacted, or are in the process of enacting, legislation to govern this. South Africa is addressing privacy concerns through the Protection of Personal Information (PoPI) Act, which imposes heavy penalties for non-compliance. This paper examines current organizational information privacy strategies and what impact the PoPI Act is making. Using a case study approach, data was collected from five organizations in the South African financial services industry. The findings offer insight into the complexities of forming and executing a privacy strategy, as well as the difficulties around complying with legislation. The PoPI Act has influenced the organizations to varying degrees, with some simply assessing its impacts and preparing to implement changes at a later point, while others have been making changes for many years. One of the key challenges that was highlighted is that it is based on principles and therefore open to interpretation. However, for most of the organizations it appears to offer benefits, such as the opportunity to bring more international business to South Africa.**

Keywords-privacy; information privacy strategy; Protection of Personal Information (PoPI)

I. INTRODUCTION

In our society, we simultaneously seek privacy while having to disclose personal information to receive services and establish friendships. Online communication and the social web have led us into the habit of sharing large amounts of information with a great number of people, yet many do not feel threatened when doing so [1]. The problem is that the same technology that makes it easy to share personal details has also led to 'greased information' – "once information is captured electronically for whatever purpose, it is greased and ready to go for any purpose" [2]. Consequently, the safety of our personal information has become of great importance and a major topic of interest to researchers, the business and IT sectors, as well as the public.

South Africa has enacted the Protection of Personal Information (PoPI) Act to promote the protection of personal information by regulating how organizations handle, store and secure this information [3]. By doing so, the country is a following a global trend, joining more than a hundred other countries that have privacy laws in place or in the process of development [4].

Given the introduction of the PoPI Act and the threat of harsh punishment for failing to comply with it, many companies are preparing to become compliant. The PoPI Act will affect all companies [5], as it applies to all organizations, public and private, of all sizes, and it applies to personal information of all types – that of customers, employees, juristic persons and any other stakeholders. Though the informational privacy strategies of companies have been explored in other countries [6; 7], no such research has been performed and published on firms in the South African context. The question guiding this research is: how are organizational information privacy strategies being impacted by the impending PoPI Act?

The rest of this document is structured as follows. The next section provides a review of relevant literature. Following this, the research methodology is presented. In the next section, the research findings are discussed. Lastly, the conclusion summarizes the research contributions.

II. LITERATURE REVIEW

This section examines the interrelationship of privacy and personal information, followed by the importance of privacy to organizations. Finally, the PoPI Act itself is briefly discussed.

A. Privacy and Personal Information

Privacy is an elusive concept, not only because it is difficult to define, but because it is a dynamic one – it is transforming over time and is often influenced by "political and technological features of the society's environment" [8]. Today, privacy is synonymous with personal information and information technology is the danger. The effect IT has had on personal privacy can be divided into four factors: 1) the amount of data that can be collected; 2) the speed at which it can be exchanged; 3) the length of time that the data can be retained; and 4) the kind of information that can be acquired [9].

Privacy can be defined as the "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others", elaborating that in terms of social interaction privacy is "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" [10]. Specifically, [9; 11] refer to informational privacy as having

control over and being able to limit access to one's personal information. It this view that is most relevant to this research.

There are numerous ethical issues around information, its existence and use. An established view is PAPA: privacy (what information should one be required to divulge about one's self to others?), accuracy (who is responsible for the authenticity, fidelity and accuracy of information?), property (who owns information?), and accessibility (what information does someone have a right to obtain?) [12]. Alternatively, [13] list four areas of consumer privacy concerns that are like PAPA: improper access to personal information, unauthorized secondary use of personal information, errors in personal information and collection of personal information. Agreeing with the above, [14] states that the "problem with databases is not that information collectors fail to compensate people for the proper value of personal information. The problem is people's lack of control, their lack of knowledge about how data will be used in the future, and their lack of participation in the process".

The expanded privacy model [15] illustrates how complicated it is for an individual to know who will have access to their data after they have shared it. While an individual knows the second party, who they have decided to provide information to, they may not know the legitimate third parties that the second party shares with, or even that the second party shares the information at all. The possibility of a fourth (illegal) party is unlikely to be factored into the decision to share information. When individuals are uncertain about the outcome of sharing information with a second party and are dependent on the decisions of the latter, trust becomes a factor [16].

B. The Importance of Privacy to Organisations

An organization manages privacy through its information privacy program, which is "the collection of policies and procedures that firms implement with respect to the collection, use, reuse, security, storage, and disposal of their customers' personally identifiable information" [17]. Fundamentally, a firm can see privacy as a threat to be dealt with or as an opportunity to be taken.

Organizations that view privacy as a threat want to comply with legislation and regulations to avoid potential trouble, particularly given that privacy issues are bad for business. Several studies have been conducted to determine the effect of breaches on the performance of a firm, particularly by looking at its stock price. Evidence shows that there is a negative effect, but it is short-lived [18; 19]. Furthermore, [20] posit that not all breaches are viewed equally by the market: those involving confidential information make a far greater impact than those that do not. Privacy issues can endanger the fiduciary relationship with shareholders if the bottom line is affected because of stock price declines, the loss of customers, fines or other costs incurred in addressing the issues [21]. Privacy breaches can lead to lower customer trust in a firm, while security breaches (which may not necessarily lead to privacy breaches) can lower a customer's willingness to deal with the company [16].

