Informing Science: the International Journal of an Emerging Transdiscipline **Volume 19, 2016**

Cite as: Pelteret, M. & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science: the International Journal of an Emerging Transdiscipline, 19,* 277-301. Retrieved from http://www.informingscience.org/Publications/3573

A Review of Information Privacy and Its Importance to Consumers and Organizations

Marc Pelteret and Jacques Ophoff
University of Cape Town, Cape Town, South Africa

marc@pelteret.net jacques.ophoff@uct.ac.za

Abstract

The privacy of personal information is an important area of focus in today's electronic world, where information can so easily be captured, stored, and shared. In recent years it has regularly featured as a topic in news media and has become the target of legislation around the world. Multidisciplinary privacy research has been conducted for decades, yet privacy remains a complex subject that still provides fertile ground for further investigation. This article provides a narrative overview of the nature of information privacy, describing the complexities and challenges that consumers and organizations face when making decisions about it, in order to demonstrate its importance to both groups. Based on this work, we present a transdisciplinary view of information privacy research linking the consumer and organization. It illustrates areas of concern for consumers and organizations together with the factors that influence the decisions they make about information privacy. By providing such a view we hope to encourage further cross-disciplinary research into this highly pertinent area.

Keywords: privacy, information privacy, personal information, privacy management, consumers, clients, transdisciplinary, organizations, literature review

Introduction

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, and 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) states that "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

Editor: Raafat Saadé
Submitted: March 24, 2016; Revised: September 27, 2016; Accepted: September 28, 2016

well as the general public. Reports focused 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).
- In February 2016, the Federal Bureau of Investigation (FBI) obtained a court order to compel Apple to break into an iPhone belonging to the perpetrator of a mass shooting (Edwards, 2016). Apple said that the only way this can be done is by creating a special version of Apple's iOS operating system that bypasses the phone's security, and opted to fight the order in court rather than comply. Ultimately, the FBI withdrew its request after finding a third party to assist in unlocking the phone, but the issue re-sparked debate about many aspects of privacy and state surveillance (Johnson, Swartz, & della Cava, 2016).
- In September 2016, Yahoo revealed that in 2014 hackers penetrated its network and stole personal data related to more than 500 million accounts (McMillan, 2016). This is believed to be the largest breach ever publicly disclosed by a company.

These are only a few examples that are spurring global discussion of privacy and the need for adequate legislation to govern it. More than a hundred countries have privacy laws in place or in the process of development (Greenleaf, 2014).

This article provides a narrative overview of the concept of privacy – a complicated and multifaceted topic – as it relates to personal information, as well as its importance to consumers and organizations in today's knowledge-centric society. Such an overview is currently lacking in this research domain. The aim of this paper is to combine research areas related to consumer and organizational privacy into a transdisciplinary view, in order to enhance the understanding of the issues and stakeholders.

The article proceeds by describing the research methodology that was followed. It goes on to examine various consumer perspectives of privacy, looking at influencing factors in privacy decision-making, concerns that arise from the sharing of personal information, and how privacy can be measured via privacy concerns. Next, it examines the importance of privacy to organizations.

Following this is a discussion of the main research contribution, a rich picture transdisciplinary view of privacy research, after which the article is concluded.

Research Methodology

This paper presents a narrative overview of information privacy research, integrating the importance of privacy from the consumer and organizational perspectives. A narrative overview is a comprehensive synthesis of previously published research in the topic area (Green, Johnson, & Adams, 2006). The narrative overview serves to discuss theory and context, with this article promoting a transdisciplinary view of information privacy research.

The literature for this review was primarily obtained by following the advice of Webster and Watson (2002). Initial articles were found through keyword searches of leading journals, such as the AIS Senior Scholars' basket of journals. Searches were conducted using database platforms which included EBSCOHost, Emerald, and ScienceDirect. Further articles were identified by backward and forward reference searching. The Web of Science service and Google Scholar were also used to identify more recent literature that has referenced significant articles. All articles were screened for relevance, in order to identify the important articles in the topic area. A significant number of sources were obtained from the reviews by Bélanger and Crossler (2011) and Smith, Dinev, and Xu (2011).

The sources consulted and referenced came not only from the field of information systems, but also from the fields of law, business, marketing, economics, management, computer security, psychology, and ethics. This broad focus was adopted in order to achieve a wider transdisciplinary view of the topic area.

Privacy and Personal Information

Privacy and personal information are intertwined issues in today's world. There are many theories about the privacy of information, but before exploring these theories we define the concept of privacy.

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 modern society we desire privacy yet at the same time we willingly share personal information in order to obtain services (such as health care and insurance) 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 ex-

changed; (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, while 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". He went on to elaborate 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" (Westin, 1967, p. 7). 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 is this view that is most relevant in the context of this article and we continue by examining theories relevant to our discussion.

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 his or her information. The theories are not incompatible, but emphasize 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, people have 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 elements into a single theory is Restricted Access/Limited Control (RALC) theory.

The RALC theory stresses that privacy and control are separate concepts. According to Tavani and 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 he or she is protected from intrusion, interference and information access by others (Tavani, 2007b). Like the restricted access theory, it emphasizes 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 recognizes 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: the individual needs to be able to choose situations that offer others the desired level of access – for example, to choose to waive the right to restrict others from accessing certain kinds of information about him or her – and the individual needs to be able to access his or her information and correct it if necessary.

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 personal information. Some of these complexities are examined below.

Numerous issues can arise from the improper use or inadequate protection of consumers' privacy and the concern about these issues can further affect their decisions. Smith, Milberg, and Burke (1996) list four areas of consumer privacy concerns that are very similar to PAPA: improper access to personal information, unauthorized 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". Ensuring privacy is a complex decision-making process and may differ from one individual or instance to another.

