A paper presented to the
Department of Information Systems
University of Cape Town
in partial fulfilment of the requirements
for Enterprise Systems and BPM
(INF4012W)

Due: 15 August 2011

# Informational privacy

By Marc Pelteret (PLTMAR004)

# 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 paper 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 his or her 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: *15/08/2011*

Full name of student: *Marc Pelteret*

## Abstract

Whereas privacy once simply meant “the right to be let alone”, today it has a variety of meanings. One of them is informational privacy: having control over one’s personal information and being able to limit the access others have to it. Informational privacy is an important and complex issue that affects the lives of everyone in our information-orientated society. In this paper we look at how informational privacy fits into the general concept of privacy, at a variety of theories concerning privacy, the complexities in making decisions about privacy, and issues to do with informational privacy. In particular we look at profiling and price discrimination, the secondary use of collected personal information, identity theft, and breaches of systems containing personal data and the theft thereof.

# Contents

# 1. Introduction

Privacy as we understand it today is not how it was understood yesterday, nor will it be the same as we will understand it tomorrow. It is an ever-evolving concept. In 1890, Warren & Brandeis defined it as “the right to be let alone”. At that time, newspapers were the threat: they were publishing photographs of and statements by individuals without their consent. Today, information technology is seen as the danger. As Acquisti (2004) 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.”*

In today’s world, 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 led us into the habit of sharing large amounts of information with great number of people, and yet many of us do not feel threatened when doing so (Trepte & Reinecke, 2011).

The problem is that this same technology makes it easier than ever to collect vast amount of data. Tavani (2008) says that the effect information technology has had on personal privacy can be viewed as the following 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.

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

And then there is another great concern for people these days, and that is the safety of the information they choose to share. In recent months, there have been numerous attacks on large databases containing personal information. In April 2011, Sony’s PlayStation Network database was breached and the account information of its 70 million users was accessed (Schreier, 2011). Sony was targeted again in June 2011: this time the private details of one million people who had entered competitions on SonyPictures.com were taken and published on the Internet (Bloxham, 2011).

The purpose of this paper is to discuss what exactly informational privacy is (or currently appears to be thought to be) and how people understand and manage it and the issues around it. To

this end, it begins by looking at the concept of privacy. Thereafter, several theories of privacy are explored in section 3. From an understanding of these theories one will learn that there are many different ways of looking at privacy and informational privacy in particular, and so making decisions about the nature and observance of privacy are complicated; section 4 will explore these complexities. Section 5 interrogates a sample of information privacy issues: profiling and price discrimination, the secondary use of information by third parties, identity theft, and the breaches of systems storing or communicating data. The paper concludes with section 6, which is a synopsis of the contents.

# 2. The concept of privacy

Privacy is an elusive concept 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, 2006, as cited in Tavani, 2008). And because it is a multi-disciplinary issue, it includes a variety of definitions, including everyday ones. 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 separate from these concepts, others argue that it is integral with them. 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).

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. Informational privacy concerns can affect personal data stored in and communicated between databases, as well as personal information communicated between parties using telephonic and digital means (such as e-mail).

It is this last view of privacy that is the subject of this paper. Having looked at the concept of privacy, it will be useful to look at some propounded theories in order to provide a foundation for our understanding of the concept of informational privacy.

# 3. Privacy theories

Privacy has been and continues to be analysed from a variety of perspectives – law, medicine, psychology, sociology, political science, and economics (Hui & Png, 2006). This section looks at several theories, starting with three sociological ones. Following this, we study the economic "free

market" theory. Finally, informational theories are discussed, with the focus being the Restricted Access/Limited Control theory.

## 3.1. Westin, Altman and Petronio's theories

Westin (1967, as cited in Margulis, 2011, p. 10) defines privacy as "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). Westin also states that privacy operates at the individual, group and organisational levels.

Altman's analysis of privacy concentrates on individual and group privacy and behaviour. According to him, privacy is "the selective control of access to the self" (1975, as cited in Margulis, 2011, p. 11) and it has five properties. Firstly, privacy involves a dynamic process of inter-personal boundary control. Secondly, there are desired and actual levels of privacy. Thirdly, it is a non-monotonic function. Fourthly, it is bi-directional – it involves input from and outputs to others. Fifthly, it operates at the individual and group levels. Altman believes there are multiple behavioural mechanisms for regulating privacy that operate as a coherent system, meaning that one mechanism can substitute for, amplify or modulate another (for instance, a nod can replace the word "yes" or slamming a door after shouting "no" reinforces the word). Three features of privacy are important in Altman's theory. Firstly, privacy is a social process. Secondly, in order to understand the psychological aspects of it one needs to look at, amongst other things, the interaction between people, their social world, the physical environment, and the time-based nature of social events. Thirdly, privacy has a cultural context.

