

2008

Empirical Research on Technology-Related Privacy Concerns: A Review and Critical Assessment

Cilona McParland

Dublin City University, cliona.mcparland2@mail.dcu.ie

Regina Connolloy

Dublin City University, regina.connolly@mail.dcu.ie

Follow this and additional works at: <http://aisel.aisnet.org/ecis2008>

Recommended Citation

McParland, Cilona and Connolloy, Regina, "Empirical Research on Technology-Related Privacy Concerns: A Review and Critical Assessment" (2008). *ECIS 2008 Proceedings*. 191.

<http://aisel.aisnet.org/ecis2008/191>

This material is brought to you by the European Conference on Information Systems (ECIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

EMPIRICAL RESEARCH ON TECHNOLOGY-RELATED PRIVACY CONCERNS: A REVIEW AND CRITICAL ASSESSMENT

McParland, Cliona, Dublin City University, Glasnevin, Dublin 9, Ireland
cliona.mcparland2@mail.dcu.ie

Connolly, Regina, Dublin City University, Glasnevin, Dublin 9, Ireland
regina.connolly@mail.dcu.ie

Abstract:

The exponential adoption of the Internet for transaction and interaction purposes continues unabated. However, despite the obvious empowering benefits of the Internet, consumers concerns regarding the ability of online vendors to collect and use information regarding them and their online interactions have also increased. Vendors facing intense competition in the marketplace are under increasing pressure to gain a more sophisticated understanding of their consumers and thus view the collection of consumers' personal and interaction information as essential to achieving that understanding. Awareness of this fact has accentuated consumers' privacy concerns and in some cases impacted interaction intentions and behaviour. Similarly, in the computer-mediated work environment, employees' awareness that communication-monitoring technologies are being used to monitor their email and Internet interactions has increased. Despite the importance of this issue, research on technology-related privacy concerns remains in an embryonic stage. Moreover, the literature indicates that much confusion surrounds the construct and in many studies the construct is neither clearly defined nor operationalised. The aim of this paper is therefore to reduce that confusion by providing a brief review of the literature while outlining potential research avenues worthy of future research. This paper provides researchers with a refined and holistic understanding of the construct and consequently makes a valuable contribution not only to information systems research but also to practitioners in their efforts to better understand the factors that predict and inhibit technology-related privacy concerns.

Keywords: Privacy, Consumer information, Consumer behavior, Frameworks, Empirical research.

1. INTRODUCTION

Privacy has always been a contentious issue as individuals strive to protect their personal information from mis-use by others. However, the advent of the Internet and the increasing proliferation of technologies in both the marketplace and workplace have been matched by a heightened awareness amongst individuals that threats to their privacy exist and must therefore be addressed. Despite the empowering benefits of the Web, consumers are increasingly aware that the technology can also be used by online vendors to collect potentially sensitive information regarding them and that this information can be used without their express permission. For example, online transactions require customers' to disclose considerably more personal and financial information than they would provide in offline transactions (Miyazaki and Fernandez, 2001). Marketers can use the trail of information that results from such Internet transactions - including information on the customer's searches, comparisons, product and brand preferences, purchase and post-purchase information - to compose very precise customer profiles in their efforts to continuously learn about changing consumer needs. With this information, vendors then have the ability to provide individuals with specifically customised information thus offering them a personalised shopping experience. From a vendor perspective the consequence is increased customer satisfaction that they hope will translate into increased retention and ultimately increased profitability within the marketplace. However, from a consumer perspective, the price of this personalised shopping experience may outweigh any customisation benefits, particularly when vendors have been known to sell information on consumers to third parties without the permission of the consumers concerned.

In the social science literature the importance of individuals' privacy concerns is widely acknowledged (e.g Konvitz, 1966; Powers, 1996; Froomkin, 2000; Rule, 2004; Cassidy and Chae, 2006) and it is recognised as a dynamic issue that has the potential to impact attitudes, perceptions, and even the environment and future technology developments (Crompton, 2001). Within the information systems field, while there is an growing awareness of the importance of technology-related privacy concerns, empirical research on the construct remains at an embryonic stage and the limited number of studies on the construct that exist tend to be limited in size and nature (Gefen and Straub, 2000; Cockcroft and Heales, 2005). Compounding the problem is the fact that some of these studies are beset by conflicting conceptualisations of the construct, as well as a lack of agreement regarding the factors that predict the perceptions, attitudes and behaviours of the consumers themselves. Consequently, it is difficult for privacy researchers within the information systems discipline to compare and contrast the results of previous studies in their efforts to progress understanding of the construct. Moreover, as far as it is possible to ascertain, there have been no studies on technology-related privacy concerns within an organisational context to date.