Challenges in Privacy Decision-making

A variety of issues influence decisions regarding privacy and can lead to inconsistencies and contradictions. Given the multifaceted nature of privacy, Acquisti (2004) maintains that its value may be discussed only once its context has been specified. Context is defined as "stimuli and phenomena that surround and thus exist in the environment external to the individual, most often at a different level of analysis" (Mowday & Sutton, 1993). Smith et al. (2011, p. 1003) list four of the most frequently cited contexts for privacy and privacy-related beliefs. The first is the type of information collected from individuals (for example, financial, medical, or demographic data). Some information is considered more sensitive than others, and so, for instance, consumers are generally more willing to provide demographic information than financial information (Phelps, Nowak, & Ferrell, 2000). Second is the use of information by a particular industry sector. The third is the political context – whether or not privacy is viewed as a right, the legislation govern-

ing privacy, the enforcement of these laws, and so on. Finally, the fourth context is that of technological applications, which can be used to either infringe upon privacy or enhance it.

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 characterized by incomplete or asymmetric information, where the different parties involved in the transaction do not have the same information 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 et al., 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, he or she may still find it difficult to follow a rational strategy because of psychological distortions that influence his or her thinking. There are numerous examples of these distortions (Acquisti, 2004; Acquisti & Grossklags, 2005, 2006). 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 possibly 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).

Thus, whenever individuals have to make a decision about privacy they rarely have all the information they need to make an informed choice. 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 his or her actual behavior is known as the privacy paradox (Nofer, Hinz, Muntermann, & Rossnagel, 2014; Norberg, Horne, & Horne, 2007). Individuals may be aware of measures that can be taken to protect their privacy, but not make use of them (Dommeyer & Gross, 2003).

Conger, Pratt and Loch (2013) propose a model (Figure 1) that illustrates how complicated it is for individuals to know who will have access to their data after they have shared it. While the individual knows the second party, who information will be provided to, he or she 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 behavior 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).

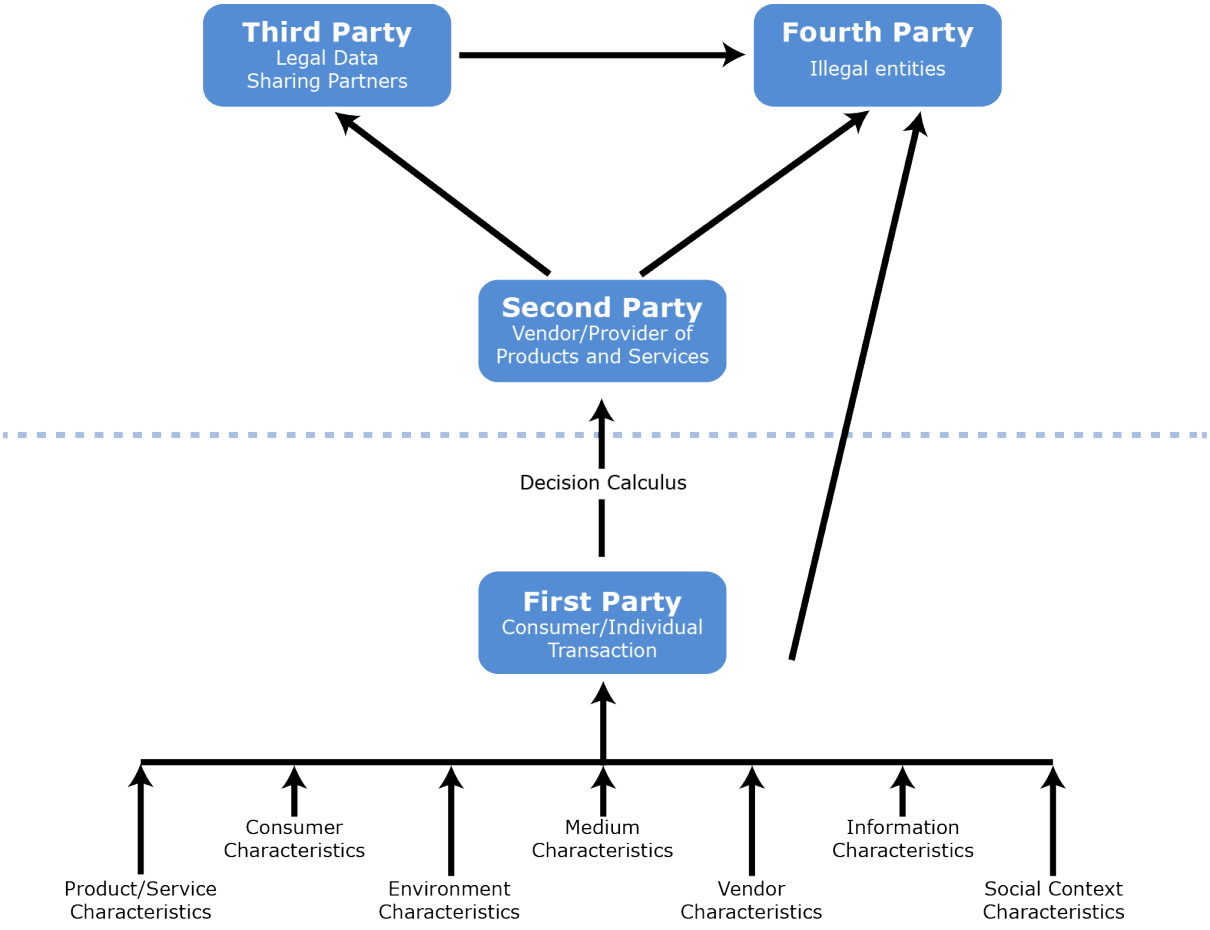

Figure 1: Expanded privacy model (Conger et al., 2013)

Information Privacy Concerns

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

Secondary use of information is when information is collected for one purpose and then later used for another. While this is neither a new phenomenon nor unique to the digital world – census data has been collected and used in a variety of ways for a long time – it is easier and cheaper than ever to carry out because of modern systems. These systems have given rise to 'big data', which is the trend of organizations collecting large and complex data sets in order to explore and analyze them for valuable information and patterns that can be used to gain new insights and improve decision-making. While big data can be used in a variety of positive ways – to improve the performance and safety of products and services, optimize operations, minimize waste, and so on – there are many ways in which it can be misused and infringe on privacy.

