INFORMATION PRIVACY STRATEGIES OF SOUTH AFRICAN FINANCIAL SERVICES ORGANISATIONS

TECHNICAL REPORT

Marc Pelteret
PLTMAR004

SUPERVISOR_ **Dr Jacques Ophoff**

Presented to the Department of Information Systems of the University of Cape Town in partial fulfilment of the requirements of the Honours Research Project course (INF4024W)

Due: 15 September 2015

DECLARATION

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this paper from the work(s) of other people has been attributed, and has been cited and referenced.
3. This report is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as their own work
5. I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Signature: *Marc Pelteret* Date: *15/09/2015*

Full name of student: *Marc Arthur Pelteret*

Dedicated to Boris, a lively character and loyal companion

Boris

(Unknown – 23 April 2015)

ACKNOWLEDGEMENTS

My sincerest thanks to my interview subjects, who were all very generous with their time. I am particularly grateful that you were prepared to meet with me given how busy the working world and life in general are.

Next, I would like to offer my sincere thanks to my supervisor, Dr Jacques Ophoff, for his guidance throughout this project. It's been a pleasure to work with you and I am very appreciative for of your thoughtful and quick responses to my ideas and questions.

To my family – my parents, Robin and Denise; my brothers, Jean-Paul and Eugene; and my sisters-in-law, Kerryn and Tammy – I say a big *thank you* for all your support. I am particularly grateful for the constant encouragement of my parents – their unwavering belief in me gives me strength.

Finally, I offer a very special thank you to my father not only for proofreading this report, but for pushing me to complete my Information Systems Honours degree. Thanks Dad!

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 and many countries have enacted or are in the process of enacting legislation to govern it.

South Africa is addressing privacy concerns through the Protection of Personal Information (PoPI) Act, which imposes heavy penalties for non-compliance. With the threat of monetary loss and other negative effects, companies are obliged to consider and address privacy concerns.

This project examines the informational privacy strategies of some prominent companies in the South African financial services industry using three frameworks: the institutional approach and resource-based view paradigms, the customer information privacy framework and the organisational privacy strategy framework.

The research was conducted using multiple case studies, with the unit of analysis being an individual company. Data was collected from five companies and through interviews with senior management, then analysed using thematic analysis and themes taken from the frameworks.

Findings suggest that companies in the financial services industry employ a variety of strategies. While many of the subjects’ strategies could be classified under a single approach in the three frameworks, some could not, suggesting that these strategies are hybrids that use elements from two approaches. Opinions were mixed on whether or not privacy is of concern to South Africans, but a belief that awareness of it is growing is sensed. PoPI has influenced the companies 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 of PoPI that was highlighted is that it is based on principles and therefore open to interpretation.

The findings offer insight into the complexities of forming and executing a privacy strategy, as well as the difficulties around complying with legislation such as PoPI.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1.

INTRODUCTION

> *In the end, one of the best law enforcement tools was Google. It seemed clear that Ross had no idea Silk Road would become such a success and was careless early on. And in the era of informational perpetuity, you only have to be careless once.*
>
> *Bearman (2015)*

Whereas we once relied on memories and paper to capture small details, these days information is stored permanently in computer systems. Banking, loyalty and other cards, the Internet, digital devices such as smart phones and tablets are a few of the many means used to track where we are, what we do, what we like, and a myriad of other minutia and personal information. All these details can be used to compile what Solove (2004) refers to as a "digital dossier" on each of us.

In our society we simultaneously seek privacy while having to disclose personal information in order 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 (Trepte & Reinecke, 2011).

The problem is that the same technology that makes it easy to share personal details has also led to what Moor (1997) refers to as *greased information* – data that moves like lightening and is difficult to hold on to. Moor (1997, p. 28) also says: "once information is captured electronically for whatever purpose, it is greased and ready to go for *any* purpose".

As a consequence, the safety of our personal information has become of great importance and a major topic of interest to the business and IT sectors, as well as the general public. Stories focussed on the issues of privacy and personal information have become more numerous and prominent in popular media.

In June 2013, The Guardian published a story on how the National Security Agency (NSA) is collecting the phone records of millions of Verizon customers on a daily basis (Greenwald, 2013). The information came from a document leaked by an NSA contract employee, the now infamous Edward Snowden.

In September 2014, several public celebrities had their personal photographs stolen from Apple’s iCloud service (Satariano & Strohm, 2014). In November 2014, Sony Pictures was hacked and thousands of confidential documents containing the personal and private information of employees and celebrities were stolen and posted online (Brandom, 2014; McCormick, 2014).

RadioShack, an iconic US electronics retail chain, filed for bankruptcy in February 2015. The data it collected on over 100 million customers was sold via auction. This sale is being contested by several parties, one claiming that the data does not belong to RadioShack, several others claiming that the company is violating its own privacy policies (Brustein, 2015). Early in July 2015 it was disclosed that breaches of databases managed by the US government’s Office of Personnel Management had exposed the sensitive information of at least 22.1 million individuals (Nakashima, 2015). Later on in July 2015, Ashley Madison – an online dating website that targets married people – was hacked and personal details on its 37 million users stolen (Krebs, 2015) and in August 2015 these details were released on to the Internet (S. Gibbs, 2015). The released data include the information of several thousand South Africans (Smillie & Child, 2015).

These are only a few examples of stories that are spurring global discussion of privacy and the need for adequate legislation to govern it.

South Africa has recently enacted the Protection of Personal Information (PoPI) Act, the aim of which is to promote the protection of personal information by regulating how organisations handle, store and secure this information (Protection of Personal Information Act (Act No. 4 of 2013)). 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 (Greenleaf, 2014).

Given the introduction of PoPI and the threat of harsh punishment for failing to comply with it, many companies are preparing to become compliant. Prominent amongst these are corporates in the financial services industry, the focus of this research. The aim of this research thus is to determine what informational privacy strategies are used by corporates in the South African financial services industry.

The positioning of this research project will be examined first by looking at its problem statement, its research question and objectives, and the assumptions and limitations of the project.

1.1. Problem Statement

Personal information is one of the key resources of most businesses in today's knowledge-centric society. Because of this, the privacy of this personal information has become an important topic and many countries have enacted or are in the process of enacting legislation to govern it.

South Africa is addressing privacy concerns through the PoPI Act. The Act will affect all companies (Burmeister, 2014), as it applies to all organisations, 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. Given this breadth, the Act will impact financial services companies deeply, as most parts of their business involve information.

The Act imposes stiff penalties for non-compliance, including a fine of up to R10 million or prison time of up to 10 years (or both). It also establishes grounds for civil lawsuits and the awarding of damages. With the threat of such significant monetary loss, as well as other negative effects such as damage to the firm's reputation and lowering of its stock price and market value, companies are obliged to consider and address privacy concerns.

Though the informational privacy strategies of companies have been explored in other countries (Greenaway & Chan, 2013; Parks & Wigand, 2014), no such research has been performed and published on firms in the South African financial services industry.

1.2. Research Question and Objectives

The question guiding this research is: *what informational privacy strategies are used by corporates in the South African financial services industry?*

In order to answer it, the following objectives will need to be met:

1. Investigate the strategies that organisations could employ by reviewing the literature available on the subject.
2. Determine organisations' privacy strategies by establishing how they:
   a. Treat personal information as a resource
   b. View informational privacy
   c. React to institutional pressures (such as PoPI)
   d. Perceive customer informational privacy preferences.
3. Determine the influence of privacy strategy on implementation, particularly with regard to PoPI.

In achieving these objectives and combining the findings, the research question will be answered.

1.3. Assumptions and Limitations

This research was undertaken with the following assumptions:

- A sufficient number of companies that are willing and able to be involved in the project will be found;
- Each company will provide access to interview subjects who are sufficiently knowledgeable about the topic; and
- The interview subjects are based in Cape Town, willing and able to be interviewed, and able to clearly communicate their knowledge.

The project has the following limitations:

- *Time*: The time available for the project was limited and it was not be possible to continue to collect case data until the point of theoretical saturation, the stage where data collection no longer leads to any data that yields new insights (Bhattacherjee, 2012, p. 97).
- *Scope*: The study was limited to corporate companies in the financial services industry. These companies were either be based in Cape Town or had knowledgeable personnel based in Cape Town who could be interviewed, as there was no budget for travel and the project had time constraints.
- *Interpretation of theoretical models*: The project made use of theoretical models that require interpretation by the researcher, which was done to the best of their abilities.
- *Generalisability*: Given the above limitations and the qualitative approach and methods, the results of the research may not be generalisable.

1.4. Structure of Report

The rest of this document is structured as follows. The next section provides the full review of the literature examined for the project. Following this, the research paradigm, approach, method and process, together which make up the research methodology, are examined. In chapter 4 the research findings are detailed, analysed and discussed. Chapter 5 concludes the report, providing a summary of it together with a discussion of the project and some recommendations, including several suggestions for future research. Following this is a list of references and, finally, two appendices.

CHAPTER 2.
LITERATURE REVIEW

In this chapter some literature that informed and helped to shape the project is examined. Addressed is the interrelationship of privacy and personal information, followed by the importance of privacy to both consumers and organisations. Finally, the PoPI Act itself is briefly described and discussed.

The literature review was structured around the advice of Webster & Watson (2002). Initial articles were found through keyword searches using the EBSCOHost and Emerald databases, as well as Google Scholar. Further articles were found by reviewing the citations of some of the literature that was read and perceived to be the most relevant to this project. The Web of Science service was also used to identify more recent literature which has referenced key articles.

2.1. Privacy and Personal Information

Privacy and personal information are intertwined issues in today's world. This section explores these two topics and their relationship by looking at the concept of privacy and several informational privacy theories.

2.1.1. The Concept of Privacy

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" (Moor, 1999, p. 260). It was once thought of as the right "to be let alone" (Cooley, as cited in Warren & Brandeis, 1890, p. 195); at the time, newspapers were the threat, as they were publishing photographs of and statements by individuals without the subjects' consent.

Today, privacy is synonymous with personal information and information technology is seen as the danger.

In our society we simultaneously seek privacy while having to disclose personal information in order to receive services (such as health care and insurance) and establish friendships. Online communication and the Social Web have nurtured in us the habit of sharing large amounts of information with a great number of people, yet surprisingly many do not feel threatened when doing so (Trepte & Reinecke, 2011). As Acquisti (2004, p. 22) puts it:

> *"In an information society the self is expressed, defined, and affected through and by information and information technology. The boundaries between private and public become blurred. Privacy has therefore become more a class of multifaceted interests than a single, unambiguous concept."*

The problem is that the same technology that makes it easy to share personal details has also led to what Moor (1997) refers to as *greased information* – data that moves like lightening and is difficult to hold on to. Moor (1997, p. 28) also says: "Once information is captured electronically for whatever purpose, it is greased and ready to go for *any* purpose". Tavani (2008) breaks down the effect information technology has had on personal privacy 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.

Privacy is a multi-disciplinary issue and therefore has a variety of definitions. Concepts such as secrecy, solitude, security, confidentiality, anonymity, liberty and autonomy, amongst others, are often viewed as part of privacy. Some argue that it can be distinguished and is distinctly separate from these concepts, others argue that it is integral with them (Tavani, 2007b). The matter of its definition is also closely related to the issue of whether privacy should be seen as a right or merely in terms of one or more interests an individual may have (Tavani, 2008).

Westin (1967, p. 7) defines privacy 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". According to him, people need privacy in order to adjust emotionally to inter-personal interactions, and it is a dynamic process (over time, we regulate it to meet short-term and long-term needs) and a non-monotonic function (it is possible to have too little, enough or too much privacy). Westin proposes four states of privacy: *solitude* (being free of observation), *intimacy* (small group seclusion to develop a relaxed relationship), *anonymity* (freedom from identification and surveillance in public), and *reserve* (which is based on the desire to limit disclosures to others, and for others to respect that desire). He also proposes four purposes of privacy: personal autonomy (the desire to avoid being manipulated, dominated, or exposed by others), emotional release (release from the tensions of social life), self-evaluation, and limited and protected communication (setting boundaries by limiting communication and sharing personal information with trusted others).

Tavani (2007a, 2008) lists four views of privacy. *Accessibility privacy*, also called *physical privacy*, is freedom from intrusion into one's physical space. *Decisional privacy* is freedom from interference with one's choices. *Psychological privacy*, also known as *mental privacy*, is the freedom of intrusion upon and interference with one's thoughts and personal identity. Finally, *informational privacy* is having control over and being able to limit access to one's personal information. It this view that is most relevant to this research and some theories about it will be explored in the next section.

2.1.2. Informational Privacy Theories

Floridi (2005) discusses two informational privacy theories: the reductionist interpretation and the ownership-based interpretation. According to the reductionist interpretation, informational privacy is valuable because it guards against undesirable consequences that may be caused by a breach of privacy. The ownership-based interpretation has the view that each person owns their information. The theories are not incompatible, but emphasise different aspects of informational privacy. However, Tavani (2008) argues that though these two theories may be appropriate for privacy in general, they may not be for informational privacy. He suggests that most analyses of issues that affect informational privacy use variations of the restricted access and control theories. According to the restricted access theory, a person has informational privacy when they are able to limit or restrict others from access to information about them. To do so, "zones" of privacy (specific contexts) need to be established. In control theory, personal choice is important and having privacy is directly linked to having control over information about oneself.

Despite their widespread use, Tavani (2008) writes that neither the restricted access theory nor the control theory provide a satisfactory explanation of informational privacy (and he discusses their flaws), though each notes something important about it. A framework that attempts to merge the important of the elements of these theories into a single theory is Restricted Access/Limited Control (RALC) theory.

The RLAC theory stresses that privacy and control are separate concepts. According to Tavani & Moor (2001), "privacy is fundamentally about protection from intrusion and information gathering by others. Individual control of personal information, on the other hand, is part of the justification of privacy and plays a role in the management of privacy".

In the framework, a person has privacy in a particular situation if they are protected from intrusion, interference and information access by others (Tavani, 2007b). Like the restricted access theory, it emphasises the importance of setting up zones that allow individuals to limit the access others have to their information, and like the control theory, it also recognises the importance of individual control. However, it does not build the concept of control into the definition of privacy, nor does it require that individuals have full or absolute control over their personal information in order to have privacy; instead, only limited controls are needed to manage one's privacy. More specifically, the individual has control over choice, consent and correction: they need to be able to choose situations that offer others the level of access they desire – for example, to choose to waive the right to restrict others from accessing certain kinds of information about them – and they need to be able to access their information and correct it if necessary.

2.2. The Importance of Privacy to Consumers

Having explored the concept of privacy, a complicated, multifaceted topic, as well as and a few informational privacy theories, the importance of privacy to consumers will be studied. This section deals with some of the complexity that individuals face when making decisions that affect these areas of concern, and certain issues that can arise from the inadequate protection of consumers' privacy and which may impact on their lives.

There are numerous ethical issues around information, its existence and use. Mason (1986) sums these up as 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?).

Smith, Milberg, & Burke (1996) list four areas of consumer privacy concerns that are very similar to PAPA: *improper access* to personal information, *unauthorised secondary use* of personal information, *errors* in personal information and *collection* of personal information.

Solove (2004, p. 89) echoes the above in stating 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".

2.2.1. Challenges in Privacy Decision-making

Ensuring privacy is a complex decision-making process and may differ from one individual or instance to another. A variety of issues influence decisions regarding privacy and can lead to inconsistencies and contradictions.

People are often treated as highly rational agents, particularly in economic studies. But according to Acquisti (2004), it is unreasonable to expect individuals to be rational when making decisions about their own privacy. Even individuals who genuinely want to protect their privacy may not do so because of the many complexities hidden inside concepts that are difficult to understand, as well as other factors which may affect both naïve and sophisticated users. Specifically, they will face three problems: incomplete information, bounded rationality and psychological distortions.

Economic transactions are often characterised by incomplete or asymmetric information, where the different parties involved in the transaction do not have the same information on it and may be uncertain about certain facets of it. Parties can be differently affected by risk and externalities, particularly the secondary use of personal information – that is, information passed on by the original collector, an event over which the subject (the individual) has no control (Acquisti & Grossklags, 2006). Privacy intrusion and protection are often bundled with other goods and services (Acquisti & Grossklags, 2005). Costs can be monetary but also immaterial (such as switching costs); benefits can be priced or intangible. Privacy calculus – where the individual weighs up the perceived likelihood and magnitude of risks and benefits (Smith, Dinev, & Xu, 2011) – can be extremely difficult to perform because of all of these issues.

Bounded rationality refers to the “inability to calculate and compare the magnitudes of payoffs associated with various strategies the individual may choose in privacy-sensitive situations” (Acquisti, 2004, p. 3). It also refers to the inability to process all the random information related to risks and the probabilities of events that lead to privacy benefits and costs. The “rational man” used in economics is assumed to always be rational and has the ability to process all information; in reality, people do not work this way. Often payoffs may only be determined through actual experience. In addition, many probability values may be almost entirely subjective.

Even if an individual has access to complete information and could process all of it, they may still find it difficult to follow a rational strategy because of psychological distortions that influence their thinking. Acquisti (2004) and (Acquisti & Grossklags, 2005, 2006) give numerous examples. Individuals tend to apply hyperbolic discounting, where they display inconsistency in their personal preferences over time – different discount rates are applied to future events than near ones. Related to this is the tendency to under-insure against certain risks. An individual may have a self-control problem and opt for self-gratification instead of choosing to wait for a future gain of a higher value. Individuals are often loss adverse – they prefer to avoid a loss than acquire a gain – and can suffer from optimism bias, where they incorrectly perceive their risks to be lower than those of others in a similar situation. Social preferences and norms, such as fairness and altruism, can also come into play. How a question is framed can affect how an individual responds to it. Heuristics – a technique that helps learning or problem solving – can guide decisions (an example of this is anchoring, where an individual gives something a specific but maybe arbitrary value, perhaps creating a bias, and then adjusts that valuation when further information becomes known). Further examples can be found in Acquisti & Grossklags (2006).