Addressing privacy can also be an opportunity for companies. Many countries have legislation that requires third parties in foreign countries, with whom a firm might share its personal information for special processing or other reasons, to be governed by equivalent law to protect the owners of that information. By complying with such legislation, companies can take advantage of cloud services to improve efficiency and reduce operating expenses [22], and multinationals can reduce their costs by applying standard processes throughout the corporation for handling data [23].

The same protection provided for customer information can guard sensitive company information, such as trade secrets and intellectual property [21]. By recognizing and acting upon its duty to ensure privacy of personal information, a firm can enhance its reputation, both internally (with employees and the board of directors, for example) and externally (with customers, regulators and the media, among others) [21].

Building trust can lead to competitive advantage, particularly if competitors are not seen as being as trustworthy and the attributes that lead to trustworthiness are difficult to imitate [24]. Organizations that are viewed as legitimate are more likely to be perceived as trustworthy [21], which will lead to customers having fewer privacy concerns and being more willing to provide personal information [25]. In addition, customers may be willing to pay a premium for privacy [26] and be more amenable to marketing if the firm is open about its policies, minimizes its requests for information, and collects only what is relevant [27]. A firm that truly embraces privacy does more than just create a privacy policy: it creates a culture of privacy within the organization through leadership, training, regular audits and by considering privacy for every new use of personal information [21; 28].

Frameworks can be used to analyze the strategies and behaviors of firms in respect of informational privacy. Established frameworks which inform this research include: the institutional approach and resource-based view [17], customer information privacy framework [6], and the organizational privacy strategy framework [7].

The first combines two paradigms: the institutional approach paradigm, which considers the role information privacy plays in either achieving firm survival through compliance with external forces, and the resource-based view paradigm, which looks at how firms can use their resources to pursue sustainable competitive advantage. The second, the customer information privacy framework, looks at a firm's privacy strategy using two dimensions: whether the company sees privacy as a risk or an opportunity, and whether the company's information management activities focus on internal or external processes and stakeholders. The third, the organizational privacy strategy framework, blends two frameworks, one of which looks at the organization's response to institutional pressures, while the other examines how proactive the organization's strategy is.

Each of these frameworks can be used to analyze the strategies and behaviors of firms in respect of informational privacy. Themes identified in them were used to prepare an interview guide and analyze the collected data.

The institutional approach paradigm suggests that the firm's primary goal is to survive by achieving legitimacy [17]. There are several forms of legitimacy: *pragmatic* (meeting the self-interested expectations of an immediate stakeholder, such as a customer); *social/moral* (considering actions in light of their effect on society); *managerial* (establishing managerial authority and structure); and *technical* (focus on the core activities of the firm). An organization's privacy practices help it to achieve a particular type of legitimacy.

On the other hand, according to the resource-based view paradigm, a firm strives for competitive advantage based on strategic differentiation. This can be done by two means. It can choose to treat information as an intellectual/knowledge resource to be mined for insight into its customers, and thus collect as much of it as possible. Alternatively, it can treat information as a social/relationship resource to be used to nurture superior customer trust; this is done by collecting less information than its competitors or collecting as much but paying much more attention to how it is gathered and used, the means by which and how well actions are conveyed to customers, and the extent to which privacy practices are established in order to protect customers.

Ultimately, the organization and consumer are heavily intertwined when it comes to information privacy. They both face numerous complexities and challenges when making decisions about it, and to fully understand these factors a transdisciplinary view on the topic is required [29].

C. The PoPI Act

In South Africa, privacy is recognized as a right in terms of common law and the Bill of Rights of the Constitution of the Republic of South Africa (chapter 2, section 14), though it is not viewed as an absolute right: it may be limited by laws and must be balanced with other rights [30]. The origin of the act is a South African Law Reform Commission discussion paper entitled Privacy and Data Protection, which was published in 2005 after an investigation that lasted several years [30]. In this paper, the authors proposed draft legislation that later became the PoPI Act.

The investigation recognized the need for legislation to govern information privacy: since the collection of personal information was being allowed by law, "the fairness, integrity and effectiveness of such collection and use should also be protected" [30]. In addition, since many countries were implementing laws to govern trans-border information flow, privacy was becoming a trade issue and having legislation would ensure that South Africa could participate in the global market [30]. The importance of data privacy legislation to trade has increased even more since the investigation: as of 2013 over 100 countries have enacted privacy laws and several others have official bills which have not yet been enacted [4].

The PoPI Act defines personal information as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person" [3]. Furthermore, it defines special personal information as "religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information" [3]. Processing of special personal information is subject to more restrictions than that of general personal information.

The PoPI Act will apply to any organization, public or private, that processes personal information. It is possibly one of the most comprehensive pieces of legislation of its type in the world [5]. Given this, becoming fully compliant will take time and effort.

III. Research Methodology

This research follows the pragmatist paradigm. The project had a positivist element, in that existing theories were used as a base for the research, but the research was performed using an interpretivist approach using qualitative methods. These methods involved endeavoring to understand the points of view of research subjects, considering each one's role and work environment, and applying the researcher's own experiences and knowledge of such environments and the research topic. Theory is used to construct a conceptual framework for the research, rather than being used to construct hypotheses to be tested using quantitative methods, and the researcher can then "compare the patterns of the conceptual model with the patterns of the findings they construct from data" [31].

A. Research Method

The research was conducted using the case study method. A case study "examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations)" [32]. The research used multiple case studies – specifically, a holistic multiple-case study where a sample of companies was involved in the research and the findings at each company comprise a case study (the unit of analysis is the organization). The aim was to understand the similarities and differences between cases [33] and improve the generalizability of the results [34; 35].