As noted by Rubinstein (2013), big data calls into question three long-standing assumptions of many privacy laws. The first is that personal data is distinct from non-personal data. Big data can include data from both and through sophisticated data mining techniques combine them to form new data that may not be labelled as personal data, and thus avoid regulation, yet still be applied to and affect individuals. Part of the concern is that with enough data organizations could generate group profiles and apply them to users to, for instance, determine who should get insurance for particular diseases or get access to credit. Actions may be applied to individuals who do not exhibit a problematic trait simply but do fall into the group. The second assumption is that anonymizing data (by removing identifying information) is an effective method of protecting users against tracking and profiling. It appears that this may not be case: in one study, researchers demonstrated that Facebook Likes can be used to accurately determine a number of personal traits (Kosinski, Stillwell, & Graepel, 2013); in another, researchers were able to predict United States social security numbers using only publicly-available data (Acquisti & Gross, 2009). The third assumption is that data minimization – restricting data collection only to minimum that is necessary – is a viable constraint. The problem is that this works directly against the underlying basis of big data and would cripple the trend, thus removing all its economic and social benefits.

Secondary use of information is by no means limited to an organization's in-house use of big data. Third parties can make secondary use of information if it is shared with them. An example of this is the sale of a mailing list, an event that often leads to spam messages: 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 same cannot necessarily be said of the incentives of the seller and third party (Varian, 1996).

One method of dealing with this matter is to assign property rights in personal information to individuals (Schwartz, 2004; Varian, 1996). Schwartz (2004) posits that five elements are required to create such a model under which individual privacy would be respected and could be maintained: limitations on an individual's right to alienate (sell or otherwise transfer) personal information; default rules that force disclosure of the terms of trade (so that individuals may be better informed of how their information will be used); a right of exit for participants in the market; the establishment of damages to deter market abuses (these should preferably be determined by the state through legislation); and institutions to police the personal information market and punish privacy violation.

Such a market would allow contracts to be written that would allow personal information to be used according to the individual's wishes (Varian, 1996). This would support those endeavoring 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 al-

ready exists, but it is the collector that holds the rights, not the individual (Varian, 1996). Yet an externality exists and the individual may have to bear costs imposed upon them by the sale of their information.

A significant 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 (Boyce, Brown, McClelland, Peterson, & Schulze, 1992; Knetsch & Sinden, 1984).

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 it must offer the consumer the opportunity to deny or allow them permission to do so. Degryse and 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 led 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.

Profiling and price discrimination can be performed using user data that has been collected**.** Many of today's websites track their visitors' behavior 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 be interested in (Odlyzko, 2003).

However, this information can also be used to institute price discrimination and exclude individuals with unattractive characteristics (Hui & Png, 2006). Purchasing behavior is of particular interest and organizations 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 personalized 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 behavior of consumers is of interest to companies because it also assists them in price discrimination (Armstrong & Zhou, 2010). In particular, it allows sellers to offer discounted prices to first time visitors, as opposed to returning ones, in order to incentivize 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, organizations 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 discrimi-

nate – many organizations make small incremental changes in order to optimize 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 he or she is 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.

Acquisti and Varian (2005) developed a model of the interaction between buyers and sellers when the buyers' identities are known in order to determine whether price discrimination based on purchase history is a viable practice. They determined that it is if the majority of the population ignores the impact of the behavior on prices or is unable to hide their identity, or if high-value customers can be offered a better price-service package or repeat users attempting to hide their identities are penalized by being offered an inferior service.

Three studies found that discrimination based on personal information does, indeed, exist on the Internet, in the form of both price discrimination and price steering (also called search discrimination), through which users with a particular profile are directed to suitably priced products (Hannak, Soeller, Lazer, Mislove, & Wilson, 2014; Mikians, Gyarmati, Erramilli, & Laoutaris, 2012, 2013).

Personalized services and offerings can provide better value to customers and improve their loyalty. However, the ability to make such offers requires access to customer information. Research by Awad and Krishnan (2006) shows that consumers who value information transparency are less willing to be profiled, though the authors note that consumers distinguish between online advertising and online service and assign more value to the latter. Personalization systems can be covert, where individuals' locations are surreptitiously determined (for example, by tracking their mobile devices) and used to send appropriate information to them, or overt, where an individual explicitly requests such information and, in doing so, provides his or her location. A study by Xu, Luo, Carroll, and Rosson (2011) used privacy calculus to explore the relationships between personalization and privacy in the context of location-aware marketing, in which the location of the consumer is used to deliver targeted advertising. It was found that personal characteristics and the personalization system used influence an individual's privacy decision-making process. Both studies emphasize that perceived benefit can outweigh concerns for privacy.

