

ONLINE PRIVACY CONCERNS: THREAT OR OPPORTUNITY?

Cliona McParland , Regina Connolly

Dublin City University Business School

Abstract

As Internet adoption continues to grow exponentially, so too have threats to privacy. While the Web empowers the consumers enormously, they are increasingly aware of the ways in which technology can be used to collect potentially sensitive information regarding them and the ability of vendors to use this information without their expressed permission. On one hand, marketers face intense competition in the marketplace and need to have sophisticated knowledge of their consumers in order to provide products and services that satisfy. However, on the other hand, consumer information privacy concerns have become an issue of great sensitivity. This paper provides a brief review of some of the issues surrounding consumer privacy in a networked era and outlines how some new technologies have exacerbated privacy concerns. It suggests that companies should respond to privacy concerns in a positive manner by treating consumer information privacy concerns as an opportunity rather than a threat.

Keywords: *Privacy, Consumer information, Technology, Data gathering.*

1 INTRODUCTION

The move from a transaction focus to a customer relationship focus has resulted in marketers having a greater need to update knowledge of consumers in order to configure products and services designed to satisfy individual user needs and tastes. This need for consumer knowledge has resulted in widespread adoption of practices where information on the individual consumer is collected, stored and analysed in an effort to continuously learn about changing consumer needs. Vast improvements in technology have resulted in a growing awareness amongst consumers that significant threats to their privacy exist and must be addressed. It is difficult to determine exactly when in history the desire for privacy first emerged as a significant concern for individuals. Christian tradition describes Adam and Eve's awareness that they had violated each other's privacy after eating the forbidden fruit resulting in their need to make cover for themselves with fig leaves sewn together (Genesis, 3:7). However, other traditions such as Greek philosophical tradition argue that the right of privacy is subject to the right of the society, with philosophers such as Aristotle emphasising that man must forsake his privacy as in his view it is not possible for private beings to subsist in a civilized society (Politics, 1253a 25-30). The Italian renaissance philosopher Machiavelli introduced the concept of separating the private individual from the public citizen, allowing each of us to take on a personal persona (The Prince, 2003), a view that is supported by the British empiricist Locke (1698: 116) who argued that '*every man has a property in his own person; this nobody has a right to but himself*'. More recently researchers (Pilon, 2003;

Litman 1999; Epstein, 1989; Miller, 1971) have argued that privacy should be treated as a property right with Pilon (2003: 146) maintaining '*property is the foundation of every right we have, including the right to be free*'. The view of privacy as a fundamental human right is enshrined in laws such as the Universal Declaration of Human Rights (UN, 1948: Article 12), the International Covenant on Civil and Political Rights (1966: Article 17) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (CoE, 1984: Article 8). In the literature, the view of privacy as a human right is supported by Fried (1970) who argues from a Kantian background that privacy is a concept that provides a 'rational context' as it is essential in order for love, friendship, trust and respect to develop among individuals. Support for this view is provided by Young (1979) and Schoeman (1984) with the latter construing privacy as a significant aspect of human decorum. Other researchers such as Kouw *et al.*, (2004) and Boatright (2004) also argue for privacy to be considered a natural or metaphysical right stemming from their beliefs that there is a 'higher law' than that of any political or governmental power that applies to everyone and serves as a standard by which we should all live. The divergent viewpoints as to whether privacy should be viewed as a property right or a human right may well be culturally biased (De Boni and Prigmore, 2002). What is clear, regardless of viewpoint, is that researchers are united in agreement that privacy concerns are a significant issue meriting our attention and protection.