B. Sample

The target population was the financial services industry – banks, credit providers, asset managers and insurance companies. More specifically, corporate companies were targeted for this research project. The rationale of the choice is that financial institutions around the world have been under intense scrutiny and pressure to reform after the 2007 global financial crisis. Much of this pressure is coming in the form of more stringent regulations that focus on supervision and compliance [36].

In 2008, the International Monetary Fund and World Bank assessed South Africa's financial system. Despite South Africa's reputation for having an effective financial regulatory framework, it still needed reform to "prioritize and strengthen both prudential and market conduct supervision and regulatory powers" [37]. Because of this, new legislation in the form of the Financial Sector Regulation Bill was drawn up, a second draft of which has been released for public discussion [38].

Given the current state of the global financial environment and the growing amount of regulation, South African financial

services corporates are very sensitive to new legislation and are therefore very likely to be considering the effects of PoPI and instituting or modifying privacy strategies. Given how comprehensive the PoPI Act is, as well as the fact that organizations struggle with change [39] and the complexity of IT projects [40], it is likely that many PoPI-compliance projects must have already begun as it is probable that they would take a long time to design and implement, and organizations are only allowed one year of grace once the Act has commenced. In addition, the fact that corporates are among the major users of private data because of their size [30], together with the financial difficulties of many consumers, particularly with debt [41], increases the possibility of them being amongst those who have the earliest PoPI-compliance complaints laid against them.

The participants have an intimate knowledge of their companies' privacy strategy and willingly participated in the research. The sample comprises five companies of stature. Two persons were interviewed at three of the companies and a single person was interviewed at the remaining two. The sample was bounded by resource constraints and priority was placed on accessing knowledgeable participants. The interviewee profiles are summarized in Table 1.

TABLE I. INTERVIEWEE PROFILES

	Job Description	**Experience in Position**
A1	Management of retail partner accounts at a national level.	17 months. Previous management position at the company: over 2 years.
B1	Head of information security. Responsible for information security strategy development.	Over 6 years.
B2	Advises on legislation compliance within the company.	Over 5 years.
C1	Information protection officer – oversees and encourages company compliance with information protection principles.	Over 5 years.
C2	Accountable for the company's data and data management; previously chaired the company's PoPI implementation project.	Over 6 years.
D1	Information security officer.	Over 2 years.
E1	Management of IT security and business continuity.	Over 4 years.
E2	Project manager for the company's PoPI project.	Unknown. Has been at the company for over 7 years.

C. Data Collection and Analysis

Ethical approval for the research was obtained before proceeding with data collection. The "responsive interviewing" technique [42] was used. The aim of this technique is to develop an understanding of the interviewee's point of view, rather than simply obtain information through short, simple or general responses to questions – the interviewer is looking for rich, detailed information. The interviews were semi-structured in nature and based on a set of prepared, open-ended questions in the form of a guide. While this guide was intended to provide some structure to the interview and direct the conversation, it was not intended to be a rigid protocol – it allowed for the interviewee to voice opinions and raise topics in addition to the questions [43]. Each interview was audio-recorded and transcribed in its entirety. Some of the subjects provided documents as supplements to interview data, and these clarified answers or provided extra detail. Information provided on the subject companies' websites was also examined and included in the analysis.

The collected data was analyzed using thematic analysis, which is a "method for identifying, analyzing and reporting patterns (themes) within data. It minimally organizes and describes your data set in (rich) detail. However, frequently [it] goes further than this, and interprets various aspects of the research topic" [44]. To assist in the analysis process, computer aided qualitative data analysis software (NVivo version 10) was used. The findings are presented in the next section.

IV. RESEARCH FINDINGS

This section presents the empirical data and findings of the study. Each subject company is treated as a separate case study. The findings of the interviews are broken down into three major themes: informational privacy strategies, the customer and the PoPI Act. Lastly, the findings are summarized to determine which informational privacy strategy are being applied by the companies.

A. Organization A

This firm operates in South Africa and two other African countries, providing credit facilities in the form of retail store cards and personal loans. It has between 1,000 and 5,000 employees and is a private company.

1) Information Privacy Strategy

Company A's goal in its approach to information privacy is a mixture of survival and competitive advantage: the firm needs to protect itself from fraud, which can be extremely costly, but customers also need to be able to trust that the organization will protect their information and thus be convinced to use its services.

The role of the firm's informational privacy strategy is to achieve all four forms of legitimacy. The interviewee mentioned that "it is the balance between using the customer data to achieve the profit objectives of the business while still operating with[in] the constraints of the law and in service to our customers. We also have a further responsibility to our retail partner who also has an interest in the customer data as they are our mutual customer". They added that gathering information to enable "big data" is a driving force in many businesses, particularly retail ones – hence the "spate of recent loyalty and customer reward programs where the main driver is the gathering of data to gain insights into the customer" (interviewee A1).

The organization's privacy activities focus on both internal and external stakeholders and processes. Internally, they deal with how customer information and accounts are handled.

Externally, it addresses the way customer information is managed in their retail partners' stores – for instance, the handling of documents such as application forms.

Privacy is seen by the organization as being a risk, not only because there is the potential to commit fraud using customer information, but also because being forced to collect less data makes it harder to obtain new customers and refine and enhance the company's product and service offering. The interviewee doesn't see much potential for major opportunities, other than perhaps through finding creative ways within the boundaries of the legislation to get broad consent from the customer to collect and use their information.