Identity theft has a variety of definitions, particularly in law around the world; some of the complexities around arriving at a single definition are discussed in Van der Meulen (2006) and Schreft (2007). For the purposes of this article, it can be defined as the deliberate use of someone else's identity without his or her permission, usually in order to obtain benefit in his or her name. It is one of the fastest growing crimes in North America: in 2008, the United States Bureau of Justice Statistics reported that an estimated 11.7 million people, or 5% of all persons aged 16 or older in the United States, had been victims of identity theft over a two-year period (Langton & Planty, 2010, p. 1); by 2014, this number had risen to approximately 17.6 million people, which was 7% of all persons aged 16 or older (Harrell, 2015, p. 1).

According to Anderson, Durbin and 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 be classified in a variety of ways (Tajpour, Ibrahim, & Zamani, 2013). *Financial identity theft* is when the victim's details are used to open new transactional accounts (*new account fraud*) or to transact using or access funds in existing accounts (*existing account fraud*). With s*ynthetic identity theft,* stolen information is combined with fictional information to create a new, false identity. *Criminal identity theft* occurs when the victim's details are provided to law enforcement during the commission of a crime, and with *business identity theft* the victim is a business. *Identity cloning* is when the victim's details are used by an imposter to create a new life. Finally, using the victim's details to obtain medical services is known as *medical identity theft*.

Personal information can be collected through low-tech methods – such as stealing from mailboxes, tricking someone into giving away their details over the phone, and "dumpster diving" (looking through garbage for documents) – and high-tech ones that involve attacks on databases, phishing e-mails, or misleading cellular phone messages (Tajpour et al., 2013). Often the victim 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 he or she would otherwise have undertaken (or even choosing to avoid online transactions altogether) – a likely occurrence if the consumer is transacting online and fears a financial loss (Hille, Walsh, & Cleveland, 2015).

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; however, this increase in data transmission and flow also 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 United States federal law, it is illegal to commit identity theft; before 1998, it was not considered a crime. There are also consumer data protection laws, which are discussed in Romanosky and Acquisti (2009). Non-legislative means include identity theft registries and the use of biometrics.

Data breaches, such as those experienced by Sony and Ashley Madison, are occurring with increasing frequency. According to Verizon's 2016 Data Breach Investigations Report, in 2015 there were 64,199 security incidents and 2,260 confirmed data breaches (Verizon, 2016a).

Verizon's Data Breach Digest illustrates how data breaches work by providing details on 18 different breach scenarios, all which were drawn from real-world investigations and were chosen because they are highly prevalent or are particularly sophisticated, damaging, or difficult to detect or contain (Verizon, 2016b). Furthermore, while the specifics of data breaches are often kept private, two very large and public breaches have been documented in some detail. In 2007, it was discovered that the network of TJX Companies, a retailer of apparel and home fashions, had been breached and the particulars of at least 45.7 million credit- and debit-cards had been downloaded

(Cereola & Cereola, 2011; Pereira, 2007). In late 2013, another retailer, Target, was the subject of a data breach which aimed to steal the details of every credit card used at its 1,767 US stores during a busy holiday period (Manworren, Letwat, & Daily, 2016).

Both of these attacks were perpetrated by external parties. However, it is important to note that this is not always the case; a variety of internal errors, often human ones, can occur while collecting, processing, and disseminating information, resulting in unintentional breaches (Liginlal, Sim, & Khansa, 2009). Insider threats – employees who are deliberately malicious – are also of concern; these users may act for revenge or profit, and steal personal information or intellectual property, or pass sensitive or classified information on to a third party (Huth, Chadwick, Claycomb, & You, 2013). A study performed by the Ponemon Institute (2015) revealed that attacks from malicious insiders take longer on average to resolve that than any other form of cyber-attack.

Stolen data can be used in a variety of ways, including being sold to spammers and used to perpetrate identity theft or fraud, possibly leading to inconvenience or financial costs. However, the effects can be far further reaching. If sensitive private information is made public, it can cause embarrassment. Time and effort may need to be expended to mitigate problems, monitor for suspicious activity (by checking banking statements, for example), or rectify issues caused by the misuse of the information. It can also cause stress in the relationship between a consumer and an organization – for instance, the perceived severity of a security breach can affect an individual's intent to shop online and the risk they perceive in doing so (Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Rao, 2016). Users tend to reuse passwords across services – even those deemed especially important – and underestimate the sophistication of attackers and their tools (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009) or, if they are aware of risks, often take inadequate precautions to protect their accounts (Bryant & Campbell, 2006). Ultimately, users fail to realize that "their most well-defended account is no more secure than the most poorly defended account for which they use that same password" (Ives, Walsh, & Schneider, 2004, p. 76). So, a data breach for one account can have a knock-on effect and broaden the scope of the user's troubles.

In order to act after a breach, the consumer has to be aware of it. They may become aware of a problem after being prevented from transacting using an account or by noticing fraudulent transactions on their statements, but neither is certain to happen or is the ideal way for them to find out. Thus 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 unauthorized party (Moore & Anderson, 2011). These laws are intended to have two effects: to incentivize 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 and 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, and Acquisti (2011) analyzed 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 and Anderson (2011) note that data leakage by firms is only one cause of fraud, so disclosure laws are only a partial solution.

Complying with breach disclosure law in the United States is complicated and expensive. There is currently no broadly applicable federal legislation covering data breaches – the existing laws apply to cybercrime in general or in specific circumstances to specific information or industries (Peters, 2014). Instead, most individual states have their own legislation covering data breach notification. However, these laws differ from one another significantly in areas such as the definition of personal information, who needs to be notified in the event of a breach, the timeframe for notification, under what circumstances notification can be delayed, and the cause of action a person injured by a breach may take (Peters, 2014).