2 PRIVACY CONCERNS & CONTROL

The first publicly acknowledged definition of privacy would appear to be that of Warren and Brandeis in their Harvard Business Review article of 1890. They argue that privacy is the right to be let alone and Sheehan (2002) contends that this definition has become the basis of much privacy legislation for the past century. Information systems researchers such as Laudon (2005: 159) extend Warren and Brandeis's definition maintaining that privacy is '*the claim of individuals to be left alone, free from surveillance, or interference from other individuals or organisations including the state*'. Control is defined as '*the power of directing command, the power of restraining*' (Oxford, 1996: 291) and is considered to be a major antecedent in explaining the concept of privacy. For many researchers the key issue in defining privacy relates to the ability to exert control over personal information. Thus, 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 theory of personal control is widely supported by privacy researchers such as Fried (1968: 482) who defines privacy as the '*control we have over information about ourselves*' and Parker (1974: 281) who defines it in terms of the '*control over who can sense us*'. Similarly, Stone *et al.*, (1983: 460) define privacy as '*the ability of the individual to control personally information about one's self*'. It is understandable that individuals should want and be entitled to a certain level of command over their personal information. Thus Elgesem (1996) comments that personal privacy is the ability to permit to the communication or distribution of one's personal privacy and Laudon (1996: 93) concurs suggesting that they aim to control its dissemination by '*sharing it with some but not with others*'. Clarke (1988) suggests personal control is important in regards information privacy specifically as it is concerned with the interest of individuals to control or significantly influence the handling of personal data. Other researchers (Goldberg, 2000; Keen *et al.*, 2000; Platt, 1995; Agranoff, 1993) also support this notion of individuals gaining specific control over the distribution of sensitive information and to have the ability to regulate information privacy concerns.

As we move further and further into a surveillance society it becomes apparent that most individuals yearn for a certain level of control over their personal and sensitive information. For example, 1999 Louis Harris poll indicated that 70% of online users felt uncomfortable disclosing personal information online while a 2003 Harris poll of 1010 adults also found that 69% of those surveyed described their ability to control the collection of personal information as being 'exceptionally important'. A subsequent (2004) Harris Poll found that 87% of the 2136 adults surveyed had made a conscious decision to protect their own privacy by requesting that companies remove personal information from their databases. This confirms the increasing concern of individuals regarding the violation of their privacy and their desire to be able to control their personal information. Interestingly, while individuals' sensitivity to control their private information is an issue of increasing concern, the truth regarding the extent of control over that personal information is often misunderstood, particularly amongst the internet-using public. This is confirmed by a 2005 study by the Annenberg Public Policy Centre which discovered that 47% of the 1500 adults surveyed falsely believed they were able to control personal information distributed about them online simply because they had the right to view data collated by the on-line vendor, while a further 50% falsely believed they could control the depth of information contained on them by having the ability to edit information as and when they saw fit (Turow *et al.*, 2005). However, online vendors do not seek to enlighten their customers that this is not the case. Not all privacy researchers concur that privacy should be described in terms of control over personal information. In fact, a diverse body of research dispute that view. For example, Schoeman (1984) argues that control is not a necessary or acceptable condition of privacy while Moor (1990; 1997) posits that privacy is better defined in terms of some level of restricted access rather than control. Agreeing with Lyon's (1994) view that to participate in modern society one must accept being under electronic surveillance, Chellappa (2001: 148) suggests that '*there is no such thing as absolute privacy in a social order*' as this is something which no individual can control, while Tavani (2001: 6) suggests that an individual can have '*control but no privacy*' or '*privacy but no control*'. Consequently, Tavani concludes that while privacy and control are mutually supporting concepts, he argues that these constructs are frequently confused and therefore surmises that it is more useful for researchers to treat these constructs separately.