The aim of this study therefore is to provide both a concise and consolidated review of the technology-related privacy literature. The literature outlining perceptions, attitudes and behaviours of consumers' in relation to their technology-related privacy concerns will be reviewed and a number of gaps in relation to technology-related privacy concerns will be outlined.

2. THE PRIVACY CONSTRUCT

Privacy is a complex construct that has received the attention of researchers from a broad spectrum of disciplines including ethics (Platt, 1995), economics (Rust *et al.*, 2002), marketing (Graeff and Harmon, 2002), management (Robey, 1979) as well as from the legal discipline even as far back as 1860 (Warren and Brandeis). However, despite this interest, the construct remains beset by conceptual and operational confusion. For example, Tavani (1999) remarks that privacy is neither clearly understood nor clearly defined while Introna (1996) comments that for every definition of privacy, it is also possible to find a counterexample in the literature. As a result, many researchers choose to define privacy specific to the focus of their specific study or the lens of their discipline in an attempt to evade this problem (Smith, 2001) and as a consequence the conceptual confusion that surrounds the

construct remains undiminished. Unsurprisingly, these differing conceptualisations have manifested in similarly differing views regarding how the construct should be examined and measured. For example, privacy researchers within the legal discipline argue that privacy should be measured in terms of the rights of the individual whilst ethics researchers contend that the morality of privacy protection mechanisms for the individual should be the focus of research attention. Interestingly, and perhaps most sensibly, some economics researchers (Parker 1974, Acquisti, 2002, Rust *et al.*, 2002) argue that in order to gain a full understanding of the privacy construct it is necessary to examine it from a multiplicity of viewpoints. Consequently, Parker (1974) maintains that privacy can be examined as a psychological state, a form of power, an inherent right or an aspect of freedom. More recently, Acquisti (2004) has emphasised the multi-dimensional nature of the construct and posited that privacy should no longer be viewed as a single unambiguous concept, but become a class of multifaceted interests.

One aspect of privacy on which many researchers concur is the central to its understanding is the issue of control, specifically the individual's need to have control over their personal information. Practitioner reports also confirm the importance that consumers attribute to being able to control their personal information (e.g Harris, 2004) Control is defined as "*the power of directing command, the power of restraining*" (Oxford, 1996: 291) and is consistently proposed in the literature as a key factor in relation to understanding consumer privacy concerns. For example, Westin (1967) argues that privacy is the claim of individuals, groups, or institutions to decipher for themselves when, how and to what extent their personal information is conveyed to others. This issue of personal control is widely supported by researchers such as Fried (1968: 482) who defines privacy as the "*control we have over information about ourselves*" and Parker (1974: 281) who defines privacy in terms of the "*control over who can sense us*". Personal control is important as it relates to the interest of individuals to control or significantly influence the handling of personal data (Clarke, 1988).

However, a diverse body of researchers dispute the relevance of control in understanding privacy concerns. They argue that to define privacy in terms of control can yield a narrow perspective as not every loss or gain of control over information constitutes a loss or gain of privacy (Parker, 1974). For example, all online consumers who voluntarily provide personal information in the course of their transactions do not necessarily view that as a loss of control and consequently a loss of privacy. Even the knowledge that each of their online interactions is providing the vendor with a potential trail of information regarding who they are, their buying habits and other personal details does not necessarily constitute a lack of control or a loss of privacy in the eyes of such consumers. With that in mind, some researchers (Moor 1990, 1997; Schoeman 1984) suggest that it would be better to focus on the issue of restricted access rather than on consumer's need for control when trying to understand technology-related privacy issues.

While agreement as to the relevance of control in relation to understanding privacy remains a disputed issue, the attention placed on this issue by researchers' points to the fact that privacy comprises ethical or moral dimensions. Ethics is the branch of philosophy that deals with theories of right and wrong behaviour and privacy issues has frequently been discussed in this in relation to ethical impacts. For example, the increasing pervasiveness of technologies into human beings' work and leisure environments has opened up a spectrum of unregulated behaviour and previously accepted distinctions regarding correct and immoral behaviour are no longer always clear (Turban *et al.*, 2006). For example, ethical questions surround the issue of surveillance – and in particular electronic surveillance - which according to Clarke (1988) is the systematic monitoring of the actions or communication of individuals. Within computer-mediated work environments, the critical need to protect the employee's privacy rights is becoming increasingly apparent as modern technologies provide the opportunity for continuous data collection. In some cases individuals may be conscious that they are being monitored, they are just not sure of the extent and detail of that monitoring. Neither are they aware of how that collated information is being employed by the monitoring body. Researchers such as Safire (2002) note how extreme pervasive surveillance tends to result in a 'creepy feeling' among those being monitored despite the fact that they have done nothing wrong to merit such scrutiny. In fact, the

monitoring of employees' computer-related interactions has previously been described as an 'electronic whip' used unfairly by management (Tavani, 2004).