One area that the state laws do have in common is the "encrypted data safe harbor" which deems notification unnecessary if the data was encrypted and the encryption key was not compromised (Joerling, 2010). Encryption is an often-touted solution to protecting data and is meant to act as a disincentive to those who want to steal data and minimize the risk of stolen data being put to malicious use. However, according to Miller and 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 the safe harbor law.

The patchwork of US federal laws and multitude of varied state laws makes for a difficult landscape. It is argued that a single federal law should be implemented (Joerling, 2010; Peters, 2014). One has been presented in the US Senate: The Data Security and Breach Notification Act of 2013 ("DSBNA"). However, it is not without fault and in fact would weaken the breach laws that exist in some states (Peters, 2014).

In the European Union (EU), Directive 2002/58/EC (known as the "e-Privacy Directive") complements the Data Protection Directive (95/46/EC) and covers breach notification. However, it is specifically limited to the telecommunications sector. It has a two-tiered form of notification: it requires organizations to report every breach (irrespective of whether or not affected individuals are at risk of harm) to a national authority without undue delay, and it requires that the consumer using the organization's service, or another individual, to be notified if the breach is likely to adversely affect the personal data or privacy of the consumer or individual (Burdon, Lane, & Von Nessen, 2012). "Adversely affected" is not strictly defined in the Directive but examples of possible harm are given and go beyond economic loss. Some countries have added additional breach notification legislation because of the limited scope of the e-Privacy Directive, but not all have, meaning that organizations operating across Europe face similar complexities to those faced by those operating in the US (Tankard, 2016, p. 5).

The new General Data Protection Regulation (GDPR), which has been adopted and will replace the Data Protection Directive in 2018, expands the scope of data protection to all entities that collect or process information on EU citizens, no matter where they are based or the data is stored (Tankard, 2016, p. 5). It will make breach notification mandatory unless the breach is unlikely to affect the rights and freedoms of individuals. If it is likely to affect individuals, the data protection authority must be notified within 72 hours, and if it poses a high risk to individuals, they must be notified without undue delay. However, the requirement to notify data subjects can be avoided under certain circumstances, such as action being taken to ensure that the risk is unlikely to materialize (de Hert & Papakonstantinou, 2016).

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 behavioral 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.

In the US, the data breach laws of most states do not provide adequate legal remedies for the consumer in the case of a breach. They primarily focus on disclosure and allow for civil action if an organization fails to disclose a breach and this leads to the consumer being injured (Fisher, 2013). The proposed DSBNA does not provide for a private cause of action and caps civil penalties, which would make class action suits less effective (Peters, 2014). Unless the consumer can prove that he or she has been harmed – as opposed to merely being put at risk – their lawsuit is likely to be quickly dismissed. However, this appears to be slowly changing as judges are considering what it means to suffer injury when one's personal information is stolen and are allowing more data breach suits to proceed (Hong, 2016).

Measuring Privacy via Privacy Concerns

As Smith et al. (2011) mention, it is nearly impossible to directly measure privacy itself, and so empirical privacy research involves the measurement of a privacy-related proxy instead. In information systems research, the measurement of *privacy concerns* – the concerns that individuals have over the information privacy practices of organizations – has emerged as the preferred construct. According to Bélanger and Crossler (2011), the majority of studies use one of two instruments for measuring concerns: concern for information privacy (CFIP) or Internet users' information privacy concerns (IUIPC).

CFIP, developed and validated by Smith et al. (1996), has 15 items that represent four dimensions of concerns: improper access to personal information, unauthorized secondary use of personal information, errors in personal information, and collection of personal information. Stewart and Segars (2002) examined and re-validated these dimensions, finding that consumers are concerned about all of them rather than any single one in particular and that accurate measurement of CFIP requires that the inter-relationships between these dimensions be taken into account.

Malhotra, Kim and Agarwal (2004), based on the belief that the concerns of online users are likely to differ from those of offline consumers, adapted CFIP to an Internet context and presented a theoretical framework that measures Internet users' information privacy concerns (IUIPC). The framework's instrument consists of 10 items that measure three dimensions: collection, control, and awareness of privacy practices. Collection refers to the information being provided under circumstances that are fair and agreed to (the consumer willingly gives up his or her information in return for something of value after having considered the effects of the trade). Control refers to the ability to approve and possibly modify the exchange or withdraw from it altogether. Finally, the consumer needs to be aware of the information collector's privacy practices, particularly how they make use of collected data.

Sipior, Ward and Connolly (2013) re-visited the IUIPC framework and assessed it in order to determine whether it is still applicable. Their findings only partially supported the results presented by Malhotra et al. (2004). They confirmed that the more trust a consumer has in an online company, the less likely the individual is to perceive providing personal information to that company as a risk and more likely the individual is to intend to provide personal information online. They also found that the more risk the consumer faces in providing personal information, the less willing he or she is to provide this information online. However, they did not find a negative correlation between the IUIPC construct and consumer trust in an online company or a positive one between the construct and consumer risk in providing information to an online company. It must be noted though that the authors concede that the study's limitations reduce the generalizability of their results and they advocate further investigation in order to confirm their results.

Bélanger and Crossler (2011) observe that CFIP is the more extensively used of the two instruments and was the preferred choice even after IUIPC was released. They suggest that this may be owing to research projects having been started before IUIPC was published or it may be because CFIP is seen as the best option for measuring information privacy concerns.

The Importance of Privacy to Organizations

Making decisions about privacy is as challenging for organizations 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 competitive advantage (Porter & Millar, 1985) and is considered as valuable as traditional organizational assets such as people, plant, and capital, which means that it needs to be managed appropriately (Lewis, Snyder, & Rainer, 1995).