3 TRUST, PRIVACY & UNCERTAINTY

The literature recognises the importance of trust in the specific business-to-consumer on-line transaction domain (Lee and Turban, 2001; Gefen, 2000; Reichheld and Scheffer, 2000). Ratnasingham (1998) contends that the influence of trust on interactions is even more crucial in global electronic commerce than in the physical marketplace, while 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.*' 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 be used to better understand the uncertainty that applies to the on-line purchase environment. This theory outlines two categories of uncertainty: *system-dependent uncertainty* and *transaction-specific uncertainty*. Both types of uncertainty exist in the on-line purchase environment. For example, the on-line 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 on-line purchase environment. Research has shown that customers frequently have legitimate anxiety about transaction confidentiality and anonymity (Ratnasingham, 1998). As each consumer is unique, the extent of perceived risk will be influenced by issues specific to the individual. For example, the extent to which on-line consumers are concerned about privacy issues is influenced by their education (Burke, 2002), Internet experience and interaction readiness (Miyazaki and Fernandez, 2001).

3.1 Internet Specific versus Internet Enhanced Concerns

The exponential growth of the Internet has ensured that threats to our privacy can occur at a magnitude previously deemed impossible. Seeking to improve our understanding of the privacy construct, Tavani (1999) subdivides privacy concerns into Internet-enhanced and Internet-specific privacy concerns. The former relate to data gathering and monitoring processes in addition to data exchange and data mining techniques, all of which combine to erode the individual's privacy. Prakabher (2000) notes that each time an individual interacts with the Web, they leave behind a trail of detailed information regarding who they are, their buying habits, financial details, and other personal details. Individuals have little control over who can access that information and what can be done with it. Market researchers with access to such information can drill down and extract data of specific interest to them. Such technological processes ensure that an Internet users' online activities can be monitored and information about them gathered either directly or indirectly leading to the exchange of personal and sometimes sensitive information at an unparalleled rate. Therefore it may be unrealistic to expect that profit-driven businesses will not infringe on consumer privacy in an environment where information on consumers is highly profitable and easy to collate. However, Prakhaber (2000) argues that the fundamental problem in Internet privacy is not the disclosure of sensitive information by itself as long as that information is given voluntarily and consumers are made aware as to how it is being used. Such a scenario is not a violation of privacy. Rather the concern relates to the collection of private information without consumer permission and the selling of that information to other databases owned by companies other than the one with whom the consumer is interacting. These internet-enhanced concerns are highlighted in practitioner reports such as the AT&T (1999) research report that found that 48% of respondents would feel more comfortable providing personal information if there was a law to prevent the site from using the information for any purpose other than processing the specific transaction, the (2003) Harris Poll which reported that 79% of individuals surveyed considered it to be extremely important to be in control of who is

allowed to access their personal information, and the (2003) PC World study which showed that 76% of the 1500 Internet users surveyed were ‘highly concerned’ with a websites’ tracking habits and that 95% of those respondents were ‘highly concerned’ with a websites’ ability to collect sensitive information. The second type of privacy concern identified by Tavani (1999) is described as Internet-specific concerns. These concerns related to certain threats to personal privacy that are attributable to the Internet itself such as the use of Internet Cookies and Search Engines. Internet Cookies have generated substantial controversy forming a paradox between the advantages and disadvantages of such a technology. Cookies allow online retailers to record an individuals’ personal information and then store it on their own system. This allows market researchers and online vendors to build up a profile on any individual that visits a certain site providing them with an insight into their behaviours and tendencies. Defenders of this facility maintain they are customising individuals shopping experiences and habits offering a service whereby they can focus in on specific needs. Opposers of this argument argue that their right of privacy is being significantly invaded and that the gathering, storing and exchange of data between the user and the website frequently occurs without the user’s knowledge or consent (Tavani, 1999). Moreover, practitioner reports such as the PC World (2003) study confirm the level of internet specific privacy concerns that exist in their finding that 88% of respondents were concerned about a website sharing or selling email addresses. The value of such surveys lies in the fact that they act as a barometer of the level of apprehension and anxiety regarding possible privacy violations that surround the use of the World Wide Web and connecting technologies over the past decade. 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).