In summary, privacy has been defined in the literature from a multiplicity of viewpoints, which has resulted in definitional and operational confusion regarding the construct. As we enter the third millennium we have turned the corner into a place where technology pervades our day-to-day lives, and many things which would previously have been considered flights of imagination, are as a result of technology, becoming part of our reality (Kostakos *et al.*, 2005, Galanxhi and Fui-Hoon 2004). Consequently, the need for an improved understanding of the nature of technology-related privacy construct has increased rather than diminished.

2.1. Privacy, Trust & Uncertainty in an Online Environment

While consumer privacy has always been a significant issue in the traditional offline market, it has assumed a greater importance with the increased adoption of the Internet (Rust *et al.*, 2002). The nature of the electronic environment has brought issues of trust, risk and uncertainty centre stage. For example the literature recognises the importance of trust in the specific business-to-consumer online transaction domain (Lee and Turban, 2001; Gefen and Straub, 2000; Reichheld and Schefter, 2000). In fact Ratnasingham (1998) contends that the influence of trust on interactions is even more crucial in the pervasive online environment than in the physical and traditional marketplace. Similarly, the Cheskin eCommerce Trust Study (1999: 2) notes that as "*the Internet develops and matures, its success will depend in large part on gaining and maintaining the trust of visitors. This will be paramount to sites that depend on consumer commerce.*" However, despite the fact that trust is a rare commodity which is built up slowly over time (Tracy, 1995) and building and maintaining it is essential for the survival of any relationship, it is a fragile bond that can be destroyed easily. In order for trust to be engendered therefore, consumers must be confident that their personal information will not be used without their consent and will not be sold to third parties. Those companies that are successful at building that trust and managing the uncertainty associated with consumer disclosure of personal information will benefit from increased consumer confidence.

The individual's need to trust relates directly to the risk involved in a given situation (Mayer *et al.*, 1995). In the business-to-consumer electronic commerce environment the degree of risk is even greater than in the traditional commercial environment (Grabner-Krauter and Kaluscha, 2003) therefore the need for trust is correspondingly greater. For example, purchasing on the Internet holds risks that are unique to that context. These include the requirement to provide sensitive information, and the uncertainty of what the retailer will do with the consumer's personal information (Grabner-Krauter and Kaluscha, 2003). In fact, it has been shown that awareness of their lack of control over personal data can lead to consumers withholding information from companies and resisting the adoption of online purchasing (Goldsmith and Bridges, 2000). Due to this lack of control and uncertainty, many consumers simply do not trust most web providers enough to engage in relationship exchanges with them (Hoffman *et al.*, 1999).

Hirschleifer and Riley's (1979) theory of information can also be used to better understand the uncertainty that applies to the online purchase environment. This theory outlines two categories of uncertainty: *system-dependent uncertainty* and *transaction-specific uncertainty*. Both types of uncertainty exist in the online purchase environment. For example, the online consumer is dependent on the technological medium for the process to take place effectively and securely but not have any control over the medium or the transmission of the data (*system-dependent uncertainty*). *Transaction-specific uncertainty* includes the possibility that even when guarantees are provided that customer data will not be passed on to third parties, the consumer does not have any guarantee that the vendor has measures in place to protect consumer data from employee theft. Hence, there is a high level of uncertainty related to the online purchase environment. The uncertainty and lack of control related to the online environment reflects the significant asymmetry that exists in terms of what the Internet means to individuals versus vendors. For example, Prakhober (2000) rightly points out that while the

technology has created better, faster and cheaper ways for businesses to meet their customers' needs and better faster and cheaper ways for customers to satisfy their own needs, the capability to leverage this technology is far higher for companies than for individual consumers. Because unequal forces, leading to asymmetric information availability, tilt the playing field significantly in favour of industry, such technologies do not create market benefit to all parties in an equitable manner.