Mason (1995, p. 55) proposes that an ethical issue arises "whenever one party in pursuit of its goals engages in behavior that materially affects the ability of another party to pursue its goals". Customer information privacy is an ethical issue because the organization 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 perceptions 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 and cloud computing, the legal issues around information and privacy have become more complex as data is transported across country boundaries.

An organization's privacy challenge is likely to include information management, ethical, and legal issues, rather than centering on a single dimension. How a firm reacts to the challenge depends on many factors, including the following: 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.

Organizations 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 and 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 for handling data throughout the corporation (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 recognizing and acting upon its duty to ensure privacy of personal information, a firm can enhance its reputation, both internally (with employees and the board of directors, for example) and externally (with customers, regulators and the media, among others) (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). Organizations 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 be more amenable to marketing if the firm is open about its policies, minimizes its requests for information, and collects only what is relevant (Phelps et al., 2000).

An organization manages privacy through its informational privacy program, which is the "collection of policies and procedures that firms implement with respect to the collection, use, reuse, security, storage, and disposal of their customers' personally identifiable information" (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 organization through leadership, training, and regular audits, and by considering privacy for every new use of personal information (Culnan & Armstrong, 1999; Culnan & Williams, 2009).

Discussion

The previous sections highlight a diverse range of information privacy research topics which have been investigated across multiple disciplines. While each study contributes within its focus area, a transdisciplinary view of information privacy research linking the consumer and organization is lacking. Such a view can inform links between previously separate research topics and open new avenues for cross-disciplinary investigation.

In order to provide a transdisciplinary view, we present a rich picture of the problem domain in Figure 2. A rich picture is a tool from the soft systems methodology domain, originally defined as "the expression of a problem situation compiled by an investigator, often by examining elements of structure, elements of process, and the situation climate" (Checkland, 1999). It establishes the issues that concern the parties involved and focuses on the interactions that take place (Fillery, Rusli, & James, 1996). It provides a holistic view of the problem domain instead of focusing on specific problem situations.

The presented rich picture separates consumer and organizational information privacy concerns and influencing factors. From a consumer perspective, concerns reflect the issues that can arise from the sharing of personal information. It is easy to capture and collect large amounts of personal information, and errors can occur while it is being or after it has been captured. Once collected, who has access to the information and what is done with it becomes of concern, with issues such as profiling and price discrimination being possibilities.

While making decisions about privacy and performing privacy calculus, consumers are influenced by a variety of factors. They may not have all the information pertinent to their decision. An individual's psychology, particularly psychological distortions and trouble with bounded rationality that he or she may be prone to, will play a role. The consumer's lack of control over and lack of knowledge about how his or her information will be used and managed may affect the decision. Lastly, the context in which the information is being collected or used – the type of information being collected, the industry sector, and so on – will be factored into the decision. These factors underscore the challenges in privacy decision-making

Identity theft, data breaches, and changes in legislation are also issues that consumers face, but we propose that they affect the consumer via the organization. These are issues that are also often of significant concern to the organization and can have reputational and economic consequences if not planned for.

Organizations have their own set of concerns about information privacy. Profitability is of major importance to most companies, and so the containing of costs and avoidance of fines, as they relate to information management and privacy, are important concerns. How a firm manages information can impact its perceived trustworthiness and is reputation – not just with consumers, but with employees, shareholders, partners, and other parties. Trustworthiness can be impacted if the organization does not adequately address consumer concerns, thus affecting the organization's ability to establish and maintain a relationship with the consumer. As previously discussed, trust characteristics include the organization's ability, integrity, and benevolence. Trouble can lead to a loss of customers and even directly impact the firm's share price.

There are several factors that can influence an organization's decisions about information privacy. The internal nature of the firm itself (its structure, dynamics, and ethics) will impact its decisions about privacy. How it manages information may impact or being impacted by these decisions. Through its privacy decisions, management, and policies, it can establish an overarching view of privacy that will guide future decisions about privacy and information management. The management of these factors often has a direct bearing on consumer privacy concerns. Consequently, these factors also play a role in the trust relationship between the consumer and organization.

There are several areas of information privacy that have yet to be researched thoroughly or at all, and which can have an impact on individuals and organizations. Smith et al. (2011, p. 992) suggest that there are four levels of analysis that can be used to classify information privacy research: individual, group, organizational, and societal. Using these levels, Bélanger and Crossler (2011) performed a review of information privacy research and found that there have been numerous studies at the individual level and several on some topics at the organizational level, there are exceeding few that have been performed at the group and society levels. There are also very few that treated information privacy as a multi-level concept.

Despite the many studies that have been conducted at the individual level, there are still aspects that have not been explored in depth. The effect of privacy experiences, privacy awareness, personality differences, demographic differences, and culture on an individual's privacy concerns are all facets that have not been well explored, as mentioned by Smith et al. (2011).