So, whenever an individual has to make a decision about privacy, they rarely have all the information they need to make an informed choice. But even if they did, it is unlikely they would be able to process all of it – and even if they could, they may well not make a rational decision. The most likely outcome will be the use of a simplified model in the process of making a decision (Acquisti & Grossklags, 2005). The difference between an individual's privacy intentions and their actual behaviour is known as the *privacy paradox* (Nofer, Hinz, Muntermann, & Rossnagel, 2014; Norberg, Horne, & Horne, 2007). An individual may be aware of measures they can take to protect their privacy, but not make use of them (Dommeyer & Gross, 2003).

Conger, Pratt, & Loch (2013) developed a model (Figure 1) that illustrates how complicated it is for an individual to know who will have access to their data after they have shared it. While 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 the individual is uncertain about the outcome of sharing information with a second party and are dependent on the decisions of the latter, trust becomes a factor (Nofer *et al.*, 2014). The trustor will rely upon the trustee if three characteristics are perceived to be met (Bhattacherjee, 2002): ability (the trustee is competent), integrity (the trustee is honest and has moral principles), and benevolence (the trustee intends to do good toward the trustor, acting beyond its own profit motive). Trust is seen as a psychological condition, not a behaviour or choice (Nofer *et al.*, 2014). It is also important to distinguish between initial trust, which is when the parties first meet and interact, and general trust, which develops over time based on experiences between the trustor and trustee (Nofer *et al.*, 2014).

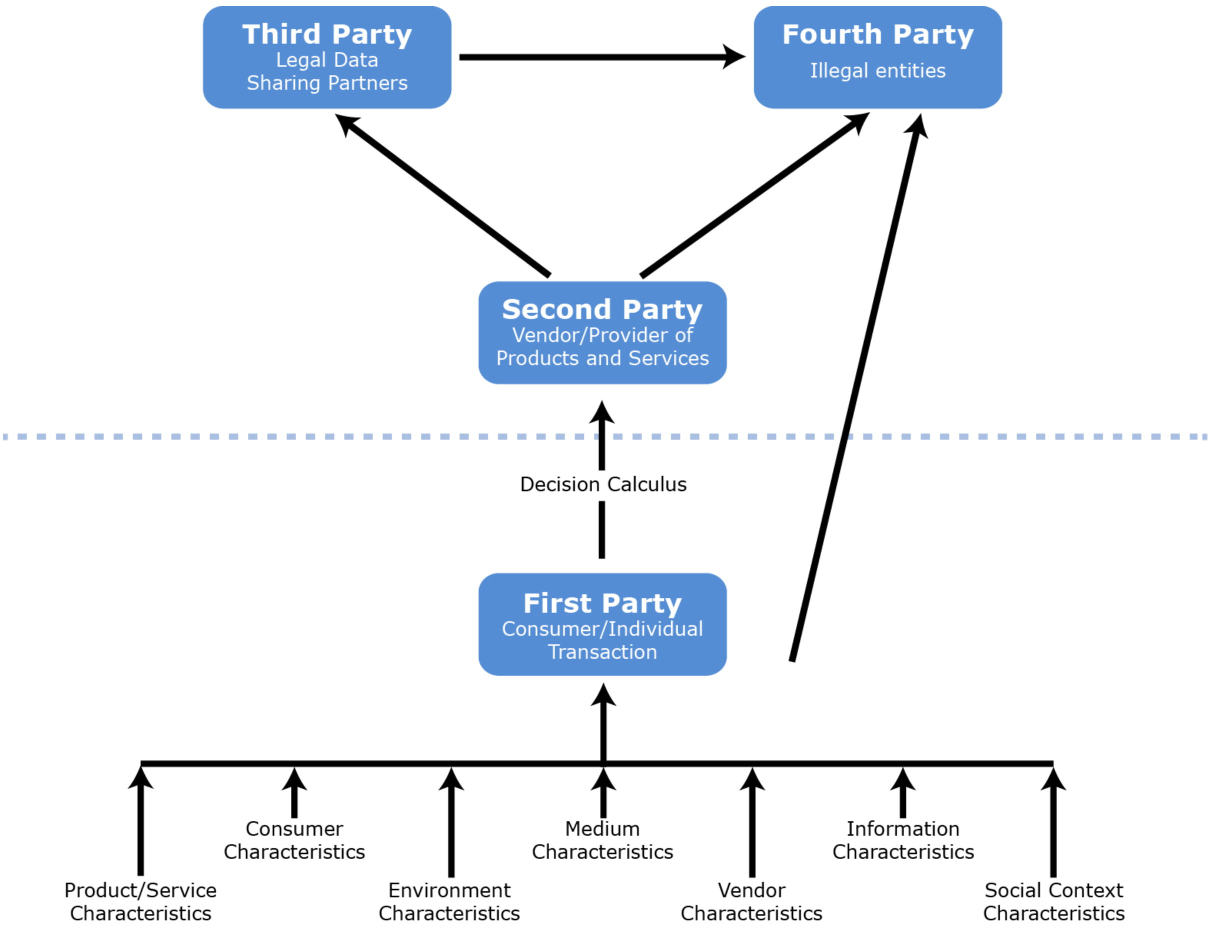

Figure 1: Conger, Pratt & Loch's expanded privacy model (Conger et al., 2013)

2.2.2. Information Privacy Issues

There are numerous issues to do with informational privacy. This section will look at three, each of which serves as an example of issues that can arise from the sharing of personal information and therefore cause concern to consumers while they decide whether or not to share such information.

2.2.2.1. Secondary Use of Information

Secondary use of information is when information about an individual (the buyer) is passed on by the original collector (the seller) to a third party. The issue is that while the buyer and seller have incentives that are more or less aligned, the incentives of the seller and third party are not so well aligned (Varian, 1996). An example of this is the sale of a mailing list, an event that often leads to spam messages.

One method of dealing with this issue is to assign property rights in personal information to individuals, but then allow contracts to be written that would allow the information to be used according to the individual's wishes (Varian, 1996). This would support individuals endeavouring to prevent their information from being resold or provided to third parties without their permission. It would also mean that these property rights could be sold on a market. Such a market already exists, but it is the collector that holds the rights, not the individual. Yet an externality exists and the individual may have to bear costs imposed upon them by the sale of their information.

One problem with property rights lies in determining their value (Hui & Png, 2006). There are two issues with this. First, the individual holding the right may not fully take into account the potential benefit of the information on uninformed parties, which can affect sellers and the overall welfare of society. Second, individuals may attach too high a price to their information and create an excessive barrier to buyers. Economic experiments have shown that people demand a higher price for their property when someone else wants to use it than what they would be prepared to pay to protect it from use.

An alternative approach is the use of opt-in and opt-out systems, whereby when a collector intends to share customer information with a third party they must offer the consumer the opportunity to deny or allow them permission to do so. Degryse & Bouckaert (2006) compared the two cases and a third option of anonymity (where all information collection or storage is prohibited, even within a firm) and found that the opt-out system lead to better societal welfare than the others. They mention that very few individuals opt into or opt out of lists, meaning that an opt-out system effectively permits information sharing and an opt-in prevents it.

2.2.2.2. Identity Theft

According to Anderson, Durbin, & Salinger (2008, p. 171), “identity theft is made possible by the nature of modern payment systems”. Sellers are willing to offer goods and services to individuals they do not know in exchange for the promise to pay. This promise must be backed up a specific account or credit history, which is linked to the individual through data. If someone is able to acquire enough of this data, they can forge the link and enrich themselves at the individual’s expense. While such anonymous transactions have been available for decades through the use of credit cards, trade has become more dependent on ready access to consumer data. This has lowered transaction costs for both consumers and sellers, but has created new opportunities for fraud. Examples include breaches of large databases to obtain such information and phishing, a method of eliciting consumer information by masquerading as a trustworthy entity (such as a bank website).

Identity theft can result in a range of issues, from existing accounts and credit cards being exploited, to misrepresentation (for example, one person posing as another when renting a car), to new accounts being opened in one’s name (Anderson *et al.*, 2008). Often a consumer is not aware of a problem until they apply for credit, check their credit report or receive an account. They then have to expend time, effort and often money to rectify the problem. There may also be indirect costs, such as a consumer foregoing a transaction they would otherwise have undertaken (they may even avoid online transactions altogether).

Ultimately, consumers and firms need decide whether the benefits of a payment system outweigh the risk of fraud. Given this decision, they also need to decide what resources they want to devote to fraud prevention. For individuals, this leads to the difficulty of trying to process all the information surrounding these issues and adequately determining and weighing up the risks. For businesses, the costs of storing and transmitting data have dropped dramatically over time, making it easier to confirm identities and fight fraud, but at the same time this increase in data transmission and flow makes identity theft more appealing (Anderson *et al.*, 2008).

There are various means of combating identity theft. Luong (2006) lists several, dividing them into two categories: legislation and non-legislation. In terms of federal law it is illegal in the United States to commit identity theft; before 1998, it was not considered a crime. There are also consumer data protection laws, which are discussed in Romanosky & Acquisti (2009). Non-legislative means include identity theft registries and the use of biometrics.

2.2.2.3. Data Breaches

Data breaches, such as the ones experienced by Sony and Ashley Madison, are occurring with increasing frequency. According to the Verizon 2014 Data Breach Investigations Report, in 2013 there were 1,367 confirmed data breaches and 63,437 security incidents (Baker *et al.*, 2014). This stolen data can be used in a variety of ways, including being sold to spammers and to perpetrate identity theft.

Breach disclosure has become an important topic for discussion, and in many countries regulation has been implemented to make it mandatory to notify individuals when their personal information has been acquired by an unauthorised party (Moore & Anderson, 2011). These laws are intended to have two effects: to incentivise firms to invest in counter-measures to reduce the possibility of a breach and to help individuals affected by a breach take steps to mitigate the effect of the breach.

Romanosky & Acquisti (2009) explored the three pieces of legislation that exist in United States law to protect consumer data: *ex ante* safety regulation, which is intended to prevent harm from occurring by enforcing minimum standards or operating restrictions; *ex post* liability, which allows victims to hold firms accountable for damages and obtain compensation; and information (breach) disclosure. They found that none of these is better than the others and each has its drawbacks.

Romanosky, Telang, & Acquisti (2011) analysed the effectiveness of data breach disclosure in combating identity theft and found that it marginally reduces the number of incidences. However, they acknowledge that the reduction of identity theft is not the only means by which the laws can be evaluated and that they may have other benefits. Moore & Anderson (2011) note that data leakage by firms is only one cause of fraud, so disclosure laws are only a partial solution.

One often-touted solution to protecting data is encryption, which is meant to act as a disincentive to those who want to steal data and minimise the risk of stolen data being put to malicious use. However, according to (Miller & Tucker, 2010), it does not reduce data loss because many instances are due to negligence or internal fraud rather than external penetration. In fact, encryption can encourage carelessness and give a false sense of security that leads to increased internal fraud. This brings into question the appropriateness of an exclusion law adopted by many states in the US, where if data stolen during a breach is encrypted the loss does not have to be reported.

An individual's reaction to a data breach and the loss of confidential information (and thus privacy) can vary – to some it is inconsequential, to others it is catastrophic. This impacts on how they perceive or understand their risks and the steps they take to mitigate them (Romanosky & Acquisti, 2009). Many of the available measures rely on consumers behaving rationally, but the reality is that they suffer from behavioural biases and transaction costs. Many of the challenges discussed earlier come into play: they have trouble determining what actions they should take because they struggle to process all the available information and determine the risks, the probability of them occurring, and the consequences of any actions they themselves may take based on these assessments. In addition, the cost of their actions might be too high and outweigh the perceived benefit.

While making decisions about privacy, particularly whether or not to share personal information, is difficult for consumers, privacy is important to them. Many issues can arise from the improper use or protection of information and these can influence consumers' privacy decisions. In the next section the importance of privacy to organisations will be examined.

2.3. The Importance of Privacy to Organisations

An organisation manages privacy through its informational privacy programme, 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" (Chan & Greenaway, 2005, p. 173). Fundamentally, a firm can see privacy as a threat to be dealt with or as an opportunity to be taken.

Organisations that view privacy as a threat want to comply with legislation and regulations in order 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. The answer is that there is a negative effect, but it is short-lived (Acquisti, Friedman, & Telang, 2006; Ko & Dorantes, 2006). Furthermore, Campbell, Gordon, Loeb, & Zhou (2003) 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 as a result of stock price declines, the loss of customers, fines or other costs incurred in addressing the issues (Culnan & Williams, 2009). 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 (Nofer *et al.*, 2014).

Addressing privacy can also be seen as 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 in order 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 (King & Raja, 2012), and multinationals can reduce their costs by applying standard processes throughout the corporation for handling data (Blume, 2015).

The same protection provided for customer information can guard sensitive company information, such as trade secrets and intellectual property (Culnan & Williams, 2009, p. 683). By recognising 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) (Culnan & Williams, 2009, p. 683).

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 (Barney & Hansen, 1994). Organisations that are viewed as legitimate are more likely to be perceived as trustworthy (Culnan & Williams, 2009), which will lead to customers having fewer privacy concerns and being more willing to provide personal information (Norberg *et al.*, 2007). In addition, customers may be willing to pay a premium for privacy (Tsai, Egelman, Cranor, & Acquisti, 2011) and more amenable to marketing if the firm is open about its policies, minimises its requests for information, and collects only what is relevant (Phelps, Nowak, & Ferrell, 2000).

A firm that truly embraces privacy does more than just create a privacy policy: it creates a culture of privacy within the organisation through leadership, training, regular audits and by considering privacy for every new use of personal information (Culnan & Armstrong, 1999; Culnan & Williams, 2009).

Three “frameworks” (a label used for simplicity) that can be used to analyse the strategies and behaviours of firms in respect of informational privacy are discussed in the following sections.

2.3.1. Institutional Approach and Resource-based View Paradigms

Chan & Greenaway (2005) proposed that organisations’ information privacy behaviours can be partly explained by the role information privacy plays in either achieving firm survival through compliance, which is explained by the institutional approach paradigm, or in achieving competitive advantage through the use of customer information, which is explained by the resource-based view paradigm.

The institutional approach paradigm considers the effects of the external environment and its forces on organisations. DiMaggio & Powell (1983) suggest that these mechanisms can be organised into three categories: coercive (legal pressures, as well as formal and informal ones from other dependent organisations), normative (cultural, primarily in striving to be professional) and mimetic (imitation, which is encouraged by uncertainty). Firms may be shaped by striving to conform to these norms and external pressures. So, for instance, they may choose not to differentiate themselves through their informational privacy programmes, but instead implement them in order to conform to external requirements or expectations.

Chan & Greenaway identified three elements of interest when considering this paradigm:

1. ***Organisational goals***: the organisation’s primary goal is to survive by achieving legitimacy. 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 organisation’s privacy practices help it to achieve a particular type of legitimacy.
2. ***Ability and willingness to respond to pressure***: the degree to which a firm is embedded in – in other words, influenced by – its social networks (which are comprised of other organisations, including competitors, regulators, customers and other stakeholders) will impact on its ability and willingness to respond to external pressure. These networks constrain response, but this does not mean that the organisation is passive – it has agency and can choose to operate outside of these norms and restrictions.
3. ***Responses to pressures***: a firm can be acquiescent and imitate other organisations seen as models or it can be proactive and lead the way. A firm may be acquiescent in order to

conform to a defined legal model or it may imitate other firms that have similar minimalist approaches to privacy (these tactics are not mutually exclusive). A proactive firm would emphasise the good differences in their privacy practices compared to those of its peers, but it would endeavour not to be seen as being outside of the norms of its industry network, nor would it want to undermine the overall perceptions of the legitimacy of their industry (so its leadership would be constrained).

A summary of the discussion of these elements is given in Table 1.

Table 1: The institutional approach to explaining organisation privacy behaviours

Element ▼	***Application to Information Privacy in Organisations***	
	Acquiescent Approach	**Proactive Approach**
Organisational Goals	▪ Pragmatic ▪ Managerial	▪ Social ▪ Technical
Ability / Willingness to Respond to Pressure	Embeddedness	Agency
Responses to Pressure	Imitation of peer organisations	Impression management to yield “constrained leadership”

In contrast to the institutional approach, the resource-based view paradigm looks from the inside out, considering how firms can use their resources to pursue sustainable competitive advantage. It is not enough for an organisation to simply own or have access to a resource; it must consider the resource’s degree of value, its rareness, its imitability and its substitutability. A firm can choose a unique combination of resources and behave independently, as opposed to the following the suggested institutional approach tactics of reacting, imitating or performing impression management: instead of its informational privacy practices being responses to external forces, they are the result of deliberate choices made to differentiate the firm’s privacy behaviours.

There are four elements to the resource-based view paradigm, as listed by Chan & Greenaway:

1. ***Organisational goals***: firms strive for competitive advantage based on strategic differentiations. This can be done by two means. The first is by highlighting the “development and use of detailed customer information to deliver superior customer insight” (Chan & Greenaway, 2005, p. 183), which is done by collecting as much

information as possible, justified by the need for input for their decision models. A second method is to nurture superior customer trust by gathering less information in order to avoid alienating customers or gather as much information as others, but pay 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.