2) Impact of the PoPI Act

The firm's privacy strategy has changed in some ways because of the introduction of PoPI. There is now more of an audit trail in its information gathering operations and access to information is being restricted to relevant users. Its information gathering process is also being scrutinized to capture the specific purpose each piece of information is required for. Overall, it is taking preparatory steps and not aiming for full compliance at this point.

The need to get specific consent for the use of data is a challenge from a commercial point of view. From an operational perspective, the need to be able to audit the gathering and usage of data is complicated. The interviewee sees no benefits to the changes brought about by PoPI, though they did also mention that it may limit the number of non-compliant credit companies, making it easier for the compliant ones to more easily market to customers ("at the moment there is a lot of noise") and provide more benefit to them.

B. Organization B

Organization B has between 1,000 and 5,000 employees and has operations in many countries around the world. It provides investment and asset management services. It is a privately held company, though its parent company is listed on two stock exchanges.

1) Information Privacy Strategy

While interviewee B1 suggested that this organization's goal in its approach to information privacy appears is more about survival than competitive advantage, interviewee B2 said it's a mixture of both. Both interviewees highlighted that it is important to be able to assure customers that their information is protected, as well as meet regulatory requirements. Interviewee B2 also mentioned that the firm's reputation is involved, particularly because of the legislative requirement to disclose breaches.

When asked what role the company's information privacy strategy plays in achieving this goal, both interviewees answered that all four of the forms of legitimacy are applicable. Interviewee B1 wrote: "we always need to balance what information we gather from the client to gain insight vs. what our regulators allow. The approach is always conservative i.e. only gather the information you need. This also applies to internal staff information. We are in the business of looking after clients' assets, so trust is a huge factor. We can't afford to lose this trust by being reckless or morally irresponsible with their information". This statement does imply, however, that intellectual differentiation is not as important as the others, and this view is reinforced by interviewee B2, who said that while it's good to have customer feedback, the firm is not as product-driven as a business focused on sales.

Company B's privacy activities focus on external stakeholders, particularly customers and regulations. As interviewee B2 explains, the aim is to make sure that customer information is relevant, up to date and protected, as well as to ensure that processes conform to legislation. Interviewee B1 mentioned that because a significant portion of the firm's back office is outsourced, it's particularly important to ensure that vendors and outsource partners comply with regulations, as the firm is seen by regulators as being the owner of that data.

Interviewee B1 sees privacy as being a risk, whereas interviewee B2 sees it as being both a risk and an opportunity. Interviewee B2 explained that there's regulatory risk and the possibilities of information leaks, fraud and so on, but there's also the opportunity to improve the customer experience by having accurate and up-to-date information and being allowed to evaluate it. They went on to say that it is also an opportunity because the firm has good security processes in place, which could make it more attractive to do business with, particularly seeing as it applies these same processes across all its international operations.

The firm reviews legislation and assesses its impact on the company, but it generally does not implement any changes until the legislation becomes more final. The reason for this is explained by interviewee B1, who said that sometime legislation is not implemented, which means that resources expended on preparing for it are wasted. PoPI, however, was an exception: not only has it existed for several years, but its core principles are based on established legislation in other countries – such as the United Kingdom – and thus unlikely to change, according to interviewee B2.

2) Impact of the PoPI Act

In interviewee B2's view, the key change to the company that the PoPI Act has brought about is greater awareness of privacy and the protection of personal information. While people within the firm did act to protect customers, there was never the sort of emphasis on it that PoPI has brought about. Little has changed in terms of its practices though, as interviewee B1 said that the Act is very similar to or even less onerous than legislation in other countries with which the firm is already complying.

The Act does have some challenges though. Its principles are of some concern because they are open to interpretation. The firm has tried to gauge the intention of each area of PoPI and act based on this assessment. Interviewee B2 acknowledges that when a Regulator is established and regulations are established the firm may need to make some adjustments. However, they also point out that principles should allow for leeway, and they hope that PoPI will not be heavily rule-based, as the Financial Intelligence Centre Act (FICA) is.

One benefit of PoPI compliance is that it can be marketed to South African customers to reassure them that their sensitive

information is being protected. While the company does say that it complies with the UK Data Protection Act, it would be more meaningful to be able to advertise that the firm complies with local law. It could also market its compliance outside of the country, particularly seeing as international customer data is processed in South Africa. Interviewee B2 believes that the company is a more secure business: the firm is more conscious of what customer information is being collected and how it is being and can be used, and more aware of the risks to the company if this information is compromised.

C. Organization C

This global organization has more than 10,000 employees and offers financial planning and advice, insurance, retirement planning and banking services. It is listed on two stock exchanges.

1) Information Privacy Strategy

The goal of Company C's approach to information privacy sits somewhere between survival and competitive advantage, according to the interviewees. Interviewee C2 said that it's about "the freedom to operate". Interviewee C1 explains that the company wants to be an organization that operates in a responsible manner, particularly with respect to data management, "so that the people know that when they give their data to us we'll look after it properly, we'll secure it, you know we won't share it". Interviewee C2 echoed this view, stating that the reputational damage that will get done to their brand if their lost customer information is more important than fines from the Regulator. However, the company also wants to avoid adversarial relationships with any of its regulators, according to interviewee C1, and it hopes to create a good one with the PoPI regulator when it is established.