3.2 Ubiquitous Computing

Weiser (1993: 71) first described the concept of ubiquitous computing as ‘*the non-intrusive availability of computers throughout the physical environment, virtually if not effectively, invisible to the user*’. Singh *et al.*, (2005: 421) follow this same belief by defining ubiquitous computing as a ‘*global computing environment where seamless and invisible access to computing resources is provided to the user*’. Wang *et al.*, (2006) concur suggesting that the main purpose of ubiquitous computing is to employ a user centric and application focused computing environment. Watson *et al.*, (2002: 336) suggest that u-commerce personifies the characteristics of ubiquity, universality, uniqueness and unison thus differentiating it from traditional commerce. They note that ‘*the ubiquity, or omnipresence, of computer chips means not only that there are everywhere but that are, in a sense, ‘nowhere’ for they become invisible as we no longer notice them.*’ Other researchers such as Langheinrich (2002b) and Schmandt and Ackerman (2004) note that ubiquitous computing has become such a large part of our daily lives that most fail to even notice it. In part this stems from the fact that technological devices can be so small that they disappear from sight and from the fact they have now become so familiar to us that we no longer notice using them (Kostakos *et al.*, 2005; Lederer, 2003).

The emergence of ubiquitous computing has resulted in increased privacy concerns among many individuals, a fact noted by many researchers from varying disciplines (Hong *et al.*,

2004; Hong and Landay, 2004; Lederer, 2003; Langheinrich, 2002a). Langheinrich (2002a) for example foresees personal privacy becoming a major concern potentially affecting the widespread deployment of ubiquitous computing and technologies. Lederer (2003) notes how the expansion of ubiquitous systems and consequently the increased level of data mining techniques that pursue have strengthened and magnified an individual's ability to track and collect personal information, thus increasing privacy concerns. It is conceivable that individuals' desire privacy-sensitive ubiquitous applications (Hong *et al.*, 2004; Hong and Landay, 2004), a concept significantly developed on by Galanxhi and Fui-Hoon (2006) who note the kinds of information that can be gathered, how it can be used, and the accountability of those that gather sensitive data are all significant privacy concerns. The authors further suggest that a users desire to become empowered decision makers regarding their own level of privacy and the fear over who can gain access to information which has been gathered are extremely relevant concerns in a ubiquitous or pervasive computing environment.

3.3 Pervasive Computing

Despite the fact that the terms 'ubiquitous' and 'pervasive' computing are often used interchangeably (Schieck *et al.*, 2006; Rao and Zimmermann, 2005; Niemela and Latvakoski, 2004; Simpson, 2004), a diverse body of research argues that they are in fact conceptually different (Singh *et al.*, 2005; Lyytinen and Yoo, 2002). For example, Dryer *et al.*, (1999: 652) define pervasive computing as a *'move from an interaction between an individual and a single device to an abundance of networked mobile and embedded computing devices that individuals and groups use across a variety of tasks and places'*. For Turban *et al.*, (2004: 273) pervasive computing is a *'world in which virtually every object has processing power with wireless or wired connections to a global network'*, while for Landry *et al.*, (2005: 445) pervasive computing technologies are systems that offer *'secure, robust, real-time, seamless universal access to data via a wide array of devices and a means to communicate all of it'*. For many researchers who bear this delineated perspective a pervasive computing environment is characterised by an emphasis on the seamless integration of the technology to the degree that it is no longer noticed and to a large extent disappears (Rao and Zimmermann, 2005; Turban *et al.*, 2004; Simpson, 2004; Lyytinen and Yoo, 2002; Satyanarayanan, 2001). The invisibility characteristic implies that such mechanisms do not impose on our consciousness. Because invisibility is a characteristic that applies equally to ubiquitous commerce (Galanxhi and Fui-Hoon, 2004; Watson *et al.*, 2002; Langheinrich, 2001; 2002b; Weiser, 1991; 1993) this leads to difficulty in distinguishing between the two constructs. Some researchers (e.g. Singh *et al.*, 2005; Lyytinen and Yoo, 2002) have sought to distinguish between the constructs by describing a ubiquitous computing environment as one that integrates the benefits and advances of both mobile and pervasive computing. Other researchers (e.g. Niemela and Latvakoski, 2004) however, remain trenchant in their view that pervasive computing is merely another term used for ubiquitous computing. Whether or not the distinction between these constructs is worthy of note, the fact remains that pervasive/ubiquitous computing raise significant privacy challenges both on a social and individual level. Satyanarayanan (2001) suggests that as a user becomes more au fait and dependent on pervasive devices the system develops an awareness and understanding of their movements, behaviour patterns and habits thus spawning considerable privacy concerns. It is the invisibility factor consistent with pervasive mechanisms that generates privacy concerns among users as it becomes more difficult to determine whether sensitive data is being gathered and used (Hong *et al.*, 2005). The greatest obstacle to its extensive deployment is