Petronio developed a theory known as *communication privacy management*, which is based on Altman's work and is very valuable in understanding computer-mediated communication. It focuses on privacy boundaries, which can have various degrees of permeability (openness), depending on what sort of access we want to give to personal information. There is tension between boundaries because there is a simultaneous need to be open and social and as well as to be private

and preserve our autonomy. We continually adapt these boundaries according internal states and external conditions. Furthermore, we make these adjustments using six principles (Petronio & Reierson, 2009): (1) people believe they own private information; (2) because they believe they own private information, they believe they have the right to control it; (3) people develop and use privacy rules, based on personally important criteria (such as cultural values, gender orientation and contextual impact), to control the flow of private information; (4) once they share that information, those they share it with become a co-owners; (5) once the information is co-owned, the parties should ideally negotiate and agree upon privacy rules for sharing the information with third parties; and (6) because people do not consistently, effectively or actively negotiate collective privacy rules, there is the possibility of *boundary turbulence* – disruptions in the way co-owners manage the flow of information to third parties. When information is shared, co-owners are expected to manage it in a way that is consistent with the owner's original rule. The co-ordination between the owner and co-owners involves determining who else the information can be shared with (*linkage rules*), how much can be shared with them (*permeability rules*), and how much control co-owners have over the information (*ownership rules*). These rules are dynamic and may be implicit (often governed by *norms*) or explicit (thereby clarifying or modifying an existing rule, or introducing a new one).

## 3.2. The economic "free market" theory

According to Hui & Png (2006), economics is a particularly appropriate discipline to use when analysing the concept of privacy as it allows one to appreciate the key trade-offs in policy toward privacy. The "Chicago School" of thought contends that privacy should be treated as any other good: a "free market" approach should be applied to it and this market will be efficient. In this approach, more information is better, provided it is obtained without cost, and thus privacy is generally considered inefficient (Hermalin & Katz, 2006). Proponents of the approach are opposed to government regulation as it stops information flows that will lead to economic efficiency. Posner (1978) put forward the view: "recent legislative emphasis on favouring individual and denigrating corporate and organisational privacy stands revealed as still another example of perverse government regulation of social and economic life".

However, there are several reasons why this approach may not work efficiently (Hermalin & Katz, 2006; Hui & Png, 2006). First, perfect information may destroy markets based on risk and asymmetric information (such as health insurance). Second, the view fails to account for the fact that there may be other market imperfections that interact with privacy; this interaction may lower welfare. Third, the argument only works when sellers have perfect information about consumers, for less than perfect information can affect efficiency. Fourth, it overlooks the fact that resources must be used in order to collect personal information and the collection may have negative consequences

for consumer welfare. Fifth, the use of this information may pose an indirect externality, such as in the case of price discrimination (discussed in section 5.1) where some consumers will end up paying a relatively higher price than others for a particular good or service. Sixth, it ignores various direct externalities associated with the collection and use of information, such as direct marketing (for example, spam) that intrudes on people. Finally, a seller may collect information in one market in order to use it in another, which may create an excessive incentive for it to collect information at the expense of its own potential consumers (in other words, it can lead to a decrease in social efficiency).

## 3.3. 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 provides a satisfactory explanation of informational privacy (and he discusses the flaws of each), 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. 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.

These are only a few of many theories on privacy. For instance, Tavani (2008) discusses a further three "benchmark theories" – theories that are outlines, rather than being full-fledged theories. In the next section, we will look at the challenges that face an individual when making a decision about privacy.

# 4. 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 psychological distortions 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, 2008). 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. A benefit-cost analysis 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 have 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, 2008) 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 read in Acquisti & Grossklags (2008).

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).

In the next section, we will look at some current issues to do with information privacy.

# 5. Information privacy issues

There are numerous issues to do with informational privacy. Four will be studied in this section: profiling and price discrimination, the secondary use of personal information, identity theft, and data breaches.

## 5.1. Profiling and price discrimination

Many of today's websites track their visitors' behaviour and interaction with the sites using cookies, server-side logging and clickstream data, which record what a user clicks on while using the site

(Montgomery, Li, Srinivasan, & Liechty, 2004). Using this information, websites can profile visitors. This profiling can be used to better serve consumers by identifying their needs and save expense for sellers – for example, targeted advertising, where consumers are shown adverts about goods they would actually interested in (Odlyzko, 2003).