While marketers need information on consumers in order to refine products and services to increase consumer satisfaction, the need to find a way in which the interests of both consumers and marketers can be served has never been more urgent. Often the information that is collated on consumers is done so without their consent thus exacerbating privacy concerns. Moreover it is apparent that not all researchers acknowledge the extent of this problem. For example, Hoyer and MacInnis (1997) maintain that one of the main reasons why privacy concerns regarding online vendors' collection of consumer information exist is due to consumers' lack of understanding regarding how this information is collected and more importantly how it will benefit them. Other researchers, such as Ratnasingham (1998) dispute this notion, arguing that customers concerns and anxieties regarding transaction confidentiality and anonymity are frequent and legitimate and should therefore be acknowledged as such.

In this environment, businesses have a choice as to how they should respond thus determining the type of buyer-seller relationships that their company has. If privacy concerns are not addressed they manifest through the costs of lost sales, through the move from online to offline business channels and through lost customer relationships. The ownership of online consumers will be predicated to a large degree on the way in which businesses seeking to leverage Internet technology gather market information whilst equally embracing the responsibility of preserving consumer privacy.

3. ANALYSIS OF THE EMPIRICAL LITERATURE

In the literature, technology-related privacy concerns have mainly been considered from a transactional perspective, with the concerns of the online consumer paramount to the discussion. However, such concerns are equally salient and critical in the organisational employment context. Therefore, in this paper, in order to provide a thorough review of the literature, the studies of technology-related privacy issues have been grouped into two main categories – consumer concerns and employee concerns. Information regarding how the authors selected their samples and the methodology used is also provided.

While the privacy literature specific to consumers' technology-related privacy concerns is remarkably limited, a number of studies stand out as deserving of comment. Udo's (2001) study of 158 online users examined their attitudes in relation to privacy and security concerns. He found privacy ranked as the highest concern among users' with threats to security and to children coming in a close second and third. Interestingly, the study findings indicate that for every three shoppers in the study who were willing to purchase online, there are seven others who are too concerned to shop in the virtual marketplace. Based on an analysis of the results the author concluded that privacy and security threats are the main barriers to e-commerce success and therefore must be dealt with accordingly.

A more detailed study of the privacy concerns that attempted to classify individuals in terms of their level of privacy concern was conducted by Sheehan (2002). She employed Westin's (1967) tripartite grouping of Internet users (pragmatists, unconcerned, privacy fundamentalists) as a guide and categorised 889 online users in terms of the degree to which are concerned about engaging in online transactions. An online survey consisting of 15 privacy related statements representing 5 different factors that can influence privacy concerns were administered to the study participants who were then measured in terms of their level of response to three different privacy scenarios. The results showed that the majority of the respondents (81%) were pragmatists in relation to their privacy concerns, 16% of the respondents were classified as being unconcerned with the remaining 3% meeting the

classification standard of privacy fundamentalists. While the author recognises the limited generality of Westin's typology, the study findings are interesting in that they point to the fact that online privacy concerns are likely to be contextually driven rather than the result of embedded psychological constructs specific to the individual.

Singh and Hill's (2003) study employed duty-based theories, social contract theory and stakeholder theories to examine the attitudes of 106 German consumers in relation to their online privacy concerns. A pencil and paper survey was administered to depict the attitudes of German consumers' towards privacy in general but more specially to Internet privacy. A 5 point likert scale measured the attitudinal responses of the respondents with only standard demographic data being considered in the results. Interestingly, the issue of control surfaced in this study with the findings identifying a strong desire among German consumers' to have some level of control over how their personal information is collated, disclosed or used. The study further highlighted the importance of online vendor responsibility and the active role the Government should play in protecting citizens' privacy. Although it is unlikely that this desire for control over personal information is limited to German consumers, whether or not this applies across other European countries remains undetermined due to dearth of cross-cultural research on this subject.

While Malthotra *et al.*, (2004) developed a scale and causal model to determine the dimensionality of an Internet users' information privacy concerns (in terms of data collection, control and awareness), they note that development of this scale was highly dependent on contextual factors and does not examine the influence of privacy concerns on actual behaviour. While they suggest that opportunities for future research in this area are abundant, it is clear that the need for a reliable culture-independent measurement instrument to measure information privacy concerns has not yet been met.