2. ***Resources***: the key resource is customer information, but how it is viewed and used by the organisation is important. In the first instance, it can either be used to spur internal innovation, achieve efficiency and improve internal learning in order to better achieve organisational goals. If this organisation were to consider privacy at all, it would aim to minimise intrusion on the collection and processing of data. In the second instance, customer information can be used to better understand customers in order to better serve their immediate or anticipate their future needs. In this approach, the firm would ensure that the information being collected is relevant, useful and timely.
3. ***Processes***: firms will choose their privacy policies based on whether they would like to emphasise the intellectual/knowledge or social/relationship aspects of their processes – in other words, whether they are collecting as much or as little information as possible.
4. ***Dynamic capability***: firms can pursue either a customer knowledge capability, where the information is treated as an internal, efficiency-focussed resource, or it can pursue a customer relationship capability, where customers' privacy concerns are given a higher priority than the organisation's information gathering. The first approach can lead to competitive advantage through the ability to track and predict customer preferences, whereas the second can lead to it through achieving trustworthiness in the eyes of customers.

The discussion of these elements is summarised in Table 2.

Chan & Greenaway combined and summarised these two approaches as presented in Table 3.

Table 2: The resource-based view to explaining organisation privacy behaviours

	Application to Information Privacy in Organisations	
Element **▼**	**Information Focus**	**Customer Focus**
Organisational Goals	Strategic differentiation based on superior customer insight	Strategic differentiation based on superior customer trust
Resource	Support efficiency focused internal innovation	Support effectiveness focused external innovation
Process	Information privacy as an intellectual/knowledge management process	Information privacy as a social/relationship management process
Dynamic Capability	Customer knowledge capability	Customer relationship capability

Table 3: Summary of theoretical explanations for information privacy behaviours

Theory **▶**	**Institutional Approach**		**Resource-based View**	
Theory Attributes **▼**	**Acquiescence Strategy**	**Proactive Strategy**	**Customer Knowledge Capability**	**Customer Relationship Capability**
Organisational Goal Argued By Theory Base	Survival		Competitive advantage	
Information Privacy Role in Achieving Organisational Goal	Source for pragmatic legitimacy	Source for social legitimacy	Support for differentiation through intellectual resource	Support for differentiation through social resource
Focus of Firm Information Privacy Activities	Internal	External	Internal	External
Information Privacy as a Mechanism for Achieving the Goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

2.3.2. Customer Information Privacy Framework

The customer information privacy framework is a two-dimensional framework for designing a privacy programme (Greenaway & Chan, 2013). One dimension is whether an organisation sees privacy action as a risk (potentially negative and costly to the organisation) or an opportunity (potentially positive and a good investment). The other dimension is whether the organisation's information management activities focus on internal or external processes and stakeholders. These two dimensions lead to four approaches to customer information privacy, as shown in Figure 2.

	Internal Focus	**External Focus**
Risk	**Minimum privacy activities to avoid breach** *"Privacy is a distraction"*	**Minimum privacy activities to avoid regulatory oversight** *"Privacy is just another compliance program"*
Opportunity	**Maximise privacy-based information collection / process improvement** *"Privacy is all about information management"*	**Maximise privacy-based customer relationships** *"Privacy is good ethics and good business"*

Figure 2: Customer information privacy framework (Chan & Greenaway, 2005)

In order to have an effective customer information programme that matches the organisation's priorities, the organisation's privacy profile needs to be aligned with the dimensions of the framework (Greenaway & Chan, 2013). This profile consists of two sets of characteristics:

1. ***Privacy outlook constraints***: the company's view of privacy and the constraints this imposes on decision-making. These characteristics are:
    a. *Reputational aims* – the firm's assumption about the relationship between privacy protection and its reputation.
    b. *Customer privacy preference assumptions* – the firm's assumptions about whether and to what extent customers care about their information privacy.
    c. *Organisational culture* – the extent to which customer information privacy is considered to be an integral part of how the firm operates.
    d. *IT investments with privacy implications* – the IT investments that the firm has made or is planning to make that will impact customers' information privacy.

2. ***Privacy implementation choices***: specific implantation decisions. These choices are not mutually exclusive and can be adjusted over time as the organisation learns or privacy regulations change. These characteristics include:
    a. *Intended outcomes* – the outcomes the firm desires to achieve from its privacy activities.
    b. *Implementation mechanisms* – how the firm puts its privacy activities in place.
    c. *Customer information and privacy linkages* – how the firm uses privacy to support its customer information activities.
    d. *Privacy-related IT investments* – the type of and extent to which the firm invests in IT to support its privacy activities.

A summary of the approaches to privacy programmes is provided in Table 4 (adapted from Greenaway & Chan, 2013, p. 147).

Table 4: Approaches to privacy programmes

Characteristic	Minimum to Avoid Breach	Minimum to Avoid Regulatory Oversight	Maximise Privacy-Based Information Collection	Maximise Privacy-Based Customer Relationships
PRIVACY OUTLOOK CONSTRAINTS				
Reputational Aims	Use privacy practices to avoid or minimise damage to reputation.		Use privacy practices to maintain reputation.	Use privacy practices to improve reputation.
Customer Privacy Preference Assumptions	Customers do not give privacy a high priority or they assume that the firm is acting to protect their information.		Customers are privacy-aware but rank convenience above privacy.	Customers value their privacy and monitor the firm's practices.
Organisational Culture	References to privacy limited to acceptable computer use policies.		Refer to privacy in documents about corporate values and/or ethics or code of conduct.	
IT Investments with Privacy Implications	Assess privacy impacts post-IT implementation – "an after-thought"; limited to security IT systems.	Assess privacy impacts post-IT implementation – "an after-thought"; limited to retro-fitting IT systems to ensure compliance.	Identify, assess and adjust for privacy impacts prior to IT implementation – "bake privacy in".	

Characteristic	Minimum to Avoid Breach	Minimum to Avoid Regulatory Oversight	Maximise Privacy-Based Information Collection	Maximise Privacy-Based Customer Relationships
PRIVACY IMPLEMENTATION CHOICES				
Intended Outcomes	Focus on security to avoid privacy breaches.	Comply with laws and regulations.	Improve accuracy of customer profiles.	Develop customer relationships.
Implementation Mechanisms	▪ Low profile, non-executive management. ▪ Narrowly focused division, such as IT security or risk management, with limited staff resources devoted to privacy. ▪ Limited budget geared to minimum necessary expenditures to meet limited intended outcomes.		▪ Higher-profile executive leadership. ▪ Privacy staff located in broadly focused division, such as marketing or information management. ▪ Dedicated privacy budget sufficient to support broad, ambitious intended outcomes, including resources for staff training and communication, and customer education.	
Customer Information and Privacy Linkages	Privacy practices are decoupled from customer information collection and use activities.		Use privacy policy to improve collection of and permission to use customer information.	Emphasise privacy practices in order to developer customer relationships and increase customer trust.
Privacy-Related IT Investments	Only invest in basic security systems.	▪ Invest in security systems. ▪ Invest in automated privacy-impact-assessment systems.	▪ Invest in security systems. ▪ Invest in automated privacy-impact-assessment systems, including module for privacy-preference management tools. ▪ Invest in knowledge management and training tools for employees.	▪ Invest in security systems. ▪ Invest in automated privacy-impact-assessment systems, including module for privacy-preference management tools. ▪ Invest in knowledge management and training tools for employees. ▪ Provide online education modules for customers.

2.3.3. Organisational Privacy Strategy Framework

This framework is a convergence of Oliver's strategic responses framework (as cited in Parks & Wigand, 2014) and Miles and Snow's typology of organisational strategy, structure and processes (as cited in Parks & Wigand, 2014).

Oliver's framework looks at the strategic behaviours that organisations may have in response to institutional pressures. The framework suggests that organisations can take five broad strategies:

1. ***Acquiescence***: comply with institutional pressures.
2. ***Compromise***: only partially comply with institutional pressures.
3. ***Avoidance***: conceal or avoid compliance.
4. ***Defiance***: actively challenge institutional pressures.
5. ***Manipulation***: actively change institutional pressures or exert power over those who introduce or enforce them.

These strategies, together with their associated tactics (and examples of these tactics), are presented in Table 5.

Table 5: Oliver's strategic responses framework

Strategy	Tactics	Examples
Acquiescence	▪ Habit ▪ Imitate ▪ Comply	▪ Following invisible, taken-for-granted norms. ▪ Mimicking institutional models. ▪ Obeying rules and accepting norms.
Compromise	▪ Balance ▪ Pacify ▪ Bargain	▪ Balancing the expectations of multiple constituents. ▪ Placating and accommodating institutional elements. ▪ Negotiating with institutional stakeholders.
Avoidance	▪ Conceal ▪ Buffer ▪ Escape	▪ Disguising nonconformity. ▪ Loosening institutional attachments. ▪ Changing goals, activities or domains.
Defiance	▪ Dismiss ▪ Challenge ▪ Attack	▪ Ignoring explicit norms and values. ▪ Contesting rules and requirements. ▪ Assaulting the sources of institutional pressure.
Manipulation	▪ Co-opt ▪ Influence ▪ Control	▪ Importing influential constituents. ▪ Shaping values and criteria. ▪ Dominating institutional constituents and processes.

Miles and Snow's typology considers three inter-related problems: the entrepreneurial problem of how the organisation manages its market share, the engineering (or operational) problem of the firm's technologies and processes, and the administrative problem of the ways the firm implements its strategies. As a result, Miles and Snow postulated that there are four strategic types of organisations:

1. ***Prospector***: dynamic and proactive, this organisation identifies and exploits new product and market opportunities.
2. ***Defender***: focuses on maintaining a stable share of the market.
3. ***Analyser***: a combination of the prospector and defender types, this organisation looks to minimise risk and maximise profit.
4. ***Reactor***: this organisation has no strategy, design or structure, and is not prepared for changes in its environment.

These strategic types and their approaches to the three fundamental problems listed above are presented in Table 6.

Table 6: Miles and Snow's typology of organisational strategy, structure and processes

	Fundamental Problems Facing Organisations		
Strategy Type ▼	**The Entrepreneurial Problem**	**The Engineering Problem**	**The Administrative Problem**
Prospector	Exploring environmental changes in search of new opportunities.	Low degree of routinisation and mechanisation.	Facilitating changing domains and flexible technologies.
Defender	Maintaining stability in existing operations.	Specialised investment in highly cost-efficient technologies.	Maintaining efficiency by achieving a strict control through structural and process mechanism.
Analyser	Maintaining both a stable and changing domain.	Dual technological core (stable and flexible component).	Maintaining a balance between stability and flexibility.
Reactor	Reluctant to act due to a pattern of inconsistencies and instability.	Unavailability of a technology strategy.	Inconsistency and lack of clarity.

Parks & Wigand (2014) proposed the organisational privacy strategy framework based on the converged insights of Oliver's and Miles and Snow's frameworks. It has two dimensions (*resistance* and *proactivity*) and four quadrants (*conformist*, *entrepreneur*, *transformer* and *defender*). A visual representation of the strategies is shown in Figure 3.

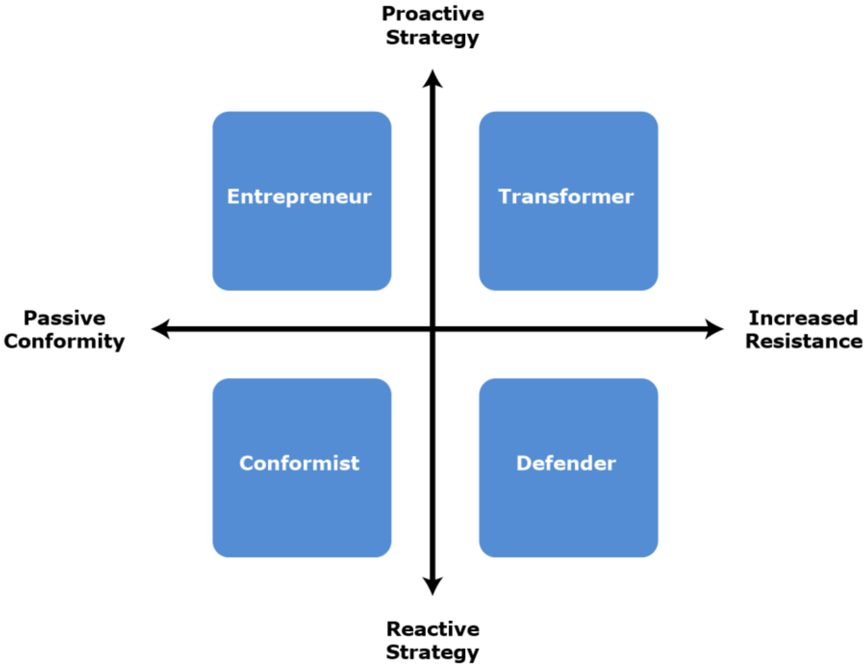

Figure 3: Organisational privacy strategy framework – four quadrants of strategic responses to information privacy (Parks & Wigand, 2014)

The ***conformist*** organisation does what the law requires and focuses on its technical security in order to avoid penalties and costly recovery procedures after a breach. It reacts either to negative publicity (for example, a breach) or to legislative pressures. Its emphasis is on maintaining stability and efficiency within the organisation, rather than concentrating on proactively protecting customer information.

Like the conformist, an organisation with an ***entrepreneur*** strategy also reacts to institutional pressures. However, unlike the conformist, often it will proactively institute measures that go beyond compliance and endeavour to cater for foreseen threats in order to leverage new customers, products or opportunities. In doing so, it develops a culture for privacy in addition to complying with institutional norms.

The ***transformer*** invests in current and future competencies, including a culture of privacy and governance processes. It looks to protect its core competencies while also looking ahead in order to anticipate issues and seek opportunities for change, as well as new markets and products. At the same time, it may attempt to transform institutional rules through lobbying, negotiations or bribery in order to improve the external conditions for its strategy.

Finally, the ***defender*** looks to maintain a stable environment while avoiding or defying regulations. It will respond if institutional pressures present a threat to their legitimacy, possibly by lobbying against them.

Table 7 summarises these strategic privacy responses and where each originates from.

Table 7: Organisational privacy strategy framework – strategic responses to information privacy

Privacy Strategies	Description	Resistance Dimension (Oliver)	Proactivity Dimension (Miles and Snow)
Conformist	Conforms to institutional requirements for the purpose of achieving organisational stability.	Acquiescence / Compromise	Reactor / Defender
Entrepreneur	Embraces a proactive approach and invests in privacy protection safeguards and strategies that account for regulators, investors, and customers.	Acquiescence / Compromise	Analyser / Prospector
Transformer	Carries out a proactive approach to privacy management and challenges institutional requirements by means of negotiation, manipulation, and bribery.	Defiance / Manipulate	Analyser / Prospector
Defender	Ignore, defend, or lobby against institutional pressures while trying to achieve organisational stability.	Defiance / Manipulate	Reactor / Defender

The section that follows briefly looks at the details of the Protection of Personal Information Act.

2.4. The Protection of Personal Information Act

In South Africa, privacy is recognised 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 has to be balanced with other rights (South African Law Reform Commission, 2005, p. iv).

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 (South African Law Reform Commission, 2005). In this paper the authors proposed draft legislation that later became the Act.

The investigation recognised 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" (South African Law Reform Commission, 2005, p. iv). 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 (South African Law Reform Commission, 2005, p. vi). The importance of data privacy legislation to trade has increased even more since the investigation: as of September 2013, 101 countries have enacted privacy laws and several others have official bills which have not yet been enacted (Greenleaf, 2014).

PoPI was signed into law by the president in November 2013. However, it has not yet commenced (come to have legal force and effect); when it does, organisations will have a year in which to comply with its provisions. As part of the Act, an Information Regulator will be established. The Regulator will handle complaints from data subjects (a data subject being the person to whom personal information relates) and will have extensive powers to investigate and punish parties that infringe. The establishment of a regulator is also in line with global trends: the majority of those countries with data privacy laws have a data protection authority (Greenleaf, 2014).

The Act defines *personal information* as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person" (Protection of Personal Information Act (Act No. 4 of 2013), p. 14). 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" (Protection of Personal Information Act (Act No. 4 of 2013), p. 38). Processing of special personal information is subject to more restrictions than that of general personal information.

PoPI will apply to any organisation, public or private, that processes personal information. It has eight conditions (principles) for the lawful processing of personal information. In addition to these conditions, there are several chapters that are of relevance to this research. The details of both sets are sketched out in Table 8 and Table 9.

Table 8: The eight conditions in PoPI and notable details of what they cover

Condition	Description
Accountability	The responsible party must ensure that the conditions for processing are lawful (in other words, comply with the Act).
Processing limitation	Personal information must be: ▪ Processed lawfully and so as not to infringe on the data subject's privacy. ▪ Adequate, relevant and not excessive for its purpose. ▪ Processed with consent from the data subject, who can withdraw consent or object at any time. ▪ Collected directly from the data subject.
Purpose specification	Personal information must be collected for a specific, explicitly-defined and lawful purpose, and must not be kept for longer than is necessary. Records must be destroyed, deleted or de-identified as soon as is reasonably practical after the responsible party is no longer allowed to retain them.