But this information can also be used to institute price discrimination and exclude individuals with unattractive characteristics (Hui & Png, 2006). Purchasing behaviour is of particular interest and organisations compile vast databases on customer purchase histories in order to make offers to specific customers and target them with relevant marketing (Acquisti & Varian, 2005). Given the power of computer systems and the speed of networks today, customers can be offered prices, coupons and recommendations personalised for them and in real-time. “Dynamic pricing” is attractive to use under certain circumstances (Acquisti & Varian, 2005), but it can backfire and anger customers, as it did when Amazon.com implemented and tested it in 2000 (Streitfeld, 2000).

The search behaviour of consumers is of interest to companies because it also assists them in price discrimination (Armstrong & J. Zhou, 2010). In particular, it allows sellers to offer discounted prices to first time visitors, as opposed to returning ones, in order to incentivise them and discourage them from searching further for rival offers. To this end, an offer to a first-time visitor may be an “exploding offer”: the new visitor must act on it immediately or not at all.

Increasingly, organisations also sell customer information to third parties – for example, a TiVo personal video recorder tracks the viewing habits of individuals and the manufacturer sells this information to Nielsen Media Research (Spangler, Hartzel, & Gal-Or, 2006).

Odlyzko (2003) believes that price discrimination will become increasingly important because many goods have a fixed one-time cost and low marginal costs. If transactions are done anonymously, it is harder to tell what the buyer is prepared to pay, so there is an incentive to collect data on buyers and build profiles on them. Often companies do not initially aim to price discriminate; many organisations make small incremental changes in order to optimise their functioning and increase their profits, and these eventually lead to price discrimination. “First degree” price discrimination, where the buyer is charged the maximum price they are willing to pay, has long been seen as unattainable; however, the erosion of privacy and today’s IT systems may well enable a close approximation to be possible.

Part of the argument advanced in support of price discrimination is that it is seen to be economically optimal and raises the overall welfare of society – it promotes economic activity with increased competition and a decrease in profits (Odlyzko, 2003). This means that government is unlikely to interfere with the privacy-eroding measures that facilitate it.

## 5.2. Secondary use of information

As mentioned in section 4, 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, 1997). An example of this is the sale of a mailing list, an event that often leads to spam.

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, 1997). 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.

Assigning property rights will cause a problem in the Chicago School "free market" theory (Hui & Png, 2006). According to the theory, a free market for personal information yields social efficiency and an explicit allocation of property rights may shift disturb the socially efficient equilibrium and reduce welfare.

Another problem with property rights is 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. Bouckaert & Degryse (2005) 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.

## 5.3. Identity theft

According to K. B. 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 (discussed in section 5.4) 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 (K. B. 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. But this raises the issues mentioned in section 4: can individuals process all the information surrounding these issues and adequately determine and weigh 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 make identity theft more appealing (K. B. 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. It is federally 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) and looked in section 5.4. Non-legislative means include identity theft registries and the use of biometrics.

## 5.4. Data breaches

Data breaches, such as the ones experienced by Sony, are occurring with increasing frequency. This 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 & R. 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.

Several studies have been conducted to determine the effect of breaches on the performance of a firm, particularly 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, & L. 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.

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. Much of what was discussed in section 4 comes 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.

These are only a few of the issues that revolve around privacy. Others include the topic of anonymity and its misuse, the relationship between privacy and trust, and privacy in social networking. The next section concludes this paper.

# 6. 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 form relationships.

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

There are numerous theories regarding the nature and manifestation of privacy. We looked at three sociological ones: those of Westin, Altman and Petronio. Westin's theory looks at states and purposes of privacy and asserts that it operates at the individual, group and organisational levels. Altman's analysis concentrates on individual and group privacy and behaviour, and to him privacy is the individual's ability to control access to them. Petronio's communication privacy management is particularly valuable in understanding computer-mediated communication. At its core are privacy boundaries, which can have varying degrees of permeability and are continually adapted according to internal states and external conditions.

We also looked at the economic "free market" theory of privacy, which is useful when considering trade-offs between various elements but requires assumptions that over-simplify the issues.

Finally, we looked at some theories that target informational privacy in particular. We concentrated on the Restricted Access/Limited Control theory, which stresses that privacy and control are separate concepts.

Making decisions about privacy, its implementation and its impact is not a straight-forward process: it involves a variety of issues to do with incomplete information, bounded rationality and

psychological distortions. These affect the thinking of even the most sophisticated and rational of individuals and can lead to inconsistencies and contradictions in decision-making.