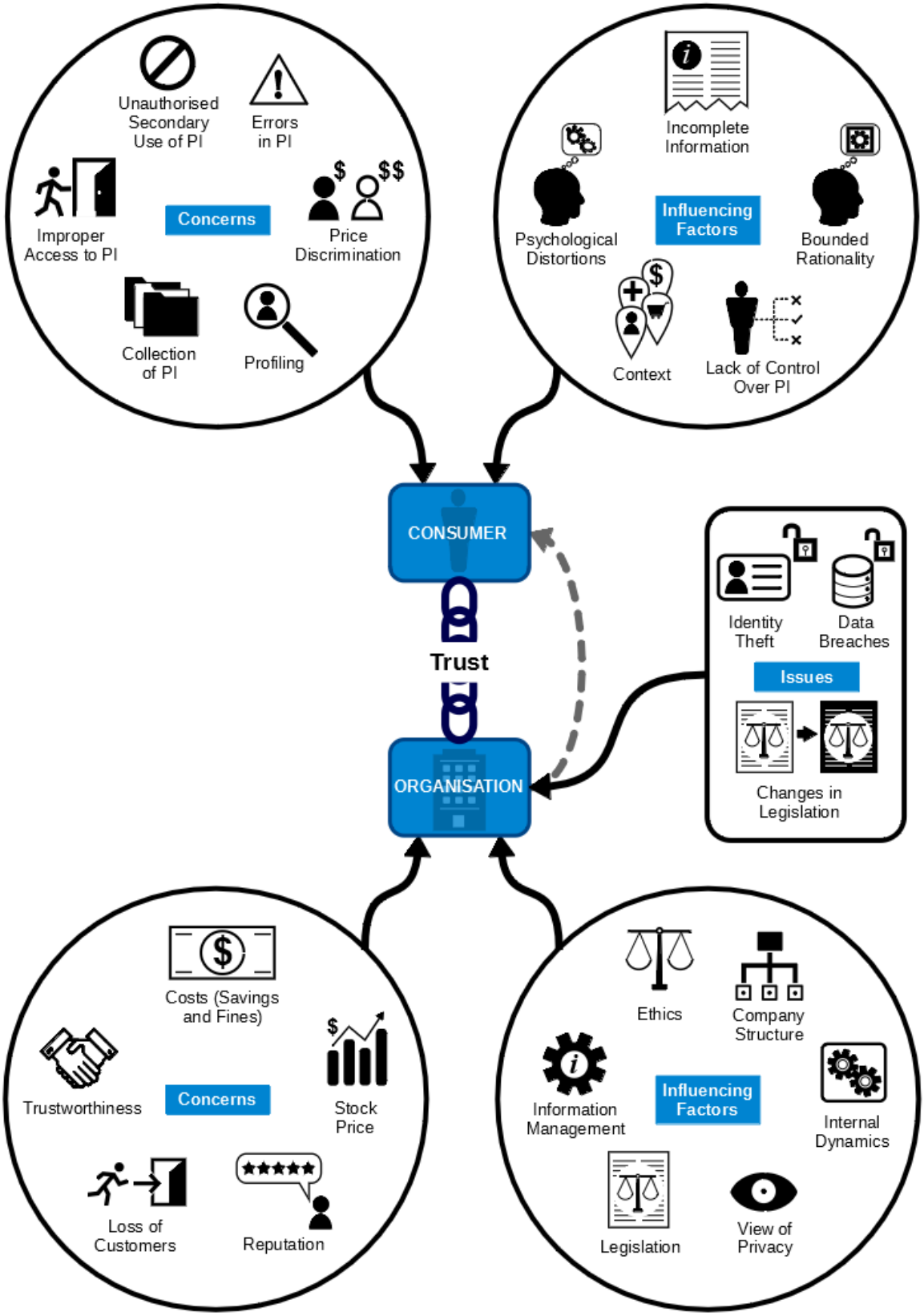

Figure 2. A transdisciplinary view of privacy research

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 obtain 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.

Privacy is important for consumers and organizations alike, but decisions about it are not simple for either. The transdisciplinary view developed in this article shows various domains that influence the problem area: technology, psychology, economics, management, and law all play a role in our view of privacy. Our view contributes a holistic understanding of the problem domain and the complex interactions that take place. Although areas are often studied in isolation it is clear that there is a close link between concerns and influencing factors for consumers and organizations alike.

To conclude, informational privacy is an important and complex issue that affects the lives of everyone in our information-oriented society. As society and technology progress, inevitably it is going to become more complex and as such require on-going thought, research and intellectual engagement. Rand (1996, p. 683) wrote: "Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization 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.

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., & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences*, *106*(27), 10975–10980.

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.

Acquisti, A., & Varian, H. R. (2005). Conditioning prices on purchase history. *Marketing Science*, *24*(3), 367–381.

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* (ELSE Working Paper No. 351). London, UK: ESRC Centre for Economic Learning and Social Evolution. Retrieved from http://eprints.ucl.ac.uk/19447/

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28.

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

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1042.

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.

Boyce, R. R., Brown, T. C., McClelland, G. H., Peterson, G. L., & Schulze, W. D. (1992). An experimental examination of intrinsic values as a source of the WTA-WTP disparity. *The American Economic Review*, *82*(5), 1366–1373.

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

Bryant, K., & Campbell, J. (2006). User behaviours associated with password security and management. *Australasian Journal of Information Systems*, *14*(1), 81–100.

Burdon, M., Lane, B., & Von Nessen, P. (2012). Data breach notification law in the EU and Australia–Where to now? *Computer Law & Security Review*, *28*(3), 296–307.

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.

Cereola, S. J., & Cereola, R. J. (2011). Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. *Issues in Accounting Education*, *26*(3), 521–545.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, *83*, 47–56.

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

Checkland, P. (1999). *Systems thinking, systems practice*. Chichester, England: John Wiley & Sons.

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.

de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179–194.

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.

Edwards, H. S. (2016, February 17). Your iPhone's Encryption Could Depend on a 227-Year-Old Law. *Time*. Retrieved from http://time.com/4227236/apple-fbi-san-bernardino-encryption/

Fillery, P. F., Rusli, A., & James, H. L. (1996). Describing the problem situation in IS studies using SSM: A practitioner's view. In *Proceedings of the 1996 Information Systems Conference of New Zealand (ISCNZ '96)* (pp. 2–9). IEEE Computer Society.

Fisher, J. A. (2013). Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach. *William & Mary Business Law Review*, *4*(1), 215–239.

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

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44–55). Pittsburgh, Pennsylvania, USA: ACM.

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

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: secrets of the trade. *Journal of Chiropractic Medicine*, *5*(3), 101–117.