Both interviewees said that the role that the firm's informational privacy strategy plays is a combination of the four types of legitimacy suggested by theory. Their ranking of the types was similar in that they listed intellectual differentiation and pragmatic legitimacy as their top priorities, but while as interviewee C1 didn't think that social legitimacy plays a role but that relationship differentiation does, interviewee C2 sees them both as playing a role, with the former ranking higher than the latter. Interviewee C2 emphasized the importance of data to the company several times during the interview. The focus of the company's information privacy activities appears to be internal stakeholders and processes. Interviewee C1 said that both are the focus, but then spoke at length about internal matters. Interview C2, on the other hand, stated that the focus is internal.

According to interviewee C1, whether privacy is seen as risk or an opportunity by the company depends on who you ask. They went on to say that "with the nature of my role, I see it as a risk because I need to ensure that everything is going right and I don't want to have breaches ... But I think it's also an opportunity to get it right and customers … know that we take the protection of personal info – of their information – seriously and … we really want to get it right, then I think they'd be inclined to give their data to us rather than a competitor that's not known for the same thing". Interviewee C2 believes it's "somewhere in the middle", later adding: "I wouldn't have said it's an opportunity for our business, but if our construct allows us to cross sell easier than [our] competitors then [we] have got strategic advantage".

The organization "tends to be an early mover in responding to regulations", according to interviewee C2, and implements draft legislation before its competitors, which is a disadvantage. However, according to interviewee C1, the company usually waits until legislation is in a final draft form before implementing it. When the company receives new legislation people within the firm analyze it and determine the impact, assess it to see which parts make sense and which do not, determine whether or not the company agrees with it, and provide feed via the firm's industry body or, on occasion, directly to the regulators. The firm did work ahead for PoPI, though: it started performing a gap analysis in 2007 and completed this in 2009, and then in 2010 it started implementing changes. The reason for starting so early is given the size of the company it would not be able to become compliant in the stipulated year of grace from the date that the Act commences.

2) Impact of the PoPI Act

There is far more focus on Company C's information privacy strategy now because of PoPI, and it has become more formalized. Interviewee C1 stated: "previously it was an over-arching statement somewhere ... [it] got lost between all the other policies; there was not a dedicated, focused approach as there is now. So, yes, it was an over-arching principle without any real meat or flesh underneath". They added that there is far more awareness, focus and action around PoPI currently, as it's being seen as a competitive advantage if you get it right. It's now being applied on a more practical level and, according to interviewee C2, with more consistency – whereas before business units would have implemented policies were implementing with different levels of strictness, the implementation is now more standardized.

It is also being focused on at a board level, partially because of the risk to the company's reputation – Company's C brand is very important to it. Risks at Company C are quantified financially using a risk matrix; the risk of a data breach carries with it a brand impact with a very substantial value and this damage can be caused by "one breach, just one customer, anywhere, because of his ability to share it and then do brand damage to our core business" (interviewee C2). Interviewee C2 used this high risk to push the PoPI project within the organization and ensure that it was given attention by senior executives.

The biggest challenge in implementing PoPI is the size of the organization and the scale of its operations. The firm has several thousand vendors, all of whom needed to be assessed in terms of their access to personal information, even though the majority have neither need of nor access to such information. Contracts needed to be put in place where they were missing or, when extant, amended with data protection paragraphs or annexures. Interviewee C1 said it is not enough to just have a contract though; a due diligence audit must be regularly performed on each vendor – a future issue because the firm does not have the resources to send teams to all its vendors. To

try to deal with this, each vendor is being given a risk rating to inform the type of audit that will be done on each, with higher risk vendors being given more rigorous and regular attention than lower risk ones.

Condition 7 of the PoPI Act, which governs security safeguards, is having a big impact because of its scope. The organization has implemented and is still implementing several security measures, including the disabling of USB ports, the installation of e-mail sniffers, the encryption of laptops, and the changing of the asset management process to include the reporting of possible breaches – an important step given that, according to interviewee C1, the firm has several thousand employees "out in the field". Interviewee C1 said the breach reporting process has taken two years to implement because of the size of the organization and continuous communication and training required to ensure that employees, both new and current, are kept aware of it.

The firm has several hundred systems and it was an immensely complex task to determine which systems use what data. One area of uncertainty is the length of time for which data can be kept. The firm has had incidents where it has had to retrieve data from as far back as 21 years, so it is not clear exactly what the cut-off period should be. A final challenge, mentioned by interviewee C2, is one of "over-compliance" where one unit will not share information with another, citing PoPI as the reason sometimes simply as an excuse to retain sole possession and control of this information.

An advantage of implementing PoPI is once the necessary consents and disclosures are in place, it is possible to do marketing, cross-selling and up-selling within the firm (across its business units). The hope is to be able to do more effective marketing by targeting customers who are interested and able to afford the products. Interviewee C2 explains: "at an industry level, if the marketing is more appropriate and if the consumers who are getting marketed to truly want to opt in and therefore are more likely to buy, then there will be a lot less waste in the industry – both marketing activity waste, as well as process waste, and in fact waste for the customer who doesn't go the duration and therefore loses that value." Another benefit, mentioned by interviewee C1, is that certain processes within the firm have been improved.

D. Organization D

Organization D has between 500 and 1,000 employees, operates in various countries around the world, and provides tax, investment and legal services. It is a privately held company.