considered to be widespread user resistance to intrusion generating the need for privacy zones (Schieck *et al.*, 2006; Kostakos *et al.*, 2004; Kostakos *et al.*, 2006).

3.4 RFID Technologies

Radio Frequency Identification technologies (RFID) have been defined as ‘*an electronic tagging technology that allows an object, place, or person to be automatically identified at a distance without a direct line-of-sight, using an electromagnetic challenge/response exchange*’ (Want, 2004: 41). These small, low-cost devices can hold a limited amount of data and report that data when queried over radio by a reader (Molnar and Wagner, 2004). The time and cost of processing tagged items is significantly reduced through the use of RFID systems (Karthikeyan and Nesterenko, 2005). Recently a close link has been identified between RFID technologies and CRM (Customer Relationship Management) techniques, forming a relationship which sustains product transparency resulting in a well managed supply chain run with on demand information in real time (Smith, 2005). Taghaboni-Dutta and Velthouse (2006) propagate that RFID technology has the potential to enhance an individuals shopping experience thus reducing shopping frustration. However, Smith (2005) notes how a precise combination of CRM processes and RFID based technology can enable a firm to track a customers buying pattern and analyse their buying behaviour dramatically improving their purchasing experience. Clearly this can lead to a conflict between the vendor’s ‘need to know’ versus the individuals ‘right not to tell’ (Platt, 1995) adding fuel to existing privacy concerns on the part of the individual. Examining the issue of privacy from a value proposition perspective, both Weiss (2003) and Hong *et al.*, (2004) note that retailers benefit from RFID through inventory tracking thus maintaining a steady and efficient supply chain whilst consumers become data sharers exposing themselves to furtive tracking often with little relevant benefits to themselves. Additional disadvantages to the consumer include the ease with which an attacker can obtain an illegitimate RFID reader since a reader is little more than a radio receiver. Jones *et al.*, (2004) argue that the fear of sensitive data being stored on the tag after the point of sale is a real concern for consumers, while Smith (2005) notes that the item tagged by RFID can still be monitored after the consumer leaves the store. Moreover, consumer privacy can be affected by target marketing if RFID is used to classify consumers’ by their shopping history and patterns (Karjoth and Moskowitz, 2005). Ohkubo *et al.*, (2003) and Shih *et al.*, (2005) suggest that placing private information on a RFID tag is potentially dangerous as such information can be acquired by an outside source if it is leaked via the network or as a direct result of the communication between the tag and reader – otherwise known as eavesdropping. A second concern, traceability, involves the tracking of individuals through the use of RFID tags and the violation of location privacy, an issue that has received much attention from privacy researchers (Taghaboni-Dutta & Velthouse, 2006; Shih *et al.*, 2005; Molnar and Wagner, 2005; Nohara *et al.*, 2005; Smith, 2005; Hong *et al.*, 2004; Johansson, 2004; Jones *et al.*, 2004; Want, 2004; Weiss, 2003). Data can be correlated from multiple tag reader locations thus tracking location, social and financial interactions. Other researchers (Karthikeyan and Nesterenko, 2005; Molnar and Wagner, 2005; Nohara *et al.*, 2005) concur that the widespread adoption of RFID devices poses considerable tracking and monitoring privacy risks that did not exist with previous technologies, all of which result from the basic functionality of RFID technologies as ‘*an ID can be read without permission, is constant and unique, and contains potentially sensitive data*’ (Ohkubo *et al.*, 2005: 68-69). Subirana and Bain (2006) summarise the situation by noting that it is the users’ sense of uncertainty and lack of control that generates the biggest privacy concerns. his uncertainty