Whilst most studies have focused on the attitudes of online consumers in relation to privacy, a recent study conducted by Van Slyke *et al.*, (2006) extends previous models of e-commerce adoption to investigate the degree to which consumers' information privacy concerns influence behavioural outcome ie their willingness to partake in transactions online. Two privacy measurement instruments were applied in this study – one to measure privacy concerns in relation to a high recognition website and the second to privacy concerns in relation to a less well known website. The study's findings show that privacy concerns, perceived risk and familiarity with the website play a significant role in consumers' willingness to transact online. However, contrary to previous studies (such as Malthotra *et al.*, 2004) a positive relationship between information privacy concerns and level of trust was identified in the study. Van Slyke *et al.*, (2006) suggest the trade-off nature of the online relationship, where information is exchanged in return for a transaction to take place, may in part explain this abnormality of this finding. Again, the lack of research on this topic and in particular comparable studies with similar type sample in other countries makes it difficult to determine whether this outcome pertains only to the authors sample or is an indication of a more complex dynamic at work. In fact, all of the above mentioned studies, except that of Singh and Hill, were conducted in the United States, emphasising the lack of research on technology-related privacy concerns from a European perspective.

A number of studies do not examine privacy issues specifically but rather include it amongst a number of variables that are being measured (e.g. Flavian and Guinaliu, 2006; Chen and Barnes, 2007). For example, Joines *et al.*, 's (2003) study of the influence of demographics and motivational factors on Internet use includes a measure of privacy along with other measures, whilst Lancelot Miltgen's (2007) study focuses on the factors that influence online consumers' decisions to provide personal information as opposed to directly focusing on privacy concerns. Similarly, a number of technology adoption studies include a measure of privacy but do not focus on it uniquely (e.g. Pavlou and Fygenon, 2006; Shih, 2004). The same holds true for many studies that examine the antecedents of trust in electronic commerce (e.g. Cheung and Lee, 2001) where the influence of privacy concerns are examined along with other measures such as security in terms of their influence on behavioural

outcome. Table 1 below provides a sample of the literature directly focusing on technology-related consumer concerns.

Study	Context	Sample	Methodology
Udo (2001).	Examine the privacy and security concerns of online users'	158 participants USA	29 item online questionnaire.
Sheehan (2002)	Study examines online consumers to see if their concerns match those in an offline environment.	889 online respondents USA.	Online survey
Singh and Hill (2003)	Focuses on consumer Internet concerns	106 online consumers. Germany	Paper and pencil survey.
Malhotra <i>et al.</i> , (2004)	Developed internet users privacy concerns measurement instrument (IUIPC)	449 respondents USA	Instrument developed through scenario testing
Van Slyke <i>et al.</i> , (2006)	Assesses the degree to which consumers' information privacy concerns affect their willingness to engage in online transactions.	Two samples were used, one representing a well known merchant (713) the other representing a less well known merchant (287) USA	Survey

Table 1: Studies of technology-related consumer concerns.

Whilst much attention has focused on internet users information privacy concerns, privacy concerns are equally important in the context of the computer-mediated work environment, particularly as most individuals spend significant amounts of their time in such contexts. For example, the use of email and Internet in the workplace has increased management fears relating to the loss of trade secrets through an aggrieved employee and the fear that offensive or explicit material could be used by an employee resulting in adverse publicity for the company (Laudon and Laudon, 2001). Consequently, it is estimated that nearly 80% of all organisations now employ some level of employee surveillance (termed dataveillance) in the day to day running of the company (D'Urso, 2006). While organisations frequently have a number of legitimate reasons to monitor their employees' internet activities, researchers such as Kierkegaard (2005) emphasise the need to investigate the level of control an employer should have over an employees' electronic communications and the degree to which employees should be concerned about this surveillance of the workplace. Other researchers (Alder *et al.*, 2006) concur and emphasise that there are valid concerns regarding the impact of internet monitoring on employees attitudes and behaviours.

Despite a remarkably limited number of studies on this issue (Boehle, 2000), those few studies that do exist provide interesting insights into the importance of this issue and its potential for research. For example, Stanton and Weiss' (2000) study examined the issue of electronic monitoring from both the

employer and employee perspective. A three part survey was derived from a longer semi-structured research instrument used by the authors in a previous study. A surveillance-related question deliberately worded with both positive and negative connotations acted as the focal point of the survey. The respondents exhibited a mixed view of attitudes in response towards electronic surveillance. Surprisingly, only a minority of those actually subjected to monitoring found it to be invasive or negative in any way. Other employees actually displayed positive attitudes towards high levels of surveillance in that it provided them with a deep sense of security and ensured that the line of command was set in place. In this way the results presented go against that of popular culture and the negative hype surrounding electronic surveillance. However, the authors note that a number of limitations in relation to their study, particularly in relation to sample size, restrict its generalisability and point to the need for more detailed research on this issue.