There are numerous complexities surrounding informational privacy and we looked at a selection of them. The profiling of customers today is ubiquitous, and while it can be used to better serve them, it can also be used in price discrimination and other abuses. While this price discrimination is seen as being unfair by many people, from an economic theorist's standpoint it is often seen to be optimal for society. The secondary use of information by third parties is also of concern to people, particularly when that information is used to make unsolicited approaches to individuals in order to market goods or services to them. Possible solutions to this issue include assigning personal information property rights to individuals and the use of opt-in and opt-out systems.

While information technology makes it easier to perform transactions, it has also created new opportunities for fraud. Identity theft can take many forms and has become a big problem over the years. Data breaches have also become more frequent and can lead to identity theft. Though there measures that can help to prevent and deal with breaches, it is often not clear exactly how effective these are.

To conclude, informational privacy is an important and complex issue that affects the lives of everyone in our information-orientated society. And as society and technology progress, 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.

# 7. References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21–29).

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

Acquisti, A., & Grossklags, J. (2008). What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies, and Practices*, 363–377.

Acquisti, A., & Varian, H. R. (2005). Conditioning prices on purchase history. *Marketing Science*, 367–381.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Fifth Workshop on the Economics of Information Security*.

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

Armstrong, M., & Zhou, J. (2010). Conditioning prices on search behaviour.

Bloxham, A. (2011, June 3). Sony hack: private details of million people posted online. *The Telegraph*. Retrieved August 9, 2011, from http://www.telegraph.co.uk/technology/news/8553979/Sony-hack-private-details-of-million-people-posted-online.html

Bouckaert, J., & Degryse, H. (2005). Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies. Presented at the The Fifth Workshop on the Economics of Information Security (WEIS 2006), England.

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.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, *7*(4), 185-200.

Hermalin, B. E., & Katz, M. L. (2006). Privacy, property rights and efficiency: The economics of privacy as secrecy. *Quantitative Marketing and Economics*, *4*(3), 209–239.

Hui, K. L., & Png, I. P. L. (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.

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.

Luong, K. (2006). The other side of identity theft: not just a financial concern. *Proceedings of the 3rd annual conference on Information security curriculum development*, InfoSecCD '06 (pp. 152–155). New York, NY, USA: ACM. doi:http://doi.acm.org/10.1145/1231047.1231081

Margulis, S. T. (2011). Three Theories of Privacy: An Overview. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web* (pp. 9-17). Heidelberg, Germany: Springer-Verlag Berlin.

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

Miller, A. R., & Tucker, C. E. (2010). Encryption and data loss. *Ninth Workshop on the Economics of Information Security (weis 2010), Cambridge: Hardvard University, http://weis2010. econinfosec. org/papers/session1/weis2010_tucker. pdf*.

Montgomery, A. L., Li, S., Srinivasan, K., & Liechty, J. C. (2004). Modeling online browsing and path analysis using clickstream data. *Marketing Science*, 579–595.

Moore, T., & Anderson, R. (2011). Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research. Retrieved from ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf

Odlyzko, A. (2003). Privacy, economics, and price discrimination on the Internet. *Proceedings of the 5th international conference on Electronic commerce* (pp. 355–366).

Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory. In T. Afifi & W. Afifi (Eds.), *Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications* (pp. 365-383). New York, NY: Routledge.

Posner, R. A. (1978). An Economic Theory of Privacy. *Regulation*, *2*(3), 19-26.

Romanosky, S., & Acquisti, A. (2009). Privacy Costs and Personal Data Protection: Economic and Legal Perspectives. *Berkeley Tech. LJ*, *24*, 1061–1647.

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.

Schreier, J. (2011, April 26). PlayStation Network Hack Leaves Credit Card Info at Risk. *Wired.com*. Retrieved August 9, 2011, from http://www.wired.com/gamelife/2011/04/playstation-network-hacked/

Spangler, W. E., Hartzel, K. S., & Gal-Or, M. (2006). Exploring the privacy implications of addressable advertising and viewer profiling. *Communications of the ACM*, *49*(5), 119–123.

Streitfeld, D. (2000, September 27). On the Web, Price Tags Blur: What You Pay Could Depend on Who You Are. Retrieved August 14, 2011, from http://www.washingtonpost.com/ac2/wp-dyn/A15159-2000Sep25

Tavani, H. T. (2007a). *Ethics and technology: ethical issues in an age of information and communication technology* (Second Edition.). Hoboken, New Jersey: 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, N.J.: Wiley-Interscience.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *SIGCAS Comput. Soc.*, *31*(1), 6–11. doi:http://doi.acm.org/10.1145/572277.572278

Trepte, S., & Reinecke, L. (2011). *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*. Springer-Verlag New York Inc.

Varian, H. R. (1997). Economic aspects of personal privacy. *Privacy and Self-regulation in the Information Age*.

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