1) Information Privacy Strategy

Company D's goal in its approach to information privacy is a combination of both survival and competitive advantage, as the company wants to comply with regulations, but having a mature privacy strategy also creates competitive advantage. The role of its informational privacy strategy is in social / relationship differentiation – "we need to ensure we have our client's trust and that data privacy is a priority for the company", and the focus of its information privacy activities are external stakeholders, customers and regulations. The company ultimately views privacy as a risk.

The organization is proactive in its handling of legislation. Several of its employees are involved in industry bodies where legislation is reviewed and they facilitate subsequent in-house discussion of this material. In the case of PoPI, its preparations have been made well ahead of the Act's impending commencement and external auditors have said that the firm is further along than many other companies. The company does not oppose legislation, but rather simply implements it.

2) Impact of the PoPI Act

The Act has affected the firm in several ways: implementing the technologies and support for them has had a financial impact; new security has been implemented because of the Act; and employees are being made aware of PoPI and in future will be trained on how to comply with it (the company is still preparing its online training material).

When asked which sections of PoPI are proving to be the most challenging to comply with and why, the interviewee stated before answering that they deal primarily with the security sections of the Act (under Condition 7), particularly technology and safe-guarding, thus limiting their answers to this area. The change of technology is troublesome because it affects computing performance (encrypting and decrypting data can take time) and persuading people in the company to accept this can be challenging. An example of the performance impact is the generation of reports may now take longer. Implementing an incident response process (to handle, for example, a data breach) has been a challenge, and data masking and making data anonymous in a development environment is complicated and something the development team must adjust to. Finally, finding skilled people to perform the technical work can be difficult.

Implementing the PoPI Act does have some advantages. The improved security has led to fewer "attack vectors" (opportunities for the computer systems to be penetrated by a malicious party). It has also allowed the firm to better assure its customers that their data is protected. It also allows for the possibility of offshoring, which could bring work into South Africa (particularly seeing as South Africa has a lower cost of labor than some other countries). A possible future benefit may be PoPI compliance certification, should this ever be created.

E. Organization E

This organization is a privately held company and offers investment and asset management services. It operates world-wide and has between 500 and 1,000 employees.

1) Information Privacy Strategy

The goal of Company E's privacy strategy is neither survival nor competitive advantage, according to both interviewees. The company is driven by doing what is best for its clients and it is vital to the firm that client trust is maintained. "We've got a core set of values that we aspire to as a business and … all those values that we have really in the end build up to the trust that our clients have with us. That's the most important thing for us, and for us as organization if a client loses their trust with us then we don't have anything", said interviewee E1. Interviewee E2 adds that "to look after people's information so that it doesn't get into the wrong hands or it's not used incorrectly even by people at Company E, is the

right thing to do". The interviewees said that the organization's information privacy strategy is a source social legitimacy and relationship differentiation, the former relating to "doing the right thing" and the latter to the emphasis on maintain customer trust.

The firm's privacy activities focus on both internal and external parties and processes. On the internal side, it's improving digital security, polishing client-facing documents, and assessing non-technical activities, such as how information is handled when it's in a physical form. On the external side, the customer is at the center of it all, but third parties are also a major focus: the organization is working to standardize the management of vendors across the company, which includes improving the rigor of contracts with these parties, and analyzing how data is shared with vendors and brokers.

Interviewee E1 mentions that whether privacy is seen as a risk or an opportunity depends on who one speaks to in the company. This was demonstrated in the two interviews: while interviewee E1 sees it as an opportunity to build trust and improve, interviewee E2 views it as a risk to be dealt with to the best of the business's ability.

The firm's approach to legislation depends on what it is. Interview E2 explained that the firm judges some legislation to be more important than others, and depending on this judgement it is either proactive or follows others in the industry. In the case of PoPI, the organization is content with being a follower. It is assessing the likely impact thereof and determining what changes it needs to make, but it is no rush to make these changes: some it is implementing now, others will be implemented after the Regulator has been established and the Act has commenced. Interviewee E2 has the view that the industry that Company E operates in is not "guilty of abusing information anywhere" and therefore not one of the key targets of PoPI.

2) Impact of the PoPI Act

The PoPI Act is not bringing about any major changes to Organization E's informational privacy strategy – "we're happy with the path that we've taken, with the decisions that we've made, with the things that we do to secure information. We haven't made any radical or new decisions to do things differently" (interviewee E2). However, it has pushed the firm to look at how it manages third parties, work it has wanted to carry out for some time now. This includes creating a register of the third parties, assessing whether they receive information and how sensitive it is, categorizing them according to risk, and then assessing their approach and security to align them with those of Company E. During the year after the Act has commenced, the firm will put its preparation into action and ensure that the third parties comply.

Dealing with the issues of third parties has been challenging because of the amount of work involved. The subject of data retention is also an issue: it is not clear how long data can or should be held for (the Act doesn't stipulate). The company has several examples of where it has had to retrieve data from up to 15 years ago to defend its actions against someone, so instead of deleting old and historical information it is instead restricting access to that information.

Having data protection legislation that's equivalent to that of other countries will allow for information from those countries to be sent to South Africa. This will benefit Company E in the long term when it tries to do business with more international companies.

F. Discussion of Findings

PoPI has influenced all the subject companies to some degree. Even those who have been operating using their self-defined privacy policies and practices for many years are being pushed to assess their strategies and routines, though they may not yet be implementing changes to achieve full compliance. For many, PoPI has brought privacy and the management of personal information to the fore, creating greater awareness and spurring action.