Alder *et al.*, (2006) contend that a critical task facing organisations and researchers is to identify the factors that improve employees' attitude and behavioural reactions to internet monitoring. These authors developed a causal model to explain the impact Internet monitoring has on advanced notification, justification and perceived organisational support in relation to organisational trust in the workplace. Following an initial survey, the respondents were unknowingly subjected to an Internet monitoring and filtering system implemented in their company. Afterwards they were informed that this monitoring activity was taking place. After a set time period, the sample group was sent a second survey to which only 63% of the original sample responded. When the level of employee trust and their attitude towards their specific job was examined, the results indicated that frequent users' of the Internet were more affected by the implementation of internet monitoring than those who used it on an irregular basis. Table 2 outlines literature representing employee concerns.

Study	Context	Sample	Methodology
Stanton and Weiss (2000)	Identifies which attitudes, perceptions, beliefs were influenced by electronic monitoring	49 respondents from approx 25 different organisations.	Online survey
Alder <i>et al.</i> , (2006)	Examines the effects of Internet monitoring on job attitudes	62 employees from a heavy service sales and equipment sales and service centre	Two paper services were administered.

Table 2: Employee dataveillance concerns.

In all of the studies reviewed respondents ranged in age, location, occupation and Internet experience. For the most part the research instruments were adapted from previous studies and reused in a way specific to the study itself. A closer look at the studies presented revealed that all the researchers employed a basic survey approach administering questionnaires and surveys to their respondents. Given the sensitive nature of the research undertaken it is not surprising to see a mixture of both paper and Web surveys utilised in the studies. For example, Alder *et al.*, (2006) opted for a traditional paper and pencil survey in their study to alleviate any concerns the employee might have in regards leaving an electronic paper trail which could be easily monitored by their employer. Similarly it may be assumed that the strict laws governing online marketing practices in Germany may in part account for the basic paper survey chosen by Singh and Hill (2003) in their study. One recurring limitation in all of the studies reviewed however appeared to be size of the samples used (Chen and Barnes, 2007; Alder *et al.*, 2006; Pavlou and Fygenson, 2006; Singh and Hill, 2003; Joines *et al.*, 2003; Stanton and

Weiss, 2000). This indicates the need for an extensive and rigorous survey containing a large sample that can provide generalisable findings to progress understanding in this area.

4. CONCLUSION

The primary objective of this paper was to provide an empirical overview of the technology-related privacy literature. In general studies on technology-related privacy concerns are few and the construct is characterised by a lack of definitional consensus that further compounds our lack of understanding. While privacy issues have long been of concern to consumers' rights advocacy groups, the increased ability of marketers to use technology to gather, store and analyse sensitive information on consumers on a continuously updated basis has increased the acuteness of such concerns. However, the nature of such concerns and important factors that can most strongly predict or inhibit those concerns remains for the main part a matter of speculation, thus limiting our understanding of the construct.

Despite the fact that the uses of employee data surveillance technologies within organisational contexts also contain significant privacy implications, this issue has received surprisingly little attention from researchers to date. Moreover, the factors influencing employers and IS managers in their decisions to electively employ such dataveillance technologies have not been explored nor has any hierarchy of privacy concerns on the part of employers and employees been ascertained. As a result, our understanding of these issues, and the ways in which employee privacy concerns could be diminished, thus positively impacting productivity and morale, remain a matter of speculation and a fruitful avenue for researchers to explore. Furthermore the contrasting perspective of the monitoring ability of such employees' in regard to their employers actions is to date an under-researched area and therefore also warrants further examination in the literature.