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

Hannak, A., Soeller, G., Lazer, D., Mislove, A., & Wilson, C. (2014). Measuring price discrimination and steering on e-commerce web sites. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 305–318). Vancouver, BC, Canada: ACM.

Harrell, E. (2015). Victims of identity theft, 2014. *US Department of Justice Bureau of Justice Statistics Bulletin, September*.

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

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, *30*, 1–19.

Hong, N. (2016, June 27). For consumers, injury is hard to prove in data-breach cases. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988

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* (pp. 471–493). Amsterdam, The Netherlands: Elsevier B.V.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers*, *15*(1), 1.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75–78.

Joerling, J. (2010). Data breach notification laws: An argument for a comprehensive federal law to protect consumer data. *Washington University Journal of Law & Policy*, *32*, 467–488.

Johnson, K., Swartz, J., & della Cava, M. (2016, March 29). FBI hacks into terrorist's iPhone without Apple. *USA Today*. Retrieved from http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/

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

Knetsch, J. L., & Sinden, J. A. (1984). Willingness to pay and compensation demanded: Experimental evidence of an unexpected disparity in measures of value. *The Quarterly Journal of Economics*, *99*(3), 507–521.

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.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805.

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

Langton, L., & Planty, M. (2010). Victims of identity theft, 2008. *US Department of Justice Bureau of Justice Statistics National Crime Victimization Survey Supplement*.

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.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, *28*(3), 215–228.

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.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257–266.

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

McMillan, R. (2016, September 23). Yahoo says information on at least 500 million user accounts was stolen. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/yahoo-says-information-on-at-least-500-million-user-accounts-is-stolen-1474569637

Mikians, J., Gyarmati, L., Erramilli, V., & Laoutaris, N. (2012). Detecting price and search discrimination on the internet. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks* (pp. 79–84). Redmond, Washington: ACM.

Mikians, J., Gyarmati, L., Erramilli, V., & Laoutaris, N. (2013). Crowd-assisted search for price discrimination in e-commerce: first results. In *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies* (pp. 1–6). Santa Barbara, California, USA: ACM.

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

Montgomery, A. L., Li, S., Srinivasan, K., & Liechty, J. C. (2004). Modeling online browsing and path analysis using clickstream data. *Marketing Science*, *23*(4), 579–595.

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.

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

Mowday, R. T., & Sutton, R. I. (1993). Organizational behavior: Linking individuals and groups to organizational contexts. *Annual Review of Psychology*, *44*(1), 195–229.

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.

Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. In *Proceedings of the Seventh Australasian Conference on Information Security - Volume 98* (pp. 71–78). Wellington, New Zealand: Australian Computer Society, Inc.

Odlyzko, A. (2003). Privacy, economics, and price discrimination on the Internet. In *Proceedings of the 5th International Conference on Electronic Commerce* (pp. 355–366). Pittsburgh, PA: ACM.

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.

Pereira, J. (2007, May 4). How credit-card data went out wireless door. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB117824446226991797

Peters, R. M. (2014). So you've been notified, now what: The problem with current data-breach notification laws. *Arizona Law Review*, *56*, 1171–1202.

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.

Ponemon Institute. (2015). *2015 cost of cyber crime study: Global* (Research Report). Traverse City, MI: Ponemon Institute.

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

Rand, A. (1996). *The Fountainhead* (Centennial Edition). New York, New York: Signet.

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.

Rubinstein, I. S. (2013). Big data: The end of privacy or a new beginning? *International Data Privacy Law*. Retrieved from http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.abstract

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

Schreft, S. L. (2007). Risks of identity theft: Can the market protect the payment system? *Economic Review-Federal Reserve Bank of Kansas City*, *92*(4), 5.

Schwartz, P. M. (2004). Property, privacy, and personal data. *Harvard Law Review*, *117*(7), 2056–2128. http://doi.org/10.2307/4093335

Sipior, J. C., Ward, B. T., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, *26*(6), 661–678.

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.

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.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49.

Streitfeld, D. (2000, September 27). *On the Web, price tags blur: What you pay could depend on who you are*. Retrieved April 25, 2015, from http://www.wright.edu/~tdung/amazon.htm

Tajpour, A., Ibrahim, S., & Zamani, M. (2013). Identity theft methods and fraud types. *International Journal of Information Processing and Management*, *4*(7).

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5–8.

Tavani, H. T. (2007a). *Ethics and technology: Ethical issues in an age of information and communication technology* (2nd ed.). 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.

Van der Meulen, N. (2006). *The challenge of countering identity theft: Recent developments in the United States, the United Kingdom, and the European Union*. Tilburg, The Netherlands: International Victimology Institute Tilburg (INTERVICT).

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

Verizon. (2016a). *2016 data breach investigations report* (Research Report). New York, NY: Verizon.

Verizon. (2016b). *Data breach digest* (Research Report). New York, NY: Verizon.

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

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52.

Biographies

Marc Pelteret is an IT professional. He is a graduate of the University of Cape Town (UCT) and holds a Bachelor of Business Science (Hons) degree specializing in Computer Science and a Bachelor of Commerce (Hons) degree specializing in Information Systems, as well as a national certificate in business analysis.

Jacques Ophoff is a Senior Lecturer in the Department of Information Systems at the University of Cape Town (UCT), South Africa. He obtained his doctorate in Information Technology from the Nelson Mandela Metropolitan University, South Africa. His research interests include behavioral information security, privacy, digital forensics, mobile technologies, and education. He is a regular reviewer for international journals and conferences. He is an active member of the Association of Information Systems and the IFIP WG8.11/WG11.13 Information Systems Security Research group.