Condition	Description
Further processing limitation	Further processing of personal information must be compatible with the purpose for which it was collected.
Information quality	Reasonable steps must be taken to ensure that personal information is complete, accurate, not misleading and updated where necessary.
Openness	The responsible party must maintain documentation of all processing operations under its responsibility in accordance with the Promotion of Access to Information Act (Act No. 2 of 2000). Reasonable steps must be taken to notify the data subject when collecting person information. Details on the information being collected, the responsible party, the purpose of the information, and various other aspects must be provided.
Security safeguards	Appropriate measures must be taken to secure data and prevent loss, damage and unlawful access to it. If a third party is used to process information, they must treat it as confidential and have the appropriate security measures to protect it in place. If there is a security breach, the Regulator and data subject whose information has been accessed must be notified as soon as possible.
Data subject participation	A data subject: ▪ Has the right to confirm, at no cost, whether a responsible party holds personal information about them. ▪ May request the record or a description of this information, including details on all third parties who have or have had access to the information. A charge may be levied for this, but an estimate of the cost must be provided beforehand. ▪ May request that information be corrected or deleted if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. ▪ May request that a record is destroyed or deleted if the responsible party is no longer allowed to retain it. Any material changes must be relayed to third parties by the responsible party.

Table 9: Further relevant chapters of PoPI and notable details of what they cover

Chapter	Detail
Direct marketing	The processing of personal information for the use of direct marketing is prohibited unless the data subject has given their consent and is a customer of the responsible party. The responsible party may approach the data subject only once in order to obtain consent as long as they have not previously withheld it.
Automated decision making	Automated decision making may not be the sole basis for a decision that affects a data subject legally or to a substantial degree.
Trans-border information flows	Personal information about a data subject may not be transferred to a third party in a foreign country unless the third party is subject to law that provides a level of protection that is equivalent to those in PoPI, the data subject consents to the transfer, and the transfer is necessary in order to fulfil the contract with the subject (or on behalf a third party that has a contract with the subject).

There are many exceptions and special cases for much of the above. For example, frequently throughout the Act exceptions are made when an action is done after obtaining consent from the data subject or when the action is in the subject's best interest.

PoPI is possibly one of the most comprehensive pieces of legislation of its type in the world (Burmeister, 2014). Given this, becoming fully compliant will take time and effort. The Regulator will have the authority to decide whether or not a firm is compliant, and the consequences for failing to comply with PoPI can include fines, imprisonment for up to 10 years, or even both.

Privacy is a complex topic that in today's world is synonymous with personal information. In this chapter, the concept of privacy was examined along with theories about informational privacy. The importance of privacy to consumers was then looked at: challenges individuals face when making decisions about privacy were discussed and three issues to do with information privacy were outlined. Finally, the importance of privacy to organisations was then studied, together with three frameworks that can be used to analyse the informational privacy strategies of organisations.

The next chapter examines the methodology employed for the project.

CHAPTER 3.

RESEARCH METHODOLOGY

The methods that were used in approaching and performing this research are detailed in this chapter. It begins by examining the research philosophy that moulded the project, as well as the nature of the approach taken in performing the research. In the section that follows, the research method is discussed and its strengths and weaknesses are examined. The research process is then detailed: the sample and time span for the project are described together with the data collection and analysis techniques that were employed. Finally, the project's ethical considerations are outlined.

3.1. Research Paradigm and Approach

Research is shaped by the researcher's paradigm (philosophy) – their mental model or belief systems (Bhattacherjee, 2012). This paradigm represents "a worldview that defines, for its holder, the nature of the 'world,' the individual's place in it, and the range of possible relationships to that world and its parts" (Guba & Lincoln, 1994, p. 107).

According to Burrell & Morgan (1979, p. 1), underlying a paradigm are two sets of philosophical assumptions: ontology and epistemology. Ontological assumptions concern the essence of the phenomena being investigated (in other words, the nature of reality): either the world is empirical and exists independent of the individual, or it exists because of the consciousness of the individual (Burrell & Morgan, 1979; Orlikowski & Baroudi, 1991). Epistemological assumptions are those about the grounds of knowledge: about how best to study and understand the world – whether knowledge should be gained objectively or subjectively. They are, by nature, linked – a stance taken in one will define the other; in other words, one either assumes a "real" world, external to the individual, and takes an objective approach to studying it, or one views the world as being internal to the individual, a product of one's mind, and takes a subjective approach when studying it.

Saunders *et al*. (2009) list four paradigms management researchers can adopt: positivism, realism, interpretivism and pragmatism.

A researcher who subscribes to *positivism* has an objective view of the social world and believes that phenomena can be observed and measured, and law-like generalisations, similar to those in physical and natural science, can be produced (Saunders *et al*., 2009). In positivism, the researcher uses an existing theory in order to generate hypotheses and then test them, leading to further development of theory and further research. The research is performed in a value-free way: the researcher neither impacts nor is impacted by the subject of the research. Positivism normally involves a high degree of structure, large samples and quantitative data collection and analysis methods.

The core of the *realism* paradigm is that objects exist independent of the human mind. It is similar to positivism in that it advocates a scientific approach to research, but differs to it in that it does not rely on theory to provide a basis for it. There are two branches of realism: direct realism, which advocates that the world is as we perceive it to be ("what you see is what you get"), and critical realism, which says that we experience sensations of the world rather than it directly. Critical realists "believe that there is an external reality that is independent of a person's thinking but we can never know such reality with any degree of certainty" (Bhattacherjee, 2012, p. 18) because the researcher is influenced by their own views and experiences, and this will affect the research. Realists use quantitative or qualitative research methods, depending on the subject.

According to *interpretivism*, reality and our knowledge of it cannot be "understood independent of the social actors (including the researchers) that construct and make sense of that reality" (Orlikowski & Baroudi, 1991, p. 13). Reality is subjectively interpreted by the researcher and so can only be understood by understanding the actions and interactions of humans. The aim of interpretive research is to understand the world at a subjective level, from the point of view of the participant rather than the observer (Burrell & Morgan, 1979, p. 28). In their interaction, the researcher and research subjects co-create data (Goldkuhl, 2012; Guba & Lincoln, 1994). Interpretivistic research data is qualitative in nature and collected through small samples and in-depth investigation.

Finally, *pragmatism* advocates that the research question being posed determines the ontology and epistemology the researcher adopts (Saunders *et al*., 2009). Furthermore, a single philosophy need not be adopted if the research question does not unambiguously suggest it;

instead, a mix of philosophies can be applied. Pragmatic research can involve a mix of quantitative and qualitative data collection and analysis methods.

For this research the pragmatist paradigm was embraced. 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 paradigm and qualitative methods. These methods involved endeavouring to understand the points of view of research subjects, taking into account each one's role and work environment, and applying the researcher's own experiences and knowledge of such environments and the research topic.

While many research projects take either a wholly deductive or inductive approach, it is possible to mix the two (Saunders et al., 2009, p. 127). Gilgun (2005a) proposed an approach called *deductive qualitative analysis* – "qualitative research that begins with theory" (Gilgun, 2010, p. 1). 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" (Gilgun, 2005b, p. 42). Deductive qualitative analysis allows for the model to be reformulated when negative cases – those which do not fit the model – are found (Gilgun, 2005a). The deductive aspect of this approach gives the project a foundation off which to work, while the inductive characteristic allows for flexibility, letting researcher explore aspects of the topic to various degrees of depth as the research progresses.

3.2. Research Method

This research was performed 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)" (Benbasat, Goldstein, & Mead, 1987, p. 370). Yin (2014) goes further to define a case study in two parts:

1. *Scope of a case study*. A case study is an empirical enquiry that investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident.
2. *Features of a case study*. A case study enquiry copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result relies on multiple sources of evidence, with data need to converge in a triangulating fashion, and as another result benefits from the prior development of theoretical propositions to guide data collection and analysis.

The research was performed through 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 organisation as a whole). The aim was to understand the similarities and differences between cases (Baxter & Jack, 2008) and improve the generalisability of the results (Bhattacherjee, 2012, p. 40; Yin, 2014, p. 64). The advantage of this approach is that the findings are considered robust and reliable; the disadvantage is that it can be time-consuming and expensive to perform (Baxter & Jack, 2008, p. 550).

Case study has several strengths and weaknesses (Bhattacherjee, 2012, p. 93). In an interpretive case study, the concepts of interest need not be known in advance, but can instead be discovered as the research progresses. It also allows for research questions to be modified during the process if the original ones are found to be less significant. However, it also has several drawbacks. It involves no experimental control, so the causality of results is weak. These results also rely heavily on the skills of the researcher to integrate them, so findings can be criticised as being subjective. Finally, because the results are contextualised, it can be difficult to generalise them.

Bhattacherjee (2012, p. 94) presents a list of five potential errors, as first detailed in Benbasat *et al.* (1987):

1. Many case studies start without specific research questions and therefore lack any specific answers or insightful findings.
2. Case subjects are often selected based on access and convenience, rather than based on their fit to the research questions, which can lead to a mismatch.
3. Researchers often do not validate data using multiple means, which may lead to bias interpretation based on biased responses from interviewees.
4. Many studies fail to provide information on how data was collected or analysed, which can raise doubts about the reliability of the findings.
5. Often studies are not longitudinal in nature, despite case study being a good longitudinal research method, leading to results that are limited in value.

Addressing these issues in terms of this research project:

1. This research poses a specific question that it aims to have answered and objectives to achieve in order to do so.

2. Sample subjects were selected based on access and convenience, a reasonable limitation for this project, but they were appropriate for the research.
3. Data was collected primarily through interviews, but was validated where possible. The use of multiple studies has assisted in rooting out interviewee bias.
4. This report provides full details on data collection and analysis, including samples of the research instruments.
5. The research was cross-sectional due to the Honours time limit.

3.3. Research Process

3.3.1. 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 (Prorokowski & Prorokowski, 2014).

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" (Botha & Makina, 2011, p. 34). As a result 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 (Jones, 2014).

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 PoPI's complexity, as well as the fact that many corporate projects take a significant amount of time to design and implement, it is likely that many PoPI-compliance projects will have to have already begun as inevitably they would take more than the year of grace allowed by the Act once it has commenced. In addition, the fact that corporates are among the major users of private data because of their size (South African Law Reform Commission, 2005, p. 5), together with the financial difficulties of many consumers, particularly with debt (Maswanganyi, 2015), increases the possibility of them being amongst those who have the earliest PoPI-compliance complaints laid against them.

Smaller organisations, in contrast, are less likely to have concrete privacy strategies or have commenced PoPI-orientated projects, as they tend to lack the resources, knowledge, skills and awareness – particularly in the legal sphere – necessary to understand the issues surrounding any legislation and undertake projects to ensure compliance (Kyobe, 2009; Nkosi, Bounds, & Goldman, 2013; Seddon & Currie, 2014).

The individuals who participated in the project 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; only a single person was interviewed at the remaining two, despite attempts to find a second appropriate interviewee in each.

3.3.2. Time Horizon

The research was cross-sectional – it looked at the informational privacy strategies of corporates at a particular point in time. This is appropriate given the time constraints of the project as set by the Honours time limit.

3.3.3. Data Collection

The most important means of data collection was interviews with senior management in the sample group. The "responsive interviewing" technique (Rubin & Rubin, 2012) was used. This entails building a relationship of trust between the interviewer and interviewee through questioning that is friendly in tone and with little confrontation. 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.

Responsive interviews consist of three question types: main questions, follow-up questions and probes (Rubin & Rubin, 2012, pp. 116–119). The goal of main questions is to answer the research question and for this project they are be based on the theories discussed in the literature review summary. Follow-up questions seek to explore the interviewee's answers for depth – in order to get more detail and to clarify aspects of it when required. Finally, probes are questions, comments or gestures used by the interviewer to manage the conversation – to keep it on topic, get clarification, encourage the interviewee to keep talking or go into more depth, and so on.

Social interactions can be construed as a drama (Goffman, 1959, as cited in Myers & Newman, 2007). An interview, being a form of social interaction, can also be viewed as such and while all participants contribute to it the interviewer has a special role in that they shape it (Hermanns, 2004). The elements of this drama are listed in Table 10, replicated from Myers & Newman (2007, p. 11).

Table 10: The qualitative interview as a drama (Myers & Newman, 2007, p. 11)

Concept	Description
Drama	The interview is a drama with a stage, props, actors, an audience, a script, and a performance.
Stage	A variety of organisational settings and social situations although in business settings the stage is normally an office. Various props might be used such as pens, notes, or a tape recorder.
Actor	Both the interviewer and the interviewee can be seen as actors. The researcher has to play the part of an interested interviewer; the interviewee plays the part of a knowledgeable person in the organisation.
Audience	Both the interviewer and the interviewee can be seen as the audience. The researcher should listen intently while interviewing; the interviewee(s) should listen to the questions and answer them appropriately. The audience can also be seen more broadly as the readers of the research paper(s) produced.
Script	The interviewer has a more or less partially developed script with questions to be put to the interviewee to guide the conversation. The interviewee normally has no script and has to improvise.
Entry	Impression management is very important, particularly first impressions. It is important to dress up or dress down depending upon the situation.
Exit	Leaving the stage, possibly preparing the way for the next performance (finding other actors – snowballing) or another performance at a later date (e.g., perhaps as part of a longitudinal study).
Performance	All of the above together produce a good or a bad performance. The quality of the performance affects the quality of the disclosure which in turn affects the quality of the data.

Based on this model, Myers & Newman (2007) suggest the following guidelines for qualitative interviewing:

1. *Situating the researcher as an actor*. The interviewer (researcher) should introduce and give some background on himself before the interview in order to help the interviewee understand the relationship between the interviewer and the subject of the interview. This information should also be included in the research write-up in order to aid its appraisal by readers.
2. *Minimise social dissonance*. It is important to reduce any discomfort the interviewee may have. This is done by managing first impressions, dressing suitably and using the appropriate language.
3. *Represent various "voices"*. By interviewing a number of people in the organisation, one can avoid having just one "voice" emerge and thereby avoid bias.

4. *Everyone is an interpreter*. Both the interviewer and the interviewee are interpreters of the interviewee's world.
5. *Use mirroring in questions and answers*. The interviewer should use the language of interviewee when phrasing questions and comments in order to better focus on their world and avoid imposing the interviewer's own.
6. *Flexibility*. By using a semi-structured or unstructured interview approach, the interviewer can improvise and adapt to the interviewee's attitude and responses in order to explore interesting areas of research.
7. *Ethics of interviewing*. Researchers should maintain ethical standards by obtaining ethics approval from appropriate ethics committees and permission from interviewees and their organisations; they should treat interviewees with respect; and they should fulfil their commitments to individuals and organisations by keeping records and information confidential, confirming information as required, and possibly presenting their findings to the interview subjects.

The "stage" for each interview was a quiet location that was most convenient to the interviewee – usually a company meeting room. The interviewer dressed in "business casual" attire (a suit without a neck tie) in order to make a good, professional impression ("entry") and minimise social dissonance.

The interviews were semi-structured in nature and based on a set of prepared, open-ended questions in the form of a guide ("script"). 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 (Flick, 2014). The interview guide is attached as appendix A.

Each interview was audio-recorded (once agreed to by the interviewee) and transcribed in its entirety. The transcriptions focused on spoken words and did not detail the manner of delivery because while there is merit in capturing such descriptive details (Roulston, 2014), they are likely of more relevance in pure social research than information systems research. Capturing them also adds complexity to the transcription process and a more complex transcription is likely to be more difficult to analyse; both of these aspects are problematic given the limited time for the project.

Limited notes of the interviewee's important comments were taken during the interviews that were recorded. In the one case where permission to record was not provided, a more detailed set of notes was taken.

Due to the nature of this project (particularly its requirement of specific expertise and knowledge), as well as its limits (in time and ready access to interview subjects), only a small number of people were interviewed in each organisation.

The ethical aspects of this project are discussed in further detail in section 3.4.

It must be noted that qualitative interviews can have difficulties, problems and pitfalls. These are summarised by Myers & Newman (2007):

1. *Artificiality of the interview*. The interviewee will typically be a complete stranger and often will be expected to give or create opinions under time pressure.
2. *Lack of trust*. Given that the interviewer is likely to be a complete stranger, the interviewee may choose not to divulge information that could be of importance to the research, thus leaving it incomplete.
3. *Lack of time*. Time pressure can leave the research incomplete or can lead to the interviewee expressing an incorrect or incomplete opinion.
4. *Level of entry*. The level at which the researcher enters the organisation is critical when obtaining pertinent information.
5. *Elite bias*. By interviewing only certain people (such as senior employees), the researcher can fail to gain a broader understanding of the issue.
6. *The Hawthorne effect*. People often change their behaviour when they know they are being observed. By intruding on the social setting, the researcher can affect peoples' actions and adversely impact that which they are attempting to study.
7. *Constructing knowledge*. The interviewer is not merely obtaining information that exists – they are actively constructing knowledge. The interviewee is also doing so, particularly if they are considering issues that they have never explicitly reflected on before.
8. *Ambiguity of language*. Despite best intentions, one's words can often be ambiguous or misconstrued and so interviewees may not fully understand questions.
9. *Interviews can go wrong*. This may happen for a myriad of reasons – for instance, the interviewer could unintentionally offend the interviewee and cause the interview to be abandoned.

Despite these potential issues, the qualitative interview is a powerful data gathering technique (Myers & Newman, 2007, p. 5).

Documents may be useful supplements to interview data, clarifying it or providing extra detail. These can include official documentation, such as privacy policies, and everyday documents and correspondence, such as memoranda and e-mails. When analysing documentation, the "intentions and purposes for documenting something in a specific form" (Flick, 2014, p. 299) need to be taken into account. Challenges in dealing with documentation include deciding how to select material (particularly seeing as it was not created for research purposes), taking into account the contexts of the items, and deciding what to select in the material (Flick, 2014).

Informational documentation required for the project was limited to that provided on the subject companies' websites. No other documentation was offered by the interviewees.