References:

- Acquisti, A. (2002). Protecting Privacy with Economic Incentives for Preventive Technologies in Ubiquitous Computing Environment. Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing: UbiComp 2002.
- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate.
- Alder, G.S., Noel, T.W and Ambrose, M.L. (2006). Clarifying the effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust. *Information and Management*, 43 (7), 894-903.
- Boehle, S. (2000). They're Watching You. *Training*, 37 (8), 68-72.
- Cassidy, C.M. and Chae, B. (2006). Consumer Information Use and Misuse in Electronic Business: An Alternative to Privacy Regulation. *Information Systems Management*, 23 (3), 75-87.
- Chen, Y. and Barnes, S. (2007). Initial Trust and Online Buyer Behaviour. *Industrial Management and Data Systems*, 107 (1), 21-36.
- Cheskin eCommerce Trust Study (1999). Cheskin Research and Studio Archetype/Sapient 'eCommerce Trust Study', 1-33. Available at <http://www.studioarchetype.com/cheskin/>
- Cheung, C. M. K. and Lee, M. K. O., (2001) 'Trust in Internet Shopping: Instrument Development and Validation through Classical and Modern Approaches', *Journal of Global Information Management*, 9(3), July-September, pp 23-35.
- Clarke, R.A. (1988). Information Technology and Dataveillance. *Communication of the ACM*, 31 (5), 498-512.
- Cockcroft, S. and Heales, J. (2005). National Culture, Trust and Internet Privacy Concerns. 16th Australasian Conference on Information Systems, Sydney.
- Concise Oxford Dictionary of Current English, Oxford University Press, England, 1996.
- Crompton, M. (2001). What is Privacy?. Privacy and Security in the Information Age Conference, Melbourne.

- D'Urso, S.C. (2006). Who's Watching Us at Work? Toward a Structural-Perceptual Model of Electronic Monitoring and Surveillance in Organisations. *Communication Theory*, **16**, 281-303.
- Flavian, C. and Guinaliu, M. (2006). Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Website. *Industrial Management and Data Management*, 106 (5), 601-620.
- Fried, C. (1968). Privacy. *Yale Law Journal*, 77 (1), 475-493.
- Froomkin, A.M. (2000). The Death of Privacy? *Stanford Law Review*, 52 (146), 1461-1543.
- Galanxhi-Janaqi, H., and Fui-Hoon Nah, F. (2004). U-commerce: Emerging Trends and Research Issues. *Industrial Management & Data System*, 104 (9), 744-755.
- Gefen, D., and Straub, D. (2000). The Relative Importance of Perceived Ease of Use in IS Adoption: A study of E-Commerce Adoption. *Journal of the Association for Information Systems*, 1 (8).
- Goldsmith, R. and E. Bridges. (2000). E-Tailing versus Retailing: Using Attitudes to Predict Online Buying Behavior. *Quarterly Journal of Electronic Commerce*, 1 (3), 245-253.
- Grabner-Krauter, S. and Kaluscha, E. (2003). Empirical Research in Online Trust: A Review and Critical Assessment. *International Journal of Human Computer Studies*, 58 (6), 783-812.
- Graeff, T.R. and Harmon, S. (2002). Collecting and Using Personal Data: Consumers' Awareness and Concerns. *Journal of Consumer Marketing*, 19 (4), 302-318.
- Harris Poll (2004). *Privacy and American Business Press Release* [online]. Available from: <http://www.epic.org/privacy/survey/>
- Hirshleifer J. and Riley J.G. (1979). The Analytics of Uncertainty and Information: An Expository Survey. *Journal of Economic Literature*, **17**, 1375-421.
- Hoffman, D.L., Novak, T.P. and Peralta, M. (1999). Building Consumer Trust Online, *Communications of the ACM*, 42 (4), 80-85.
- Hoyer, W.D and MacInnis, D.J. (1997). *Consumer Behaviour*, Houghton Mifflin Company, Boston.
- Introna, L.D. (1996). Privacy and the Computer: Why we need Privacy in the Information Society. *Ethicomp e-Journal*, 1.
- Joines, J.L., Scherer, C.L. and Scheufele, D.A. (2003). Exploring Motivations for Consumer Web Use and their Implications for E-Commerce. *Journal of Consumer Marketing*, 20 (2), 90-108.
- Kierkegaard, S. (2005). Privacy in Electronic Communication- Watch Your E-Mail: Your Boss is Snooping. *Computer Law and Security Report*, 21 (3), 226-236.
- Konvitz, M.R. (1966). Privacy and the Law: A Philosophical Prelude. *Law and Contemporary Problems*, 31 (2), 272-280.
- Kostakos, V., O'Neill, E., Little, L., & Silence, E. (2005). The Social Implications of Emerging Technologies. *Editorial/ Interacting with Computers*, **17**, 475-483.
- Lancelot Miltgen, C. (2007). Customers' Privacy Concerns and Responses towards a Request for Personal Data on the Internet: An Experimental Study. *Information Management in the Networked Economy: Issues and Solutions*, 400-415.
- Laudon, K.C. and Laudon, J.P. (2001) *Essentials of Management Information Systems: Organisation and Technology in the Networked Enterprise*, Prentice Hall, 4th Ed.
- Lee, M. & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, 6 (1), 75-91.
- Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Casual Model. *Information Systems Research*. 15 (4), 336-355.
- Mayer. R. C., Davis, J.D. and Schoorman, F.D. (1995). An Integrative Model of Organisational Trust. *Academy of Management Review*, 20 (3), 709 – 734.
- Miyazaki, A.D. and Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs*, **35**, Summer, 27-44.
- Moor, J.H. (1990). Ethics of Privacy Protection. *Library Trends*, 39 (1&2), 69-82.
- Moor, J.H. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society*, 27 (3), 27-32.
- Parker, R.B. (1974). A Definition of Privacy. *Rutgers Law Review*, 27 (1), 275.