Though the sample for this research is relatively small, it is clear that South African organizations in the financial services industry employ a range of strategies. There are many reasons for this: whether the company views privacy as a risk or an opportunity, its culture, its size, its perceptions of the importance of privacy to its customers and consumers in general, whether or not it sees benefit in applying privacy practices – all of these and many more aspects affect an organization's strategic approach to privacy and managing personal information.

Of the five companies interviewed, the goals of four in their approach to information privacy are a mixture of survival and competitive advantage, though Organization C's approach can be interpreted as actually being competitive advantage. For Organization E, it is neither. Four of the organizations believe that their strategies are sources of all the forms of legitimacy, though in some cases they provide evidence of certain forms being more important. Two of them focus on both internal stakeholders and processes, one has an internal focus, and the remaining two have an external focus.

Whether privacy is seen as a risk or an opportunity generally depends on who you ask in the company (as evidenced by the contrasting responses of the interviewees of organizations C and E), and sometimes it is seen as both. All the companies are members of influential industry bodies and provide feedback on legislation through those bodies. They are also all proactive in their approach to assessing the impacts of legislation on their organizations, but, depending on the particulars of a piece of legislation, only some extend this proactive approach to implementing changes in actuality.

The Act poses a fair number of challenges. Perhaps the greatest of these lies in it being principle-based and relying on interpretation, which is leading to it not being applied with consistency across organizations. Some companies are taking a "wait and see" approach for some parts of the Act until the Regulator proposes regulations or the first major cases of non-compliance are dealt with by the Regulator. Until then each industry, and even each company, may have to interpret PoPI to the best of its ability. Two specific, notable challenges around interpretation are the issue of data retention, where it is unclear how long data should be kept (especially given that companies can be forced to address issues from decades ago), and the management of third parties, where it is uncertain how

much effort companies must put into ensuring the compliance of their vendors and partners. Several practical difficulties were also mentioned by the interviewees, including how the size of a company and its operations can influence the implementation of changes and cause delay; getting people in the organization to accept changes can be problematic; and installing new security technologies can impact budgets and the performance of processes.

Most of the companies do see benefits to PoPI though. Compliance can potentially be advertised to local and international markets to reassure existing customers and possibly attract new ones, particularly in the case of sophisticated international customers who may be unwilling to deal with countries that do not have comprehensive privacy legislation. It also offers the opportunity and motivation to improve processes and security measures throughout. Finally, future marketing should be more effective as customers must give consent for it because they are interested in receiving product and service offers, thus reducing wasted effort for the company and irritation for the customer.

V. Conclusion

This paper provides insight into information privacy strategies employed by South African organizations in the financial services industry, finding a range of strategies being employed. There are many reasons for this, including whether the company views privacy as a risk or an opportunity, its culture, its size, its perceptions of the importance of privacy to its customers and consumers in general, and whether it sees benefit in applying privacy practices.

The introduction of PoPI has prompted companies throughout, including the financial services industry, to assess their privacy and personal information management practices, which are directed by their information privacy strategies. PoPI has influenced the companies to varying degrees: some are assessing the impacts it will have and preparing to implement changes after they have done so, while others have been making changes for many years. The Act imposes several challenges to the firms, perhaps the most important of these being that it is based on principles and therefore open to interpretation. However, for most of the organizations it appears to offer benefits, such as the opportunity to bring more international business to South Africa.

References

[1] S. Trepte and L. Reinecke, Privacy online: Perspectives on privacy and self-disclosure in the social web. Springer, 2011.

[2] J. H. Moor, “Towards a theory of privacy in the information age,” Computers and Society, vol. 27, no. 3, pp. 27–32, 1997.

[3] Protection of Personal Information Act (Act No. 4 of 2013). 2013. Government Gazette, vol. 581, no. 37067.

[4] G. Greenleaf, “Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories,” Journal of Law, Information & Science, vol. 23, no. 1, p. 4, 2014.

[5] B. Burmeister, “Pay attention to the Protection of Personal Information Bill,” Finweek, p. 7, 06-Mar-2014.

[6] K. E. Greenaway and Y. E. Chan, “Designing a Customer Information Privacy Program Aligned with Organizational Priorities.,” MIS Quarterly Executive, vol. 12, no. 3, 2013.

[7] R. F. Parks and R. T. Wigand, “Organizational privacy strategy: Four quadrants of strategic responses to information privacy and security threats,” Journal of Information Privacy and Security, vol. 10, no. 4, pp. 203–224, 2014.

[8] J. H. Moor, “Using genetic information while protecting the privacy of the soul,” Ethics and Information Technology, vol. 1, no. 4, pp. 257–263, 1999.

[9] H. T. Tavani, “Informational privacy: Concepts, theories, and controversies,” The handbook of information and computer ethics, pp. 131–164, 2008.

[10] A. F. Westin, “Privacy and freedom,” Washington and Lee Law Review, vol. 25, no. 1, p. 166, 1968.

[11] H. T. Tavani, Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology, 2nd ed. Wiley, 2007.

[12] R. O. Mason, “Four ethical issues of the information age,” MIS Quarterly, vol. 10, no. 1, pp. 5–12, 1986.

[13] H. J. Smith, S. J. Milberg, and S. J. Burke, “Information privacy: measuring individuals’ concerns about organizational practices,” MIS Quarterly, vol. 20, no. 2, pp. 167–196, 1996.

[14] D. J. Solove, The digital person: Technology and privacy in the information age. NYU Press, 2004.