3.3.4. Data Analysis

Data analysis was performed concurrent with data collection. The benefit of this approach is that the collection process can be adjusted marginally according to the themes that emerge during analysis and these themes can be investigated in more detail when uncovered (Bhattacherjee, 2012, p. 96).

The collected data was analysed using thematic analysis, which is a "method for identifying, analysing 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" (Braun & Clarke, 2006, p. 79).

Before performing thematic analysis, a number of points need to be considered and decisions about them made (Braun & Clarke, 2006, pp. 81–86):

1. *What counts as a theme?* "A theme captures something important about the data in relation to the research question, and represents some level of patterned response or meaning within the data set."
2. *Should a rich description of the data set or a detailed account of one particular aspect be provided?*
3. *Inductive versus theoretical thematic analysis.* Themes can be identified from the data (inductive) or analysis can be driven by the researcher's theoretical interest.
4. *Semantic or latent themes.* Themes can be identified at an explicit (semantic) level using only explicit or surface meanings of what a subject has said or what has been written, or they can be identified at an interpretive (latent) level through examining underlying ideas, assumptions, conceptualisations and ideologies that shape or form the semantic data.
5. *Epistemology: essentialist/realist versus constructionist thematic analysis.* This is usually decided while a research project is being planned and it affects the analysis.

6. *The many questions of qualitative research.* Care needs to be taken in distinguishing between research questions, interview questions and questions that guide data coding and analysis. This is not necessarily a relationship between these three.

The analysis for this research project generated a rich description of the data set, and it was performed using a combination of the inductive and theoretical approaches: themes identified through the literature review were used, whilst the analysis also sought to identify new themes.

Braun & Clarke (2006, p. 87) provide a step-by-step guide to performing thematic analysis, which is reproduced in Table 11.

Table 11: Step-by-step guide to performing thematic analysis (Braun & Clarke, 2006, p. 87)

Phase	Description
1. Familiarising yourself with your data	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes	On-going analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

There are several potential pitfalls to avoid when using this technique (Braun & Clarke, 2006, pp. 94–95). The first is a failure to perform analysis by simply stringing together a number of extracts; extracts must be used to illustrate points. Secondly, interview questions should not be used as themes. The third is a weak analysis where the themes appear not to work, have too much overlap between them or they are not consistent. The fourth is where analytic claims cannot be supported by the data or are even contradicted by it. Finally, the fifth is a "mismatch between theory and analytic claims, or between the research questions and the form of thematic analysis used" (Braun & Clarke, 2006, p. 95) – interpretations of the data need to be consistent with the theoretical framework.

Braun & Clarke (2006) also offer several advantages of thematic analysis. Those most relevant to this project are:

- It offers flexibility.
- It is a relatively quick and easy method to learn and do.
- It is accessible to researchers with little or no experience of qualitative research.
- It can highlight similarities and differences across the data set.
- It can generate unanticipated insights.

To assist in the analysis process, a computer aided qualitative data analysis software (CAQDAS) package was used. According to G. R. Gibbs (2014, p. 280), any CAQDAS package should be appropriate for thematic analysis. This project used NVivo version 10, which is offered and supported by the university.

3.4. Ethical Considerations

Confidentiality is a key factor in convincing subjects to participate in research, gain access to important data and elicit candid responses from participants (Benbasat *et al.*, 1987, p. 373). Interview subjects and their companies are not identified in this research report or any other document that may become public. Both groups were assigned codes that are used to identify them in public documents.

Informed, voluntary consent to perform interviews was obtained in writing from the individual interview subjects; this included consent to the audio-recording of their interviews. The individuals had the right to withdraw from the research at any stage. The consent form together with an introductory letter is attached as appendix B.

All research data files, including recorded audio files, transcription documents and the document linking codes to identities are kept in a virtual drive which is stored as a single encrypted file. All participants (individuals and organisations) will be sent a copy of the final version of the report so that they may verify that their responses have been kept confidential.

Ethical approval for the research was obtained from the Commerce Faculty Ethics in Research Committee. The researcher read and complied with all prescribed ethics codes and policies stipulated by the university, including but not limited to:

- The UCT Policy for Responsible Conduct of Research;
- The UCT Research Ethics Code for Research Involving Human Participants; and
- The Commerce Faculty Ethics in Research Policy.

This chapter detailed the research methodology of this research project. The project was moulded by the pragmatist research paradigm, as it had a positivist element (existing theories were used as a base for the research), but the research was performed using an interpretivist paradigm and qualitative methods. It was approached using deductive qualitative analysis – qualitative research that is based on theory. The research was performed using multiple case studies, with a single company being the unit of analysis. The project sample was five corporates in the financial services industry, which were examined at a single point in time. Data was collected through semi-structured interviews and analysed using thematic analysis and qualitative analysis software called Nvivo.

In the next chapter, the research findings will be detailed, analysed and discussed.

CHAPTER 4.

RESEARCH FINDINGS

The findings of this research project are detailed below. Each subject company is treated as a separate case study. Each study begins with some high-level background information on the company and interviewees (most of which was taken from their LinkedIn profiles), as well as some basic information on the interviews. Next, the findings of the interviews are presented, broken down into three major themes: informational privacy strategies, the customer and the Protection of Personal Information Act. Lastly, the findings are analysed in order to determine which of the strategies presented in the three informational privacy strategy frameworks are being applied by the company. The applicable aspects of each framework, as determined by the analysis, are highlighted in orange and marked by [*], and the determined strategy is highlighted in green and marked by [**]. A discussion of the findings and analysis results of all of the case studies concludes the chapter.

4.1. Case Study: Company A

4.1.1. Company, Interviewee and Interview Details

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.

The table below provides a brief profile of the interviewee and some background details on the interview. Unfortunately, it was not possible to arrange an interview with a second person.

Table 12: Interviewee profile and details on the interview for Company A

	Interviewee A1
Job Description	Management of retail partner accounts at a national level.
Experience in Position	17 months. Previous management position at the company: over 2 years.
Interview Audio Recorded?	Yes.
Place of Interview	Interviewer's residence.
Additional Interview Details	Questions 9, 10, 11 and 12 were answered via e-mail, as the interview was cut short. The second interview question was re-answered via e-mail by the interviewer's request, as the interviewer felt it had been poorly asked and answered because of its complexity.

4.1.2. Findings

The following are the findings for company based on the interview and presented according to the grouping of the interview questions.

4.1.2.1. Informational Privacy Strategy Frameworks

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 organisation 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 wrote: "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 in order 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 organisation'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 manner in which customer information is managed in their retail partners' stores – for instance, the handling of documents such as application forms.

The firm does have some of its own self-defined privacy practices. It has several technical IT controls in place: for instance, USB ports on computers are blocked and mobile devices with company e-mail access can be wiped remotely by the company. There are also random checks performed on employee computers to ensure that sensitive customer information isn't being stored on them or sent out from them when it shouldn't be. Company A's website offers no information privacy policy documentation, but it does provide the manual required by the Promotion of Access to Information Act (PAIA), which covers how to request access to information that the company has on you.

Privacy is seen by the organisation as being a risk, not only because there is the potential to commit fraud using customer information, but also because "the less information that we're able to get and use the harder it is for us to be able to acquire customers and for us to refine and enhance our product and service offering" (interviewee A1). 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.

The organisation opposes legislation through the various associations it belongs to. At times it also provides feedback on the impact of changes to law directly to regulators. It also tries to anticipate and work ahead of some legislation changes through two means. Firstly, it is a member of the Direct Marking Association, where they discuss legislation and its impacts with other members. Secondly, they engage with retail and strategic partners in other industries whose operations are very sensitive to changes in legislation, so they can leverage off the thinking of those partners. They also need to understand the thinking of some partners because how those partners react to changes in law can directly affect Company A's operations.

4.1.2.2. Customer

The interviewee believes that privacy is of concern to South Africans in two ways. The first is that "a small percentage of the South African market" (interviewee A1) is concerned about being bombarded by marketing messages. The second is that people are worried about security, particularly with Internet and mobile banking and commerce, and the risk of being defrauded. However, the interviewee believes that people are not too careful about the information they share through social media, which gives them the impression that "if asked I'm conscious about security, but actually I'm not really that conscious about security on the day-to-day stuff" (interviewee A1). They feel this extends to consumers, who say they're concerned about privacy, but often don't act like they are. "Asking consumers if they are concerned about information security and seeing those answers against consumer behaviour reflects a conflict – because saying you are concerned is the 'right answer'", said interviewee A1; "often it's that convenience factor that trumps the fear of privacy".

South Africans are willing to provide information for benefits – the number of loyalty and rewards programmes on offers is evidence of this. However, "often the lack of context of how and where this information can be used and re-used is missing from consumers" (interviewee A1).

4.1.2.3. Protection of Personal Information 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 scrutinised in order 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.

4.1.3. Analysis

With the goal of Company A's strategy seemingly being a combination of survival and competitive advantage, the role of its strategy being a mix of all the sources of legitimacy, and its focus being on both internal and external stakeholders and processes, it is unclear which strategy it is employing in terms of the institutional approach and resource-based view paradigms.

Table 13: Analysis of Company A's information privacy strategy using the institutional approach and resource-based view paradigms

Theory ▶	Institutional Approach		Resource-based View	
Theory Attributes ▼	Acquiescence Strategy	Proactive Strategy	Customer Knowledge Capability	Customer Relationship Capability
Organisational Goal Argued By Theory Base	Survival [*]		Competitive advantage [*]	
Information Privacy Role in Achieving Organisational Goal	Source for pragmatic legitimacy [*]	Source for social legitimacy [*]	Support for differentiation through intellectual resource [*]	Support for differentiation through social resource [*]
Focus of Firm Information Privacy Activities	Internal [*]	External [*]	Internal [*]	External [*]
Information Privacy as a Mechanism for Achieving the Goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

The organisation views privacy as a risk. Considering this together with its simultaneous internal and external focus, its strategy in terms of the customer information privacy framework appears to lie somewhere between one of *minimum privacy activities* to avoid breach and *minimum privacy activities to avoid regulatory oversight*. This result is reinforced by (a) its privacy activities appearing to be primarily security focussed, (b) its approach to PoPI concentrating on preparation rather than implementation, (c) there being no information about its privacy policy on its website, and (d) its view that PoPI's changes offer no benefits.

Table 14: Analysis of Company A's information privacy strategy using the customer information privacy framework

	Internal Focus [*]	External Focus [*]
Risk [*]	**Minimum privacy activities to avoid breach [**]** *“Privacy is a distraction”*	**Minimum privacy activities to avoid regulatory oversight [**]** *“Privacy is just another compliance program”*
Opportunity	**Maximise privacy-based information collection / process improvement** *“Privacy is all about information management”*	**Maximise privacy-based customer relationships** *“Privacy is good ethics and good business”*

Company A appears to be following a *compromise* strategy in terms of the resistance dimension of the organisational privacy strategy framework, as it opposes or provides feedback on legislation through its industry bodies or directly to regulators. In terms of the proactivity dimension, the organisation seems to be following a *defender* strategy: it works ahead of legislation in order to protect its own operations, its self-defined practices are security-focussed, and it is in no rush to implement changes brought about by PoPI. Taken together, its overall strategy is one of a *conformist* seeking to maintain stability within the organisation.

Table 15: Analysis of Company A's information privacy strategy using the organisational privacy strategy framework

Privacy Strategies	Description	Resistance Dimension (Oliver)	Proactivity Dimension (Miles and Snow)
Conformist	Conforms to institutional requirements for the purpose of achieving organisational stability.	Acquiescence / Compromise	Reactor / Defender
Entrepreneur	Embraces a proactive approach and invests in privacy protection safeguards and strategies that account for regulators, investors, and customers.	Acquiescence / Compromise	Analyser / Prospector
Transformer	Carries out a proactive approach to privacy management and challenges institutional requirements by means of negotiation, manipulation, and bribery.	Defiance / Manipulate	Analyser / Prospector
Defender	Ignore, defend, or lobby against institutional pressures while trying to achieve organisational stability.	Defiance / Manipulate	Reactor / Defender

4.2. Case Study: Company B

4.2.1. Company, Interviewee and Interview Details

Company 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.

The table below provides a brief profile of the interviewees and some background details on the interviews.

Table 16: Interviewee profiles and details on the interviews for Company B

	Interviewee B1	Interviewee B2
Job Description	Head of information security. Responsible for information security strategy development.	Advises on legislation compliance within the company.
Experience in Position	Over 6 years.	Over 5 years.
Interview Audio Recorded?	Yes.	Yes.
Place of Interview	Company meeting room.	Company meeting room.
Additional Interview Details	The second interview question was re-answered via e-mail by the interviewer's request, as the interviewer felt it had been poorly asked and answered because of its complexity.	None.

4.2.2. Findings

The following are the findings for company based on the interviews and presented according to the grouping of the interview questions.

4.2.2.1. Informational Privacy Strategy Frameworks

While interviewee B1 suggested that this organisation'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: "there's going to be huge reputational [impact] as well because of the need to disclose any breaches in the legislation. And then, obviously, the competitive as well, is in there as well. I think they come together".

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 "I suppose it's always good to have customer feedback, but we're not I suppose as product-driven as maybe a full-out sales business".

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.

The organisation belongs to the Association for Savings and Investment South Africa (ASISA), which represents a range of financial services companies, including asset managers, investment firms and life insurance companies. The firm has very few self-defined policies on top of those prescribed by legislation and by the industry, particularly ASISA. Interviewee B2 notes that many of the company's practices are becoming standardised within the industry because of PoPI. One example of an additional practice that the firm has is its classification policy, which is used to classify the sensitivity of information in order to determine which controls need to be in place when accessing and using the information.

The firm provides a number of policies on its company group website, all in one section that is easy to locate. These cover, amongst other things, privacy when using the website, the protection of data provided to the company, communication terms and conditions, and disclosures required by and information on various regulations, including the PAIA. Most of these documents are written in plain English (rather than legal language). The data protection policy includes explanations in broad terms of what data may be collected, how it will be used, circumstances under which it may be disclosed, and how a customer may access the information.

Interviewee B1 sees privacy as being a risk, whereas interviewee B2 sees it as being both a risk and an opportunity. Interviewee B2 explains: "there's regulatory risk, there's risk of information leaks, fraud, that sort of thing, as [a] result. But it's an opportunity as well to make sure that the client experience is better through having accurate up-to-date information and through allowing us to, I suppose, evaluate what information we have on a client to improve their experience”. 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 “sometimes the regulation also just falls away, so, it's like, you waste your time and money and resources and then nothing happens”. PoPI, however, was an exception: not only has it existed for a number of 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.

The firm keeps up to date with legislation and the industry’s reaction to it through ASISA’s standing committee for PoPI, of which interviewee B2 is a member. Through ASISA the company provides feedback on legislation in order to align it with the industry, industry standards and the company’s business processes, and help make it practical to implement. Through the standing committee it has helped to draft an industry code, as allowed for by the PoPI Act, which will be presented to the Regulator once it has been established.

4.2.2.2. Customer

Privacy is of concern to South Africans, both interviewees say. Interviewee B1 said: “I often wonder where my information is, especially in the digital world that we're in. In my role, I'm constantly paranoid”, adding that they “see what happens and I see how they do it and how easy it is to do also”. Of concern to them is how PoPI is going to be enforced because though South Africa is good at creating regulations, enforcing them is often an issue as enforcement bodies can be overwhelmed with work. Interviewee B2 said privacy is of concern to the company’s clients; because they are wealthy they may be more concerned with privacy as they have more money to lose than lower-income individuals.

Interviewee B1 believes that the average South African is willing to provide any personal information in return for benefits and that South Africans are less conscious about privacy than citizens of other countries, such as the United Kingdom. Interviewee B2 thinks it depends on the type of information and benefits, as well as the sophistication and knowledge of the individual, which may be indicated by their financial status. They offer this example: “when fraud’s occurred often bank accounts are opened in the name of a third party and the common trend in the township is a fraudster will go and offer someone a thousand rand to open an account in their name and then give all the banking details to, you know… So that’s an example of real, sensitive personal information being bought for a thousand rand, whereas you’re not going get that with a high net-worth individual”.

4.2.2.3. Protection of Personal Information 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. In particular, 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 explains: “we do what we can when we’re certain on certain areas and we tweak as it gets closer. So now when I say we’re fully compliant, but we’re fully compliant on our interpretation of it. When a Regulator is established, regulations are issued, and inspections are done, obviously there may be different interpretations. We may need to adjust then”. They add: “the Act is based on principles and if you're going to have principles it’s difficult then to prescribe rules and regulations because the principle should give you leeway. The regulation should just provide guidance, nothing more. Like FICA [the Financial Intelligence Centre Act], the regulation has actually been hard core rule-based. Hopefully they won't do that in PoPI”.

On the practical side, the handling of “unstructured data” that sits in documents and spread sheets is an area the company needs to do more work on. From a project perspective, interviewee B2 notes that implementing change can be difficult because it requires time from people who already have a large volume of day-to-day work to handle.

One benefit of PoPI compliance is that it can be marketed to South African customers in order 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. Interviewee B1 goes further and said “it would be nice for PoPI to be enforced and [for us to be able to] say we apply all the rules and we're complying with the regulatory requirements”. 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.

4.2.3. Analysis

The goal of Company B's approach to information privacy appears to be a combination of survival and competitive advantage – it is not clearly one of the other. The role of its privacy strategy is also a combination of the forms of legitimacy, though intellectual differentiation plays less of a role than the other forms. Its focus is external, primarily on customers and regulations.

Considering these elements using the institutional approach and resource-based view paradigms, it's not clear which strategy Company B is applying – it could be the *proactive strategy* or the *customer relationship capability*, or possibly a combination of the two.