- Pavlou, P.A. and Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behaviour. *MIS Quarterly*, 30 (1), 115-143.
- Platt, R.G. (1995). Ethical and Social Implications of the Internet. *The Ethicomp E-Journal*, 1.
- Powers, M. (1996). A Cognitive Access Definition of Privacy. *Law and Philosophy*, 15 (4), 369-386.
- Prakhaber P.R.. (2000). Who owns the Online Consumer? *Journal of Consumer Marketing*, 17 (2), 158-171.
- Ratnasingham, P. (1998). Trust in Web-based Electronic Commerce Security. *Information Management and Computer Security*, 6 (4), 162-168. MCB University Press. <http://www.emerald-library.com/pdfs/04606dc2.pdf>.
- Reichheld, F.F. and Scheffer, P. (2000). E-Loyalty: Your Secret Weapon on the Web. *Harvard Business Review*, 78 (4), 105-113.
- Robey, D. (1979). User Attitudes and Management Information System Use. *Academy of Management Journal*, 22 (3), 527-538.
- Rule, J.B. (2004). Towards Strong Privacy: Values, Markets, Mechanisms, and Institutions. *University of Toronto Law Journal*, 54 (2), 183-225.
- Rust, R.T., Kannan, P.K. and Peng, Na. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30 (4), 455-464.
- Safire, W. (2002). The Great Unwatched. *New York Times*. Available at <http://query.nytimes.com/gst/fullpage.html?res=9A03E7DB1E3FF93BA25751C0A9649C8B63>
- Schoeman F. (1984). Privacy: Philosophical Dimensions of the Literature: in *Philosophical Dimensions of Privacy: An Anthology* (F.Schoeman, ed., 1984).
- Sheehan, K.B. (2002). Towards a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18, 21-32.
- Shih, H. (2004). Extended Technology Acceptance Model of Internet Utilization Behaviour. *Information and Management*, 41 (6), 719-729.
- Singh, T. and Hill, M.E. (2003). Consumer Privacy and the Internet in Europe: A View from Germany. *Journal of Consumer Marketing*, 20 (7), 634-651.
- Smith, H.J. (2001). Information Privacy and Marketing: What the U.S Should (and Shouldn't) Learn from Europe. *California Management Review Reprint Series*, 43 (2), 8-33.
- Stanton, J.M. and Weiss, E.M. (2000). Electronic Monitoring in their Own Words: An Exploratory Study of Employees' Experiences with New Types of Surveillance. *Computers in Human Behavior*, 16 (4), 423-440.
- Tavani, H.T. (1999). Internet Privacy: Some Distinctions between Internet Specific and Internet-Enhanced Privacy Concerns. *The ETHICOMP E-Journal*. 1, 1999.
- Tavani, H.T. (2004). *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Wiley International Edition, John Wiley and Sons.
- Tracy, B. (1995). *Advanced Selling Strategies*. Simon and Schuster Paperbacks, New York.
- Turban, E., Leidner, D., McClean, E., & Wetherbe, J. (2006). *Information Technology for Management – Transforming Organisations in the Digital Economy*. 5th Edition. John Wiley & Sons Inc, USA.
- Udo, G.J. (2001). Privacy and Security Concerns as Major Barriers for E-Commerce: A Survey Study. *Information Management and Computer Security*. 9 (4), 165-174.
- Van Slyke, C., Shim., J.T., Johnston, R. and Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal for the Association of Information Systems*, 7 (6), 415-444.
- Warren, S and Brandeis, L.D. (1860). The Right to Privacy. *Harvard Law Review*, 4 (193).
- Westin, A. (1967). *Privacy and Freedom*. Ateneum, New York.