[15] S. Conger, J. H. Pratt, and K. D. Loch, “Personal information privacy and emerging technologies,” Information Systems Journal, vol. 23, no. 5, pp. 401–417, 2013.

[16] M. Nofer, O. Hinz, J. Muntermann, and H. Ro\s snagel, “The economic impact of privacy violations and security breaches,” Business & Information Systems Engineering, vol. 6, no. 6, pp. 339–348, 2014.

[17] Y. E. Chan and K. E. Greenaway, “Theoretical explanations for firms’ information privacy behaviors,” Journal of the Association for Information Systems, vol. 6, no. 6, p. 7, 2005.

[18] A. Acquisti, A. Friedman, and R. Telang, “Is There a Cost to Privacy Breaches? An Event Study,” in 5th Annual Workshop on the Economics of Information Security, WEIS 2006, Robinson College, University of Cambridge, England, UK, June 26-28, 2006, 2006.

[19] M. Ko and C. Dorantes, “The impact of information security breaches on financial performance of the breached firms: an empirical investigation,” Journal of Information Technology Management, vol. 17, no. 2, pp. 13–22, 2006.

[20] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, “The economic cost of publicly announced information security breaches: empirical evidence from the stock market,” Journal of Computer Security, vol. 11, no. 3, pp. 431–448, 2003.

[21] M. J. Culnan and C. C. Williams, “How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches,” Mis Quarterly, pp. 673–687, 2009.

[22] N. J. King and V. Raja, “Protecting the privacy and security of sensitive customer data in the cloud,” Computer Law & Security Review, vol. 28, no. 3, pp. 308–319, 2012.

[23] P. Blume, “It is time for tomorrow: EU data protection reform and the Internet,” Journal Of Internet Law, vol. 18, no. 8, pp. 3–13, 2015.

[24] J. B. Barney and M. H. Hansen, “Trustworthiness as a Source of Competitive Advantage,” Strategic Management Journal, vol. 15, no. S1, pp. 175–190, 1994.

[25] P. A. Norberg, D. R. Horne, and D. A. Horne, “The privacy paradox: Personal information disclosure intentions versus behaviors,” Journal of Consumer Affairs, vol. 41, no. 1, pp. 100–126, 2007.

[26] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, “The effect of online privacy information on purchasing behavior: An experimental study,” Information Systems Research, vol. 22, no. 2, pp. 254–268, 2011.

[27] J. Phelps, G. Nowak, and E. Ferrell, “Privacy concerns and consumer willingness to provide personal information,” Journal of Public Policy & Marketing, vol. 19, no. 1, pp. 27–41, 2000.

[28] M. J. Culnan and P. K. Armstrong, “Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation,” Organization science, vol. 10, no. 1, pp. 104–115, 1999.

[29] M. Pelteret and J. Ophoff, “A Review of Information Privacy and Its Importance to Consumers and Organizations,” Informing Sci. Int. J. Emerg. Transdiscipl., vol. 19, pp. 277–302, 2016.

[30] South African Law Reform Commission, “Privacy and data protection (No. Discussion paper 109, project 124).”, 2005. Available: http://www.justice.gov.za/salrc/dpapers/dp109.pdf

[31] J. F. Gilgun, “Qualitative research and family psychology.,” Journal of family psychology, vol. 19, no. 1, pp. 40–50, 2005.

[32] I. Benbasat, D. K. Goldstein, and M. Mead, “The Case Research Strategy in Studies of Information Systems,” MIS Quarterly, vol. 11, no. 3, pp. 369–386, 1987.

[33] P. Baxter and S. Jack, “Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers,” The Qualitative Report, vol. 13, no. 4, pp. 544–559, Dec. 2008.

[34] A. Bhattacherjee, Social Science Research: Principles, Methods, and Practices, 2nd ed. 2012.

[35] R. K. Yin, Case Study Research: Design and Methods, 5th ed. SAGE Publications Ltd, 2014.

[36] L. Prorokowski and H. Prorokowski, “Organisation of compliance across financial institutions,” Journal of Investment Compliance, vol. 15, no. 1, pp. 65–76, 2014.

[37] E. Botha and D. Makina, “Financial regulation and supervision: theory and practice in South Africa,” The International Business & Economics Research Journal (Online), vol. 10, no. 11, p. 27, 2011.

[38] G. Jones, “Revised financial regulation bill clarifies ‘twin peaks’,” 17-Dec-2014. Available: http://www.bdlive.co.za/business/financial/2014/12/17/revised-financial-regulation-bill-clarifies-twin-peaks.

[39] S. Rosenberg and J. Mosca, “Breaking down the barriers to organizational change,” Int. J. Manag. Inf. Syst., vol. 15, no. 3, pp. 139–146, 2011.

[40] W. Xia and G. Lee, “Grasping the complexity of IS development projects,” Commun. ACM, vol. 47, no. 5, pp. 68–74, 2004.

[41] N. Maswanganyi, “Debt weighing on consumer finances, index shows,” 11-Feb-2015. Available: http://www.bdlive.co.za/economy/2015/02/11/debt-weighing-on-consumer-finances-index-shows.

[42] H. Rubin and I. Rubin, Qualitative Interviewing, 3rd ed. SAGE Publications Ltd, 2012.

[43] U. Flick, An Introduction to Qualitative Research, 5th ed. SAGE Publications Ltd, 2014.

[44] V. Braun and V. Clarke, “Using thematic analysis in psychology,” Qualitative Research in Psychology, vol. 3, no. 2, pp. 77–101, Jan. 2006.