Table 17: Analysis of Company B's information privacy strategy using the institutional approach and resource-based view paradigms

Theory ▶	Institutional Approach		Resource-based View	
Theory Attributes ▼	Acquiescence Strategy	Proactive Strategy [**]	Customer Knowledge Capability	Customer Relationship Capability [**]
Organisational Goal Argued By Theory Base	Survival [*]		Competitive advantage [*]	
Information Privacy Role in Achieving Organisational Goal	Source for pragmatic legitimacy [*]	Source for social legitimacy [*]	Support for differentiation through intellectual resource	Support for differentiation through social resource [*]
Focus of Firm Information Privacy Activities	Internal	External [*]	Internal	External [*]
Information Privacy as a Mechanism for Achieving the Goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

The company appears to view privacy as being both a risk and an opportunity, possibly leaning more towards it being a risk. Taking this into account together with its focus on external stakeholders and processes, the organisation's strategy according to the customer information privacy framework is once again not clear cut: it appears to fall somewhere between the *minimum privacy activities to avoid regulatory oversight* strategy and the *maximise privacy-based customer relationships* one.

Table 18: Analysis of Company B's information privacy strategy using the customer information privacy framework

	Internal Focus	External Focus [*]
Risk [*]	**Minimum privacy activities to avoid breach** *“Privacy is a distraction”*	**Minimum privacy activities to avoid regulatory oversight [**]** *“Privacy is just another compliance program”*
Opportunity [*]	**Maximise privacy-based information collection / process improvement** *“Privacy is all about information management”*	**Maximise privacy-based customer relationships [**]** *“Privacy is good ethics and good business”*

Though the firm does comply with institutional pressure, it does not simply acquiesce: it provides feedback on legislation and helps to improve it and make it practical. So, in terms of the resistance dimension of the organisational privacy strategy framework, the organisation appears to be following the *compromise* strategy. How proactive the company is unclear though: while it does review and assess the impacts of new legislation, it does not implement changes until the legislation is close to being finalised. It also does not appear to have much in the way of self-defined policies and practices. Once again, its type of strategy is a mix: it seems to fall between being a *defender* and an *analyser*.

Overall, Company B's strategy appears to fall between that of the *conformist* and the *entrepreneur*.

Table 19: Analysis of Company B's information privacy strategy using the organisational privacy strategy framework

Privacy Strategies	Description	Resistance Dimension (Oliver)	Proactivity Dimension (Miles and Snow)
Conformist [**]	Conforms to institutional requirements for the purpose of achieving organisational stability.	Acquiescence / Compromise [*]	Reactor / Defender [*]
Entrepreneur [**]	Embraces a proactive approach and invests in privacy protection safeguards and strategies that account for regulators, investors, and customers.	Acquiescence / Compromise [*]	Analyser / Prospector [*]
Transformer	Carries out a proactive approach to privacy management and challenges institutional requirements by means of negotiation, manipulation, and bribery.	Defiance / Manipulate	Analyser / Prospector [*]
Defender	Ignore, defend, or lobby against institutional pressures while trying to achieve organisational stability.	Defiance / Manipulate	Reactor / Defender [*]

4.3. Case Study: Company C

4.3.1. Company, Interviewee and Interview Details

This global organisation 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.

The table below provides a brief profile of the interviewees and some background details on the interviews.

Table 20: Interviewee profiles and details on the interviews for Company C

	Interviewee C1	Interviewee C2
Job Description	Information protection officer – oversees and encourages company compliance with information protection principles.	Accountable for the company’s data and data management; previously chaired the company’s PoPI implementation project.
Experience in Position	Over 5 years.	Over 6 years.
Interview Audio Recorded?	Yes.	Yes.
Place of Interview	Company meeting room.	Interviewee’s company office.

	Interviewee C1	Interviewee C2
Additional Interview Details	The second interview question was re-answered via e-mail by the interviewer's request, as the interviewer felt it had been poorly asked and answered because of its complexity.	The interview also attended by second person who was shadowing the interviewee. They were engaged by the interviewee on a few occasions, but did not participate in the interview directly.

4.3.2. Findings

The following are the findings for company based on the interviews and presented according to the grouping of the interview questions.

4.3.2.1. Informational Privacy Strategy Frameworks

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 seen as an organisation 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 emphasised the importance of data to the company several times in the interview, saying at one point: "as an organisation we've always had a very strong culture around data – very strong; in the extreme strong".

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.

Company C has several self-defined privacy practices on top of the industry's standards and codes. The organisation has numerous sets of policies and guidelines, some of which are stipulated by its head office (which is outside of South Africa), others of which are written when interviewee C1 notices that they are receiving many questions on a particular topic. There is also a code of conduct which employees must comply with and annually attest to. This code includes a policy on data usage and access and is reinforced through online training and communications, some of which are general, some of which are tailored to the different business units and their operations. The firm also has a clean desk policy – employees must not leave sensitive documents on their desks but must rather lock them away. Communal printers also now require a personal code to be entered before print jobs are run in order to prevent printed documents being left at these printers. The firm is in the process of disabling all USB ports and has implemented e-mail sniffers (a sniffer is a piece of software or hardware that intercepts, analyses and logs traffic over a network), both aimed at preventing sensitive information being sent outside of the organisation. It has also modified its asset management process so that if an item such as a laptop is lost, one step of the process involves ensuring that it is reported as a possible breach so that the incident can be investigated.

The organisation has an extensive section covering governance issues on its website. It provides information on all its member companies (business units), its company financials, its regulatory bodies, details on how to complain and report fraud, various company policies, a PAIA user guide (written by the PAIA Unit of the South African Human Rights Commission), disclosures according to various acts including PAIA and PoPI, and copies of various Acts. One of its policies covers customer privacy and explains in broad terms what data the firm may collect, how the data may be used, circumstances under which it may be disclosed, how the data is safeguarded, and how a customer can access and correct this data.

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 my competitors then I have got strategic advantage".

The organisation "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 "analyse it and determine the impact, see if, does it make sense, does it not make sense, do we agree, do we not agree, and we provide input via ASISA – our industry body – or sometimes we go directly to the regulators, depending on the nature of the concerns involved” (interviewee C1). 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.

4.3.2.2. Customer

Up until now, privacy hasn’t been of major concern to South Africans, according to interviewee C1; both consumers and those who handle other people’s information have been “blasé” about the issue. However, there is now a growing awareness of it, particularly in light of identity theft becoming a greater problem.

Interviewee C2 believes that education plays a major role in this and that “the average European is far better educated about these things than the average South African”. In their view, “middle and upper classes are hacked off that their phones can get messages all the time. I think at the lower end of the spectrum they think that’s just normal”. They went on to say: “if I was the Regulator, I would go for a big breach early. I would like to make a big splash to give the industry a bit of a slap and a wake-up call, and also to get some publicity going in the public domain”. They noted that in the past six months they have received a large amount of direct marketing on their phone, possibly because companies with large databases are making use of those databases while they still can (before the legislation begins to be enforced), and this may make people wary of sharing their cell phone numbers.

Whether or not South Africans are willing to provide personal information in return for benefits depends on how it the proposition is positioned and exactly what those benefits are, in interviewee C1’s opinion. For instance, sharing information with or selling it to third parties would serve as a deterrent. Interviewee C2 is more inclined to trust companies, but thinks that perhaps “people will share if they haven’t been burnt or if they haven’t heard of anyone who’s been burnt”. They added that South Africans are probably more aware of scams and phishing attempts because of the large amount of phishing that happens in the banking industry.

Interview C1 believes that PoPI will make a difference to the company’s customer base because “if they feel safe or they feel that we will treat their information in a responsible manner, I think they would be more inclined to give it to us than not”.

4.3.2.3. Protection of Personal Information Act

There is far more focus on Company C's information privacy strategy now because of PoPI, and it has become more formalised. 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 said there is "much more action now, there's lots more movement – more focus and awareness. 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 standardised.

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 organisation and ensure that it was given attention by senior executives.

The biggest challenge in implementing PoPI is the size of the organisation 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 has to be regularly performed on each vendor – a future issue because "we just don't have those resources to send teams to all our vendors". To try to deal with this, each vendor is being given a risk rating in order 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 Protection of Personal Information Act (Act No. 4 of 2013) (2013), which governs security safeguards, is having a big impact because of its scope. The organisation 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 organisation and continuous communication and training required to ensure that employees, both new and current, are kept aware of it.

One area of uncertainty is the length of time for which data can be kept. The firm has several hundred systems and the problem is that “mapping out which systems access those data and inadvertently deleting some of that data, thinking you're doing a good thing and meanwhile there's a system that uses pieces of some of those fields... It was just extremely complicated” (interviewee C1). 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. So I would hope that [post-PoPI] the industry will be doing less business possibly, definitely doing it differently, but hopefully better business with better informed customers. That would be an ideal outcome”.

Another benefit is that certain processes have been improved – for example, the organisation’s “asset management process was cleaned up as a result of PoPI, so it works more effectively” (interviewee C1).

4.3.3. Analysis

While the interviewees initially said that Company C's approach to information privacy is somewhere between survival and competitive advantage, they both later said that if the company's approach is correct, it will have competitive advantage. (Interviewee C1 said “it's being seen as a competitive advantage if you get it right”, while interviewee C2 said “if our construct allows us to cross sell easier than my competitors then I have got strategic advantage”.) It therefore appears that the firm's goal is actually to achieve competitive advantage.

While information privacy has various roles in the organisation, intellectual differentiation appears to be the primary one given the organisation's focus on data. The focus of the company's information privacy activities is internal stakeholders and processes.

Therefore, when examined using the institutional approach and resource-based view paradigms, the company's information privacy strategy appears to be one of *customer knowledge capability*.

Table 21: Analysis of Company C's information privacy strategy using the institutional approach and resource-based view paradigms

Theory ▶	Institutional Approach		Resource-based View	
Theory Attributes ▼	Acquiescence Strategy	Proactive Strategy	Customer Knowledge Capability [**]	Customer Relationship Capability
Organisational Goal Argued By Theory Base	Survival		Competitive advantage [*]	
Information Privacy Role in Achieving Organisational Goal	Source for pragmatic legitimacy	Source for social legitimacy	Support for differentiation through intellectual resource [*]	Support for differentiation through social resource
Focus of Firm Information Privacy Activities	Internal	External	Internal [*]	External
Information Privacy as a Mechanism for Achieving the Goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

Privacy is seen as both a risk and an opportunity by the company. Viewed together with the firm's internal focus, in terms of the customer information privacy framework, the firm is either following a strategy of *minimum privacy activities to avoid breach* or *maximise privacy-based information collection / process improvement*. However, when the description of the latter strategy as laid out in Table 4 is read and compared to the information provided by the interviewees, there is little doubt that this is the strategy that the company is following. Elements that ring true include:

- Reputational Aims: Use privacy practices to maintain reputation.
- Organisational Culture: Refer to privacy in documents about corporate values and/or ethics or code of conduct.

- Intended Outcomes (of privacy implementation choices): Improve accuracy of customer profiles.
- Customer Information and Privacy Linkages: Use privacy policy to improve collection of and permission to use customer information.

Table 22: Analysis of Company C's information privacy strategy using the customer information privacy framework

	Internal Focus [*]	External Focus
Risk [*]	**Minimum privacy activities to avoid breach** *"Privacy is a distraction"*	**Minimum privacy activities to avoid regulatory oversight** *"Privacy is just another compliance program"*
Opportunity [*]	**Maximise privacy-based information collection / process improvement [**]** *"Privacy is all about information management"*	**Maximise privacy-based customer relationships** *"Privacy is good ethics and good business"*

Company C does offer some resistance to institutional pressure by providing feedback on legislation, either directly to legislators or through industry bodies. However, it does comply with legislation. It therefore appears to be following the *compromise* strategy. At the same time it is proactive and working to adapt to the new environment, though it does not appear to be going as far as looking for new opportunities – it appears to be trying to maintain and possibly strengthen its existing position. This makes it an *analyser* in terms of the proactivity dimension of the organisational privacy strategy framework. Overall, it appears to be following an *entrepreneur* privacy strategy.

Table 23: Analysis of Company C's information privacy strategy using the organisational privacy strategy framework

Privacy Strategies	Description	Resistance Dimension (Oliver)	Proactivity Dimension (Miles and Snow)
Conformist	Conforms to institutional requirements for the purpose of achieving organisational stability.	Acquiescence / Compromise [*]	Reactor / Defender
Entrepreneur [**]	Embraces a proactive approach and invests in privacy protection safeguards and strategies that account for regulators, investors, and customers.	Acquiescence / Compromise [*]	Analyser / Prospector [*]
Transformer	Carries out a proactive approach to privacy management and challenges institutional requirements by means of negotiation, manipulation, and bribery.	Defiance / Manipulate	Analyser / Prospector [*]
Defender	Ignore, defend, or lobby against institutional pressures while trying to achieve organisational stability.	Defiance / Manipulate	Reactor / Defender

4.4. Case Study: Company D

4.4.1. Company, Interviewee and Interview Details

Company 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.

The table below provides a brief profile of the interviewee and some background details on the interview. Unfortunately, it was not possible to arrange an interview with a second person.

Table 24: Interviewee profile and details on the interview for Company D

	Interviewee D1
Job Description	Information security officer.
Experience in Position	Over 2 years.
Interview Audio Recorded?	No – interviewee declined. Notes taken by interviewer.
Place of Interview	Company meeting room.
Additional Interview Details	The second interview question was re-answered via e-mail by the interviewer's request, as the interviewer felt it had been poorly asked and answered because of its complexity.

4.4.2. Findings

The following are the findings for company based on the interview and presented according to the grouping of the interview questions.

4.4.2.1. Informational Privacy Strategy Frameworks

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, in particular customers and regulations. The company ultimately views privacy as a risk.

When asked whether Company D has any of its own self-defined privacy practices on top of the industry's standards and codes, the interviewee noted that they can only answer from an information security point of view. The organisation applies the principle of least privilege, where an employee gets access only to the information they need for their role. It also has various non-disclosure agreements that employees must sign and it is regularly audited by external auditors. Overall, the firm has a culture of privacy and its employees do not readily provide information, even to others in the company (as has been noticed when group meetings are held).

The firm provides a limited set of policies on its website. Its privacy and data protection policy provides high-level details that are not country specific. It does, however, provide a complaints policy specific to the South African Financial Advisory and Intermediary Services Act and a PAIA manual.

The organisation 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.

4.4.2.2. Customer

In the interviewee's opinion, privacy is not of concern to South Africans – the interviewee believes that people readily share their information. Whereas privacy is ingrained in European Union citizens (for example), this is not so in South Africans, though they are becoming more aware because of legislation such as the Consumer Protection Act (and it is the interviewee's hope that PoPI will do the same). The interviewee also believes that South Africans are probably willing to provide personal information in return for benefits, feeling that the "man on the street" is susceptible to scams, and that it will take education and time to change this.

PoPI will make a difference to Company D's client base, as it will mean that South Africa will be operating under a privacy law that is equivalent to those overseas, which will in turn facilitate offshoring.

4.4.2.3. Protection of Personal Information Act

The Act has affected the firm in several ways: implementing the technologies and support for these technologies has had a financial impact; new security has been implemented as a result 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 has to 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. As mentioned above, 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 labour than some other countries). A possible future benefit may be PoPI compliance certification, should this ever be created.

4.4.3. Analysis

With its goal in its approach to information privacy being a combination of both survival and competitive advantage, Company D appears to fit in both the institutional approach and resource-based view paradigms. However, given that its information privacy strategy role is to ensure relationship differentiation and the focus of its privacy activities being external processes and stakeholders (customers and regulations), it seems to best fit the *customer relationship capability* strategy.

Table 25: Analysis of Company D's information privacy strategy using the institutional approach and resource-based view paradigms

Theory ▶	**Institutional Approach**		**Resource-based View**	
Theory Attributes ▼	**Acquiescence Strategy**	**Proactive Strategy**	**Customer Knowledge Capability**	**Customer Relationship Capability [**]**
Organisational Goal Argued By Theory Base	Survival [*]		Competitive advantage [*]	
Information Privacy Role in Achieving Organisational Goal	Source for pragmatic legitimacy	Source for social legitimacy	Support for differentiation through intellectual resource	Support for differentiation through social resource [*]
Focus of Firm Information Privacy Activities	Internal	External	Internal	External [*]
Information Privacy as a Mechanism for Achieving the Goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

When evaluated using the customer information privacy framework, the company looks to be following the strategy of *minimum privacy activities to avoid regulatory oversight* because of its external focus and its view that privacy is a risk.

Table 26: Analysis of Company D's information privacy strategy using the Customer Information Privacy Framework

	Internal Focus	External Focus [*]
Risk [*]	**Minimum privacy activities to avoid breach** *“Privacy is a distraction”*	**Minimum privacy activities to avoid regulatory oversight [**]** *“Privacy is just another compliance program”*
Opportunity	**Maximise privacy-based information collection / process improvement** *“Privacy is all about information management”*	**Maximise privacy-based customer relationships** *“Privacy is good ethics and good business”*

Analysing Company D’s strategy using the organisational privacy strategy framework, the firm appears to be applying an *entrepreneur* privacy strategy. On the resistance dimension, it does not oppose legislation, preferring instead to simply implement it – in other words, it follows an *acquiescence* strategy when dealing with institutional pressure. On the proactivity dimension, while it is a proactive organisation, because it views privacy as a risk rather an opportunity it is more likely to be an *analyser* than a *prospector*.

