INFORMATION PRIVACY AND ITS IMPORTANCE TO CONSUMERS AND ORGANISATIONS

Marc Pelteret
marc@pelteret.net

Honours Student
Department of Information Systems
University of Cape Town

30 November 2015

PART 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 (Gibbs, 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. More than a hundred other countries have privacy laws in place or in the process of development (Greenleaf, 2014). 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)). The harsh penalties for failure to comply with the Act demonstrate how important legislators consider the topic of privacy to be.

This essay briefly explores the concept of privacy – a complicated and multifaceted topic – as it relates to personal information, as well as its importance to both consumers and businesses in today's knowledge-centric society.

PART 2.

PRIVACY AND PERSONAL INFORMATION

Privacy is an elusive concept, not only because it is difficult to define, but because it is a dynamic one transforming over time and 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 modern society we desire privacy yet at the same time we willingly share personal information in order to obtain services and make friends. 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."

However, the same technology that makes it easy to share our personal information is also a danger: once our information has been shared it is difficult or even impossible to maintain control over it. 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.

There are a number of theories regarding informational privacy. One that seeks to combine elements of several classic theories into a unified one is the Restricted Access/Limited Control theory of privacy (Tavani, 2007b, 2008). It recognises the importance of an individual being able to restrict access to their personal information while at the same time having control over this information in order to be able to manage it. The concept of control is not built into the definition of privacy, however, and only limited control is required in order 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.

PART 3.

THE IMPORTANCE OF PRIVACY TO CONSUMERS

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?).

Individuals face numerous complexities when considering these questions while making decisions about privacy and whether or not to share of their personal information. Some of these complexities are examined below.

Numerous issues can arise from the improper use or inadequate protection of consumers' privacy and concern about these issues can further affect their decisions; three examples are discussed below. Smith, Milberg, & Burke (1996) catalogue 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 this 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".

3.1. 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 that 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 and 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 information 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 is 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).

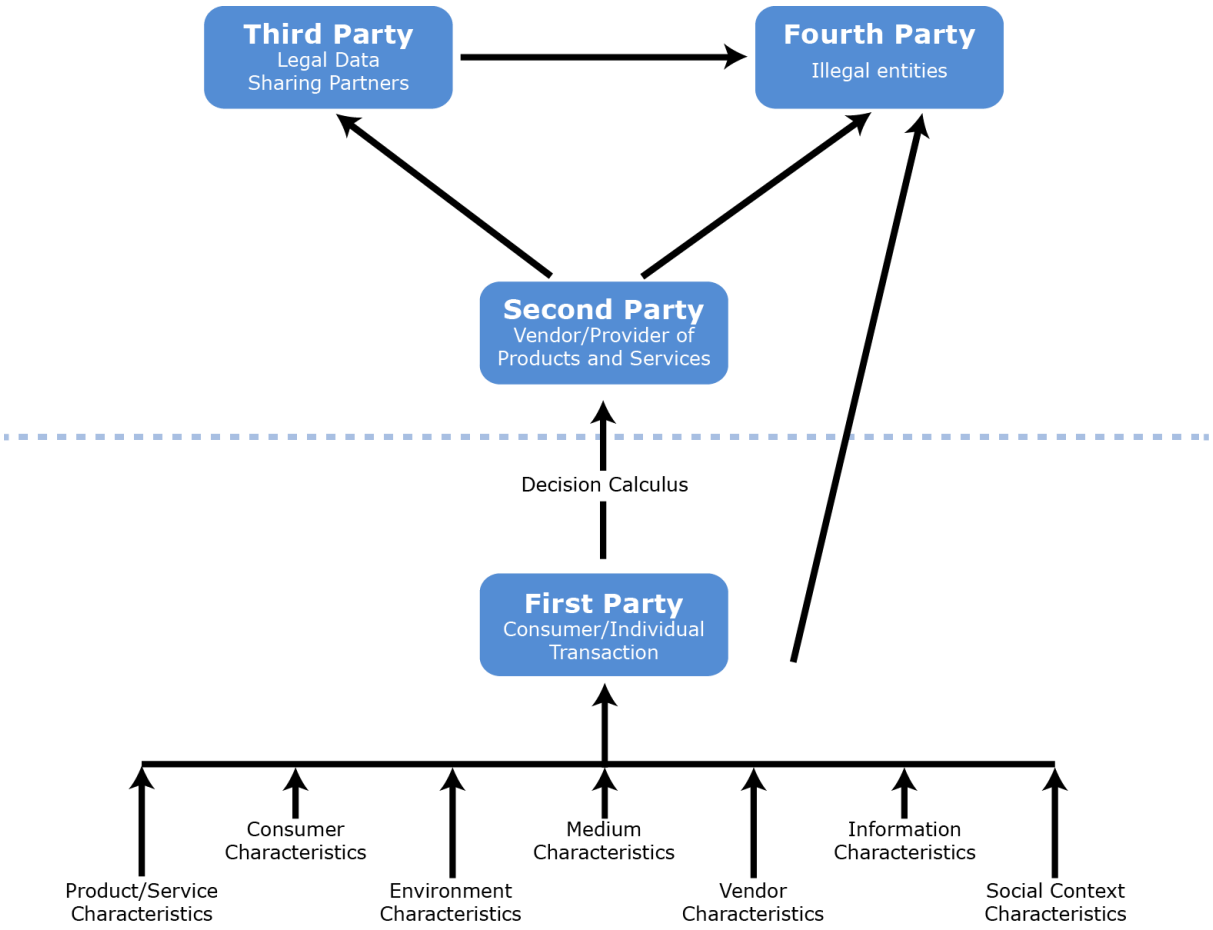

Figure 1: Conger, Pratt & Loch's expanded privacy model (Conger et al., 2013)