Table 27: Analysis of Company D's information privacy strategy using the Organisational Privacy Strategy Framework

Privacy Strategies	Description	Resistance Dimension (Oliver)	Proactivity Dimension (Miles and Snow)
Conformist	Conforms to institutional requirements for the purpose of achieving organisational stability.	Acquiescence / Compromise [*]	Reactor / Defender
Entrepreneur [**]	Embraces a proactive approach and invests in privacy protection safeguards and strategies that account for regulators, investors, and customers.	Acquiescence / Compromise [*]	Analyser / Prospector [*]
Transformer	Carries out a proactive approach to privacy management and challenges institutional requirements by means of negotiation, manipulation, and bribery.	Defiance / Manipulate	Analyser / Prospector [*]
Defender	Ignore, defend, or lobby against institutional pressures while trying to achieve organisational stability.	Defiance / Manipulate	Reactor / Defender

4.5. Case Study: Company E

4.5.1. Company, Interviewee and Interview Details

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

The table below provides a brief profile of the interviewees and some background details on the interviews.

Table 28: Interviewee profiles and details on the interviews for Company E

	Interviewee E1	Interviewee E2
Job Description	Management of IT security and business continuity.	Project manager for the company's PoPI project.
Experience in Position	Over 4 years.	Unknown, but has been at the company for over 7 years.
Interview Audio Recorded?	Yes.	Yes.
Place of Interview	Company meeting room.	Company meeting room.
Additional Interview Details	None.	None.

4.5.2. Findings

The following are the findings for company based on the interview and presented according to the grouping of the interview questions.

4.5.2.1. Informational Privacy Strategy Frameworks

The goal of Company E's privacy strategy is neither survival nor competitive advantage, according to both of the 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 organisation 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 organisation's information privacy strategy is a source for all four forms of legitimacy. However, social legitimacy and relationship differentiation may be the most important of the four, 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 centre of it all, but third parties are also a major focus: the organisation is working to standardise the management of vendors across the company, which includes improving the rigor of contracts with these parties, and analysing how data is shared with vendors and brokers.

The organisation aligns its security practices with the International Organization for Standardization (ISO) 27001, which is a specification for an information security management system, though it does not have certification for this standard. The company has assessed its level of concern around various data and instituted controls to limit access to them. Data masking and de-identification has been in place in the firm's software development environment for several years. A plain English, single page privacy policy is provided on the company's website, together with its PAIA manual. This policy covers, at a high level, the use, sharing and security of personal information.

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 explains: "some legislation is more important than others, in our opinion or in our business, and then we're a lot more proactive with it, and others you really don't want to be a kind of leader in that thing". In the case of PoPI, the organisation 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.

The company is a member of several industry bodies, including ASISA, where it sits on the PoPI standing committee. It regularly provides feedback on legislation through these bodies. "For most legislation that affects us we'll try and have some say in the way it's implemented", said interviewee E2.

4.5.2.2. Customer

Interviewee E1 is of the opinion that the majority of South Africans are not concerned about privacy. They think that perhaps most people are “mainstream” and their information is not interesting, and therefore they are not concerned about it, whereas the “fringe” people in society are more readily focussed on and concerned about their privacy. They added that the general inefficiency in businesses often drives repeated requests for information (such as copies of ID books) and that South Africans have become used to complying with these requests in order to get service. The interviewee feels that the irritation caused by direct marketing messages is where the concern about privacy often stems from. They also think that “PoPI is something that’s been forced on us” (interviewee E1); however, they also think “it’s good that people become more responsible with the data that they’re got” (interviewee E1). Interviewee E2 believes that privacy is of concern to South Africans, especially when it comes to direct marketing, but that some more readily act on that concern than others.

Interviewee E2 said that people are definitely prepared to offer personal information in return for benefits, the evidence being the many loyalty and reward cards and discounts on offer from companies.

Privacy is of concern for some customers, but for others it is not; either way, the company does work to act in its clients’ best interests and protect them. Interviewee E2 believes that PoPI will not make a difference to the firm’s customers, primarily because of its good reputation. However, PoPI will make it easier to do business with international companies because it will enable trans-border information flows.

4.5.2.3. Protection of Personal Information Act

The PoPI Act is not bringing about any major changes to Company 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 (as mentioned above), 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, categorising them according to risk, and then assessing their approach and security in order 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; it will also act on any additional regulations that the Regulator may stipulate.

Another area that the firm is working on is its policy documentation around personal information and privacy, which is currently being consolidated and “cleaned up”.

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 in order 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.

4.5.3. Analysis

The goal of the organisation's information privacy strategy is neither survival nor competitive advantage, but is instead to best serve its customers and maintain their trust. The strategy aims to achieve all the forms of legitimacy, social legitimacy and relationship differentiation appear to be the most important ones. The firm's privacy activities focus on both internal and external processes and stakeholders. When analysed using the institutional approach and resource-based view paradigms, Company E appears to have either a *proactive strategy* or a *customer relationship capability* strategy. However, considering that the firm does not try to be a leader when it comes to its privacy practices (as a company following a *proactive strategy* would), but it does heavily depend on having superior customer trust, it is very likely following the *customer relationship capability* strategy.

Table 29: Analysis of Company E's information privacy strategy using the institutional approach and resource-based view paradigms

Theory ▶	**Institutional Approach**		**Resource-based View**	
Theory Attributes ▼	**Acquiescence Strategy**	**Proactive Strategy**	**Customer Knowledge Capability**	**Customer Relationship Capability [**]**
Organisational Goal Argued By Theory Base	Survival		Competitive advantage	
Information Privacy Role in Achieving Organisational Goal	Source for pragmatic legitimacy	Source for social legitimacy [*]	Support for differentiation through intellectual resource	Support for differentiation through social resource [*]
Focus of Firm Information Privacy Activities	Internal [*]	External [*]	Internal [*]	External [*]

Information Privacy as a Mechanism for Achieving the Goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

Privacy is seen as a risk or an opportunity by the company, depending on who one speaks to, and the organisation has both an internal and an external focus. Given this, it could be following any of the strategies indicated by the customer information privacy framework. However, given the emphasis of the customer being central to all its actions, as well as the emphasis on "doing the right thing", the company's privacy strategy is almost certainly to *maximise privacy-based customer relationships*.

Table 30: Analysis of Company E's information privacy strategy using the customer information privacy framework

	Internal Focus [*]	**External Focus [*]**
Risk [*]	**Minimum privacy activities to avoid breach** *"Privacy is a distraction"*	**Minimum privacy activities to avoid regulatory oversight** *"Privacy is just another compliance program"*
Opportunity [*]	**Maximise privacy-based information collection / process improvement** *"Privacy is all about information management"*	**Maximise privacy-based customer relationships [**]** *"Privacy is good ethics and good business"*

Company E appears to be following the *compromise* strategy of the resistance dimension of the organisational privacy strategy framework, as it provides feedback on legislation and helps to improve it. In terms of the proactivity dimension, the *analyser* strategy seems to best fit the firm: it is flexible and seeks to protect customer against foreseen threats, but it does not use its privacy activities to actively compete for new customers (as a company with a *prospector* strategy would). Therefore, overall, its strategy appears to be one of the *entrepreneur*.

Table 31: Analysis of Company E's information privacy strategy using the organisational privacy strategy framework

Privacy Strategies	Description	Resistance Dimension (Oliver)	Proactivity Dimension (Miles and Snow)
Conformist	Conforms to institutional requirements for the purpose of achieving organisational stability.	Acquiescence / Compromise [*]	Reactor / Defender
Entrepreneur [**]	Embraces a proactive approach and invests in privacy protection safeguards and strategies that account for regulators, investors, and customers.	Acquiescence / Compromise [*]	Analyser / Prospector [*]
Transformer	Carries out a proactive approach to privacy management and challenges institutional requirements by means of negotiation, manipulation, and bribery.	Defiance / Manipulate	Analyser / Prospector [*]
Defender	Ignore, defend, or lobby against institutional pressures while trying to achieve organisational stability.	Defiance / Manipulate	Reactor / Defender

4.6. Discussion of Findings

Of the companies researched, the goals of four of five in their approaches to information privacy are a mixture of survival and competitive advantage, though Company C's approach can be interpreted as actually being competitive advantage. For Company E it is neither. Four of the companies 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.

All of the organisations have some self-defined privacy practices on top of industry standards and codes. Whether privacy is seen as a risk or an opportunity generally depends on who you ask in the company 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 organisations, but, depending on the particulars piece of legislation, only some extend this proactive approach to implementing changes in actuality.

The strategic approach of each company was analysed and classified using the three frameworks; a summary of this is provided in Table 32.

Table 32: Summary of the strategic approaches to information privacy of the subject companies as classified using the theoretical frameworks

Theory ▶ *Company* ▼	Institutional Approach and Resource-based View Paradigms	Customer Information Privacy Framework	Organisational Privacy Strategy Framework
A	*Unclear*	Minimum privacy activities to avoid breach Minimum privacy activities to avoid regulatory oversight	Conformist
B	Proactive Strategy Customer Relationship Capability	Minimum privacy activities to avoid regulatory oversight Maximise privacy-based customer relationships	Conformist Entrepreneur
C	Customer Knowledge Capability	Maximise privacy-based information collection / process improvement	Entrepreneur
D	Customer Relationship Capability	Minimum privacy activities to avoid regulatory oversight	Entrepreneur
E	Customer Relationship Capability	Maximise privacy-based customer relationships	Entrepreneur

Several of the companies have a strategy that does not conform to a single approach in each of the frameworks, suggesting that they are employing hybrid strategies. In the case of Company A and the institutional approach and resource-based view paradigms, it was not possible to classify the firm's strategy at all; having a second interviewee may have helped to rectify this defect.

When examined using the institutional approach and resource-based view paradigms, the majority of companies appear to be primarily using customer information as a resource in order to achieve customer advantage, despite them saying that the goals of their strategies are a mix of survival and competitive advantage. Companies A and B are exceptions: Company A's strategy is unclear in terms of this framework and Company B has a hybrid approach through which it aims to survive by conforming institutional pressures and thrive by improving its relationships with customers. It is likely that more data is required in order to clarify Company A's approach.

The subject companies employ the full range of strategies suggested in the customer information privacy framework. Three of them appear to have a strategy that combines elements from two strategic approaches.

The companies' strategies exhibited very few differences when examined using the organisational privacy strategy framework. This could be a result of the particular firms selected for this project or perhaps it arises from the fact that this research was performed in the financial services industry in South Africa, whereas the base research for the paper it is presented in was performed in the healthcare industry in the US. Another possibility is that the framework is too extreme in its assessment of the reaction of firms to institutional pressures and resistance thereto: the avoidance, defiance and manipulation strategy types of the resistance dimension involve active measures to avoid compliance or challenge legislation or interfere with enforcement of it. However, it is also unlikely that an Honours research project would be able to uncover actions of this nature.

There are mixed opinions as to whether or not privacy is of concern to South Africans. Some of the interviewees believe that it is of concern; some believe it is a concern in theory (perhaps because being concerned is seen as being the "right" thing to be), but not in practice; and others believe it's not of concern, possibly because people believe they and their information are fundamentally not very interesting. The issues of privacy not being ingrained in South African culture (whereas it is in other areas of the world) and the level of education and its effect on privacy decisions were also raised. Those interviewees who think privacy is not a topic of concern generally believe this is changing as awareness of it grows. The issue of direct marketing and the irritation it causes was also mentioned by several interviewees as a possible causal factor.

South Africans are definitely prepared to provide personal information in return for benefits, but what and how much information they provide is determined by their level of knowledge and sophistication as well as the type of benefits they will receive in return. In other words, individuals will perform privacy calculus and weigh up the risks and benefits of providing information. PoPI will make a difference for some customers, particularly those who are concerned about privacy; it will also make a difference to foreign customers, who will be comforted by knowing that South Africa has data protection legislation that is world-class.

The perceived disconnect between peoples' concerns and actions, as well as the effect of education, knowledge and experience on their decisions, echoes factors mentioned in the literature about the complexities an individual faces when making decisions about their privacy.

PoPI has influenced all of 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 in order 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.

The Act poses a fair number of challenges. Perhaps the greatest of these lies in it being principle-based and relying on interpretation. This may change when the Regulator is created, as it may propose more specific regulations; but 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 that the size of a company and its operations can influence the implementation of changes and cause delay; getting people in the organisation to accept of changes can be problematic; and installing new security technology 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 in order 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 will have to give consent for it because they are interested in receiving product and service offers, thus reducing wasted effort on the company’s side and irritation on the customer’s.

The findings of the project were reported, analysed and discussed in this chapter. The subject companies employ a range of strategies, most of which appear to conform to a single approach in each framework, but in some cases appear to be a mix of two approaches. Opinions on whether privacy is of concern to South Africans and whether PoPI will make a difference to customers are mixed, but it was agreed that South Africans are willing to offer personal information in return for benefits, though there are factors that affect this decision. PoPi has influenced the companies to varying degrees and poses challenges for them, but in general they do also see benefit in complying with it.

The next chapter concludes the report by summarising its contents, discussing the project as a whole, and providing some recommendations based on its findings.

CHAPTER 5.
CONCLUSION

This final chapter of the report begins by summarising the project. Following this, a discussion of what can be learned from this research is presented. Finally, some recommendations for future research are made.

5.1. Summary

In today’s technology-driven society, computer systems are used to track, store and process a variety of details on us and our daily lives. We seek privacy yet also disclose personal information using technology in order to obtain services and build friendships. The problem is that once this information is in a computer system, it can easily be shared and used for any number of purposes, legitimate and nefarious. As a consequence of this, the safety of this information has become of great importance to us all.

Numerous public incidents involving large companies and the personal information of millions of people have helped to bring the topic of privacy to the fore and promote the need for legislation to govern it. South Africa has recently enacted the Protection of Personal Information (PoPI) Act, which aims to regulate how organisations of all sizes handle, store and secure information, and offers harsh penalties for failure to comply with it. Though it has been signed into law, it is not yet being enforced, though this is expected to change very soon.

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. It is these strategies that this research project aimed at examining in order to answer the question: what informational privacy strategies are used by corporates in the South African financial services industry? Though similar research has been performed in other countries, none has been performed and published in South Africa.

The literature reviewed for this project is discussed in chapter 2. Starting with the basics on privacy and personal information, it shows that privacy is a concept that is complex, multi-disciplinary, and influenced by many parts of society's environment, which means that it is ever-evolving. Today it is synonymous with personal information. There are several theories about the information of privacy and those examined indicate that an important feature is an individual's ability to limit access to their information.

Privacy is important for both consumers and organisations alike. Consumers are concerned about issues like improper access to and use of personal information, as well as its collection and the possibility of errors in that information. For individuals, making decisions about privacy is a complex process that involves numerous factors and difficulties, including that of weighing up the benefits of revealing information with the cost of doing so. The outcome of this process may not be optimal or may even be paradoxical if the individual's actions do not match their intentions. Issues such as the secondary use of information, identity theft and data breaches increasingly are of concern to individuals and can impact their privacy decisions.

Organisations can see privacy as a risk or an opportunity. A company that views it as a risk aims at avoiding potential trouble by complying with regulations. Privacy issues can be bad for business and affect a firm's share price, lead to a loss of customers, and result in fines and other costs, all of which affect its bottom line. On the other hand, a company can view privacy as an opportunity to gain new customers, improve efficiency and reduce operating expenses. Building trust with customers can lead to competitive advantage and customers are more likely to share information with companies they trust.

Three frameworks that can be used to analyse the strategies and behaviours of firms in respect of informational privacy were studied and used in this research. The first combines two paradigms: the institutional approach paradigm, which considers the effects of the external environment and its forces on organisations, 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 organisational privacy strategy framework, blends two frameworks, one of which looks at the organisation's response to institutional pressures, while the other examines how proactive the organisation's strategy is.

The methods used in carrying out the research for this project are outlined in chapter 3. The project used a mixed approach known as *deductive qualitative analysis* in which theory is used as a base for qualitative research. The research was performed using multiple case studies, with the unit of analysis being a single company. The research sample included five organisations from the financial services industry. Data was collected through interviews with senior management at the subject firms; at two companies single interviews were performed and at the other three firms two were conducted. The interviews were semi-structured and based on an interview guide containing twelve open-ended questions. They were audio recorded if the interviewee consented to it (which all but one did) and these recordings were later transcribed. The interviews and other collected data were analysed using qualitative analysis software and thematic analysis, which is a method for identifying, analysing and reporting patterns (themes) within data. The themes used in this analysis were taken from the frameworks mentioned before.

The findings of the research are detailed and discussed in chapter 4. Each case study covers the information learned through interviews about a single company's informational privacy strategy together with its perceptions of customers and their concerns about privacy, and some of impacts that PoPI has had on the organisation. This information was then analysed in order to determine the approach of the company according to each framework.

It was found that the companies employ a variety of approaches when implementing information strategies. In several cases a company's strategy did not conform to just one approach, suggesting that it is employing a hybrid strategy that contains elements of two approaches. In one case, under one framework, it is unclear which strategy is being employed, possibly because more data on the company is required. The companies exhibit few differences when analysed using the organisational privacy strategy framework; several possible causes for this are discussed.

Questions about whether or not privacy is of concern to South Africans and whether or not PoPI will make a difference to customers yielded mixed opinions. However, the opinions on whether South Africans in general are prepared to offer personal information in return for benefits were unanimously positive, though factors that affect the decision were suggested.

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 a number of 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 organisations it appears to offer benefits, such as the opportunity to bring more international business to South Africa.

5.2. Discussion

The process of collecting information by means of interviews yielded a rich level of detail. It is a time-consuming approach, with accurate transcription in particular taking a significant amount of time and effort, but its strength lies in being able to probe responses and collect background and tangential information that falls outside of the boundaries created by questions, and thereby construct a fuller, more worthwhile picture. Through this the researcher can achieve an understanding of the context of the information provided and thus better interpret it.

Analysis of the collected data was a relatively quick process, as the frameworks provided themes that were used to structure the interview questions and analyse the responses, and analysis software helped with the work. Writing case studies based on this analysis was a lengthier task, but the result allows one to compare the subject companies and determine their similarities and differences.

This project's research process could have been improved in two ways in particular. Firstly, as the project progressed it became apparent that it would have been ideal to have subjects from several different areas in each organisation in order to get a wider variety of perspectives and better insight into how those areas view and execute the company's privacy strategy. A good mix would probably have been one subject from the pure business area, one from the legal or compliance division, and one from IT. Secondly, some of the interview questions could be improved. The second question, which asks about the role of the firm's strategy in achieving its goal in its approach to information privacy, is very theoretical and initially was poorly responded to. When the interviewees were offered options they were able to respond appropriately. Question eight also was problematic and in effect should have been two questions: one about whether PoPI will make a difference to the firm's customer base, the other about whether the interviewee thinks privacy is of concern to South Africans.

The authors of the theoretical frameworks used in this research say that it is possible for organisations to change their information privacy strategy type – for example, Parks & Wigand (2014, p. 218) mention that "privacy strategy is not a static state". However, this research found that in practice it seems that a firm can not only shift its strategy but can have one that is nuanced, a blend of two approaches.

Though the sample for this project is relatively small, it is clear that South African organisations in the financial services industries 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 organisation’s strategic approach to privacy and managing personal information.

Another important finding is that PoPI is open to interpretation and therefore not being applied with consistency across companies. Some companies are taking a “wait and see” approach for some parts of the Act until the Regulator is formed and regulations are proposed or the first major cases of non-compliance are dealt with by the Regulator.

Given the qualitative nature of the research and the small sample size, the findings may not be able to be statistically generalised; had the project run for longer, a mixed methods approach could have been used to quantitatively validate the qualitative finds. However, this does not mean that they are without merit, as they offer some insight into the complexity of forming and executing an information privacy strategy, and provide evidence that interpreting and complying with legislation such as PoPI is not a simple task. They also provide fertile ground for possible future research, some suggestions for which are offered in the next section.

5.3. Recommendations

Concrete regulations or guidelines for implementing the PoPI Act would greatly assist companies in their working towards becoming compliant with the Act. Arguably, this should be first on the Information Regulator’s agenda when it is established.

There is a still great deal to be researched on the subjects of privacy, personal information and the PoPI Act. The following are some suggestions for possible future research projects.

- An extended research project following the same lines of this one. Key improvements to make include simplifying some questions and including more interview subjects (both discussed above).
- A similar project but in another industry, perhaps the retail industry.
- A quantitative survey of privacy strategies across one or multiple industries.
- Further exploration of the impacts of PoPI on companies, perhaps once the Act has commenced or even once the compliance grace period has passed.
- An exploration of the reactions of small- and medium-sized enterprises to PoPI.
- A new conceptual framework called the *company information privacy orientation* (Greenaway, Chan, & Crossler, 2015) was proposed after this project had been designed; it should be included in any future research of a similar nature, but also lends itself to being investigated on its own.
- A research project that mixes elements of the above.

CHAPTER 6.
REFERENCES

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21–29). New York, NY: ACM.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *ICIS 2006 Proceedings* (pp. 1563–1580). Milwaukee, WI: Association for Information Systems (AIS).

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Acquisti, A., & Grossklags, J. (2006). What can behavioral economics teach us about privacy. Presented at the Emerging Trends in Information and Communication Security (ETRICS 2006), Freiburg, Germany.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *The Journal of Economic Perspectives*, *22*(2), 171–192.

Baker, W., Jacobs, J., Spitler, M., Thompson, K., Widup, S., Porter, C., … Kennedy, D. (2014). *Verizon 2014 Data Breach Investigations Report*. Technical report. Retrieved from http://www.verizonenterprise.com/DBIR/2014/

Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a source of competitive advantage. *Strategic Management Journal*, *15*(S1), 175–190.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, *13*(4), 544–559.

Bearman, J. (2015, May 1). The Untold Story of Silk Road, Part 2: The Fall. *WIRED*, *23*(05), 90–118.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, *11*(3), 369–386.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211–241.

Bhattacherjee, A. (2012). *Social science research: principles, methods, and practices* (2nd Edition). Florida, USA: Global Text Project. Retrieved from http://scholarcommons.usf.edu/oa_textbooks/3/

Blume, P. (2015). It is time for tomorrow: EU data protection reform and the Internet. *Journal of Internet Law*, *18*(8), 3–13.

Botha, E., & Makina, D. (2011). Financial regulation and supervision: Theory and practice in South Africa. *International Business & Economics Research Journal (IBER)*, *10*(11), 27–36.

Brandom, R. (2014, November 24). Hackers shut down Sony Pictures' computers and are blackmailing the studio. Retrieved March 5, 2015, from http://www.theverge.com/2014/11/24/7277451/sony-pictures-paralyzed-by-massive-security-compromise

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brustein, J. (2015, March 24). RadioShack's bankruptcy could give your customer data to the highest bidder. Retrieved April 24, 2015, from http://www.bloomberg.com/news/articles/2015-03-24/radioshack-s-bankruptcy-could-give-your-customer-data-to-the-highest-bidder

Burmeister, B. (2014). Pay attention to the Protection of Personal Information Bill. *Finweek*, 7–7.

Burrell, G., & Morgan, G. (1979). *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*. London: Heinemann.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Chan, Y. E., & Greenaway, K. E. (2005). Theoretical explanations for firms' information privacy behaviors. *Journal of the Association for Information Systems*, *6*(6), 7.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401–417.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673–687.

Degryse, H., & Bouckaert, J. (2006). *Opt in versus opt out: A free-entry analysis of privacy policies* (Working Paper No. 1831). Munich, Germany: CESifo Group.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160. http://doi.org/10.2307/2095101

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*(2), 34–51.

Flick, U. (2014). *An introduction to qualitative research* (Fifth edition). London, UK: SAGE Publications Ltd.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology*, *7*(4), 185–200.

Gibbs, G. R. (2014). Using software in qualitative analysis. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 277–294). London, UK: SAGE Publications Ltd.

Gibbs, S. (2015, August 19). Ashley Madison condemns attack as experts say hacked database is real. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports

Gilgun, J. F. (2005a). Deductive qualitative analysis and family theory building. *Sourcebook of Family Theory and Research*, 83–84.

Gilgun, J. F. (2005b). Qualitative research and family psychology. *Journal of Family Psychology*, *19*(1), 40–50.

Gilgun, J. F. (2010). A primer on deductive qualitative analysis theory testing & theory development. *Current Issues in Qualitative Research*, *1*(3).

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146.

Greenaway, K. E., & Chan, Y. E. (2013). Designing a Customer Information Privacy Program Aligned with Organizational Priorities. *MIS Quarterly Executive*, *12*(3).

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: a conceptual framework. *Information Systems Journal*.

Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: origins, significance and global trajectories. *Journal of Law, Information & Science*, *23*(1).

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. Retrieved March 26, 2015, from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of Qualitative Research*, *2*(163-194).

Hermanns, H. (2004). Interviewing as an activity. In U. Flick, E. von Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 209–213). London, UK: SAGE Publications Ltd.

Hui, K.-L., & Png, I. P. (2006). The economics of privacy. In T. Hendershott (Ed.), *Handbooks in Information Systems, Vol. 1: Economics and Information Systems* (Vol. 1, pp. 471–493). Amsterdam, The Netherlands: Elsevier B.V.

Jones, G. (2014, December 17). Revised financial regulation bill clarifies “twin peaks.” Retrieved April 6, 2015, from http://www.bdlive.co.za/business/financial/2014/12/17/revised-financial-regulation-bill-clarifies-twin-peaks

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, *28*(3), 308–319. http://doi.org/10.1016/j.clsr.2012.03.003

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management*, *17*(2), 13–22.

Krebs, B. (2015, July 15). Online Cheating Site AshleyMadison Hacked. Retrieved from http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

Kyobe, M. (2009). Factors influencing SME compliance with government regulation on use of IT: The case of South Africa. *Journal of Global Information Management (JGIM)*, *17*(2), 30–59.

Luong, K. (2006). The other side of identity theft: Not just a financial concern. In *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development* (pp. 152–155). Kennesaw, GA: ACM.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5–12.

Maswanganyi, N. (2015, February 11). Debt weighing on consumer finances, index shows. Retrieved March 29, 2015, from http://www.bdlive.co.za/economy/2015/02/11/debt-weighing-on-consumer-finances-index-shows

McCormick, R. (2014, December 4). Sony Pictures hackers stole 47,000 social security numbers, including Sly Stallone’s. Retrieved March 26, 2015, from http://www.theverge.com/2014/12/4/7337407/sony-pictures-hackers-stole-47000-social-security-numbers-including-stallone/in/7116622

Miller, A. R., & Tucker, C. (2010). Encryption and data loss. In *Ninth Workshop on the Economics of Information Security (WEIS 2010)*. Cambridge, MA.

Moore, T., & Anderson, R. (2011). *Economics and Internet security: A survey of recent analytical, empirical and behavioral research* (Technical Report No. TR-03-11). Cambridge, MA: Harvard University Computer Science Group. Retrieved from ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, *27*(3), 27–32.

Moor, J. H. (1999). Using genetic information while protecting the privacy of the soul. *Ethics and Information Technology*, *1*(4), 257–263.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

Nakashima, E. (2015, July 9). Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

Nkosi, E., Bounds, M., & Goldman, G. (2013). Skills required for the management of Black-owned small enterprises in Soweto: original research. *Acta Commercii*, *13*(1), 1–10.

Nofer, D.-K. M., Hinz, O., Muntermann, J., & Rossnagel, H. (2014). The economic impact of privacy violations and security breaches. *Business & Information Systems Engineering*, *6*(6), 339–348.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1–28.

Parks, R. F., & Wigand, R. T. (2014). Organizational Privacy Strategy: Four Quadrants of Strategic Responses to Information Privacy and Security Threats. *Journal of Information Privacy and Security*, *10*(4), 203–224.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41.

Promotion of Access to Information Act (Act No. 2 of 2000). (2000). *Government Gazette*, *416*(20852). Retrieved from http://www.justice.gov.za/legislation/acts/2000-002.pdf

Prorokowski, L., & Prorokowski, H. (2014). Organisation of compliance across financial institutions. *Journal of Investment Compliance (Emerald Group)*, *15*(1), 65–76.

Protection of Personal Information Act (Act No. 4 of 2013). (2013). *Government Gazette*, *581*(37067). Retrieved from http://www.justice.gov.za/legislation/acts/2013-004.pdf

Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, *24*, 1061.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256–286.

Roulston, K. (2014). Analysing interviews. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 297–312). London, UK: SAGE Publications Ltd.

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (Third edition). Thousand Oaks, CA: SAGE Publications, Inc.

Satariano, A., & Strohm, C. (2014, September 2). Apple says iCloud not breached for hacked actors' photos. Retrieved March 26, 2015, from http://www.bloomberg.com/news/articles/2014-09-02/apple-says-icloud-not-breached-for-hacked-actors-photos

Saunders, M., Philip, L., & Thornhill, A. (2009). *Research Methods for Business Students* (5th Edition). Harlow, England: Pearson.

Seddon, J., & Currie, W. (2014). Institutional Effects of Comparative Government Regulation for the Protection and Privacy of Health Data in the Cloud. In *Proceedings of the 8th Mediterranean Conference on Information Systems*. Verona, Italy: Association for Information Systems (AIS).

Smillie, S., & Child, K. (2015, August 21). Look who's on Ashley. *Times LIVE*. Retrieved from http://www.timeslive.co.za/thetimes/2015/08/21/Look-whos-on-Ashley

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York, NY: NYU Press.

South African Law Reform Commission. (2005). *Privacy and data protection* (No. Discussion paper 109, project 124). Pretoria, South Africa: South African Law Reform Commission. Retrieved from http://www.justice.gov.za/salrc/dpapers/dp109.pdf

Tavani, H. T. (2007a). *Ethics and technology: Ethical issues in an age of information and communication technology* (Second Edition). Hoboken, NJ: John Wiley & Sons.

Tavani, H. T. (2007b). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22.

Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 131–164). Hoboken, NJ: John Wiley & Sons.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society*, *31*(1), 6–11.

Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Berlin, Germany: Springer Science+Business Media.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254–268.

Varian, H. R. (1996). Economic aspects of personal privacy. In *Privacy and Self-regulation in the Information Age*. Washington, DC: National Telecommunications & Information Administration.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), pp. 193–220.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), 3.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Yin, R. K. (2014). *Case study research: Design and methods* (Fifth edition). Thousand Oaks, CA: SAGE Publications, Inc.

CHAPTER 7.

APPENDICES

A. Interview Guide

OPENING

- Thank you very much for being prepared to let me interview you.
- As I mentioned in my introductory letter, I'm researching informational privacy strategies in corporates in the financial services industry. I think it's a good time to do so given that PoPI has been enacted and should commence very soon – companies are thinking about privacy and have PoPI projects on the go.
- I've got a number of questions I'd like to ask, but this is really intended to be more of a conversation than a question and answer session. If you have any thoughts as we go along, please feel free to share them.

QUESTIONS

Informational Privacy Strategy Frameworks

1. What is your company's goal in its approach to information privacy?
   - *(Probe) Theory suggests that it's either survival or competitive advantage.*
2. What role does your informational privacy strategy play in achieving this goal?
   - *(Probe) Theory suggests legitimacy (pragmatic, social) or differentiation (intellectual / knowledge, social / relationship).*
3. What is the focus of your company's information privacy activities – internal or external processes and stakeholders?

- *(Probe) Internal: security, information collection, process improvement. External: regulations, customers.*

4. Does your company have any of its own self-defined privacy practices on top of the industry's standards and codes? Could you give some examples of these?
5. Is privacy seen as a risk or an opportunity by your company?
6. Does your company try to anticipate and work ahead of possible threats or opportunities created by legislation, or do you prefer to handle legislation when it becomes more definite?
7. Does your company ever oppose legislation (for instance, by providing feedback against it when it is announced in the Government Gazette)?

Customer

8. Do you think PoPI will make a difference to your customer base – do you think privacy is of concern to South Africans?
9. Do you think South Africans are willing to provide personal information in return for benefits? What information are they willing to provide?

Protection of Personal Information Act

10. How has your informational privacy strategy changed in light of PoPI?
11. Which parts of the Act are proving to be the most challenging to comply with and why?
12. What benefits can the changes brought about by PoPI have for your company?

CLOSING

- Thanks very much once again for your time.
- If I need any other details or have a few follow-up questions, do you mind if I e-mail you?
- Is there anyone else you can suggest I talk to?

B. Introductory Letter with Consent Form

University of Cape Town • iYunivesithi yaseKapa • Universiteit van Kaapstad

Department of Information Systems

Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3, Rondebosch, 7701

Tel: +27 (0) 21 650 2261
Fax: +27 (0) 21 650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

28 May 2015

Dear Sir/Madam

Request to participate in research study

I am a part-time student completing my Honours degree in Information Systems at the University of Cape Town. The course requires me to conduct a research study and submit a report of my findings. The aim of my research is to determine what informational privacy strategies are used by corporates in the South African financial services industry.

Your participation in this research would be greatly appreciated. Participation involves a 45–60 minute interview, with possible follow-up questions via e-mail if clarification or further detail is required. The interview would be conducted at a time and place that is most convenient to you.

This research has been approved by the Commerce Faculty Ethics in Research Committee. Participation is voluntary and you can choose to withdraw from it at any time. All information you provide will be kept strictly confidential and will only be used for this study. None of the information you provide will be attributed to you or your company by name in the final report or any other publication. A copy of the report will be provided to you once it has been completed.

If you are willing to participate, please complete and sign the attached consent form. If you would like to know more about my professional background, you can view my LinkedIn profile (`https://www.linkedin.com/in/marcpelteret`). If you would like to know more about the project or have any questions, please feel free to contact me using any of the details below. Alternatively, you can contact my supervisor, Dr Jacques Ophoff.

Thank you in anticipation of your time and participation.

Yours sincerely

Marc Pelteret

Honours Student
Department of Information Systems
University of Cape Town

Tel.: 072 611 9053
E-mail: marc@pelteret.co.za

Dr Jacques Ophoff

Research Supervisor
Department of Information Systems
University of Cape Town

Tel.: 021 650 4387
E-mail: jacques.ophoff@uct.ac.za

Department of Information Systems

Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3, Rondebosch, 7701

Tel: +27 (0) 21 650 2261
Fax: +27 (0) 21 650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

Consent to Participate in Research Study titled "Informational Privacy Strategies of Corporates in the South African Financial Services Industry"

In signing below, I hereby grant consent for the researcher, Marc Pelteret, to interview me as a participant of the research study described in the accompanying cover letter.

I acknowledge that:

- My participation is voluntary and can be withdrawn at any time.
- All information I provide will be kept confidential and used only for this study.
- Any information I provide may be used in anonymous form the final technical report of the project.

In addition,

□ I grant permission for the audio of any interview I participate in to be recorded.

□ I do not grant permission for the audio of any interview I participate in to be recorded.

(Please tick whichever option applies.)

I do so understanding that any audio recording made will be kept confidential and will only be used for this research study.

Signature: ____________________

Name: ____________________

Date: ____________________