3.2. Information Privacy Issues

Numerous issues can arise from the sharing personal information, and these can cause concern to consumers while they decide whether or not to share such information and ultimately impact their decision-making process. Three are explored here.

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 permit 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 the owner's

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; the individual, however, may have to bear costs imposed upon them by the sale of their information, whether they benefit from it or not.

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. Research has 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.

Identity theft is the deliberate use of someone else's identity, usually in order to obtain benefit in their name. According to Anderson, Durbin, & Salinger (2008, p. 171), it 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 problems, 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 cost of storing and transmitting data has 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.

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 of discussion, and in many countries regulations have 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 incidents. 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 United States of America, 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.

PART 4.

THE IMPORTANCE OF PRIVACY TO ORGANISATIONS

Making decisions about privacy is as challenging for organisations as it is for individuals.

Information plays a crucial role in all businesses in today's world. The "information revolution" was brought about by significant improvements in computer technology and rapid reductions in the cost of owning and operating this technology. Information technology has long been seen as a means of gaining competitive advantage (Porter & Millar, 1985). It is also considered as valuable as traditional organisational assets such as people, plant and capital, which means that it needs to be managed appropriately (Lewis, Snyder, & Rainer Jr, 1995).

Mason (1995, p. 55) proposes that an ethical issue arises "whenever one party in pursuit of its goals engages in behaviour that materially affects the ability of another party to pursue its goals". Customer information privacy is an ethical issue because the organisation uses customer information in its pursuit of its goals and in doing so affects its customers (Greenaway, Chan, & Crossler, 2015). This view can be extended to include employee information, which can be as sensitive as customer information. The trouble with ethical issues is that perception influences our decisions about them: one's perception of oneself, the perception of our actions by others, and our perception of "universal laws" all play a role (Hartman, 2001).

Privacy has become a prominent legal issue, with debate about it spurred by constant improvements in technology. With the advent of "big data" (the trend of companies collecting large and complex data sets in order to explore and analyse them for valuable information and patterns)

and cloud computing, the legal issues around information and privacy have become more complex as data is transported across country boundaries.

An organisation's privacy challenge is likely to include information management, ethical and legal issues, rather than centring on a single dimension. How a firm reacts to the challenge depends on many factors, including: its goals; its culture; how it implements its strategies; the degree to which it is affected by its social networks; whether it is proactive or reactive in its response to external pressures; how much information it collects; whether it collects information to spur internal innovation or better understand customers; its perception about how much its customers value privacy; how and to what extent it invests in information technology; and how it puts its privacy activities in place and the outcomes it desires from these activities (Chan & Greenaway, 2005; Greenaway & Chan, 2013; Parks & Wigand, 2014). However, 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) suggest 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), leading 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 may be 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).

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

PART 5.

CONCLUSION

The concept of privacy has transformed and evolved over time and in today's information age the privacy of personal information has become of paramount importance. We all face the simultaneous need to maintain privacy and reveal personal information in order to interact socially and have access to services.

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.

Information privacy is essentially about having control over one's personal information and being able to limit the access others have to it. Amongst other things, this can affect how this data is stored and communicated in telephonic and digital systems.

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 choices.

Privacy decisions are no simpler for organisations. Privacy is a challenge comprising information management, ethical and legal components, and how the firm reacts to the challenge depends on a variety of factors. However, organisations can essentially see privacy as a risk or an

opportunity. A company that views it as a risk aims to avoid 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 create competitive advantage and customers are more likely to share information with companies they trust.

To conclude, informational privacy is an important and complex issue that affects the lives of everyone in our information-orientated society. And as society evolves and technology progresses, inevitably it is going to become more complex and as such require on-going thought, research and intellectual engagement. Ayn Rand wrote: "Civilisation is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilisation is the process of setting man free from men." Through an on-going consideration of the nature and implementation of informational privacy we shall seek to find the right balance between the demands of the individual and the society in which they live.

PART 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.

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

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

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

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

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

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.

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.

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

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

Hartman, L. P. (2001). Technology and ethics: privacy in the workplace. *Business and Society Review*, *106*(1), 1–27.

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.

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/

Lewis, B. R., Snyder, C. A., & Rainer Jr, R. K. (1995). An empirical assessment of the information resource management construct. *Journal of Management Information Systems*, *12*(1), 199–223.

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.

Mason, R. O. (1995). Applying ethics to information technology issues. *Communications of the ACM*, *38*(12), 55–57.

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.

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/

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.

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.

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review*, *63*(4), 149–152.

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.

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

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.

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.

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.

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