and lack of control related to all of the technologies mentioned reflect the significant asymmetry that exists in terms of what the Internet means to individuals versus companies. For example, Prakhober (2000) rightly points out that while the technology has created better, faster and cheaper ways for businesses to meet the needs of their customers and better faster and cheaper ways for customers to satisfy their needs, however 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.

4 SUMMARY

While privacy issues have long been of concern to consumers' privacy 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 these concerns. This paper has outlined a number of ways in which as the technological environment has become more sophisticated it consequently accentuates consumer privacy concerns. While marketers need information on consumers in order to refine products and services thus increasing 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. In this environment, businesses have a choice as to how they should respond. Their choice will determine 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. Trust is key to the success of electronic commerce. In order for trust to be engendered, consumers must be confident that their personal information will not be used without their consent and will not be sold to third parties. That bond of trust is fragile. 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 ownership of on-line consumers will be predicated to a large degree on the way in which businesses seeking to leverage Internet technology will gather market information while equally embracing the responsibility of preserving consumer privacy.

REFERENCES

- Agranoff, M.H. 1993. 'Controlling the Threat to Personal Privacy'. *Journal of Information Systems Management*, 8(3): 48-52.
- AT&T Research. 1999. Centre for Democracy and Technology [online]. Available from: <http://www.cdt.org/privacy/survey/findings/index.shtml#att1999>
- Boatright, R.J. 2004. 'Ethics and the Conduct of Business'. Pearson Education, London.
- Burke, R.R. 2002. 'Technology and the Customer Interface: What Consumers Want in the Physical and Virtual Store'. *Journal of the Academy of Marketing Science*, Vol. 30 (Fall): 411-432.
- Chellappa, R.K. 2001 'Contrasting Expert Assessment of Privacy with Perceived Privacy: Implications for Public Policy'. Redondo Beach, CA: 147-154.
- Cheskin eCommerce Trust Study (1999) Cheskin Research and Studio Archetype/Sapient (1999), 'eCommerce Trust Study' pp. 1-33. Available at <http://www.studioarchetype.com/cheskin/>
- Clarke, R.A. 1988 'Information Technology and Dataveillance'. *Communication of the ACM*, 31(5): 498-512.
- Concise Oxford Dictionary of Current English. 1996. Oxford University Press, England.
- De Boni, M., and Prigmore, M. 2002. 'Cultural Aspects of Internet Privacy'. IN: *Proceedings of the 7th Annual UK Academy for Information Systems Conference (UKAIS'02)*, Leeds.

- Dryer, D.C., Eisbach, C., & Ark, W.S. 1999. 'At What Cost Pervasive? A Social Computing View of Mobile Computing Systems'. *IBM Systems Journal*, 38 (4): 652-676.
- Elgesem, D. 1996. 'Privacy, Respect for Persons, and Risk'. *Philosophical Perspectives on Computer Mediated Communication*, edited by C.Ess, New York: State University of New York Press.
- Epstein, R.A. 1989. 'Takings: Private Property and the Power of Eminent Domain'. *Harvard University Press*, USA.
- Fried, C. 1968. 'Privacy' *Yale Law Journal*, 77(1): 475-493.
- Fried, C. 1970. 'Privacy: A Rational Context,' Chap. IX in *Anatomy of Values*, (Cambridge University Press, New York).
- Galanxhi-Janaqi, H., and Fui-Hoon Nah, F. 2004. 'U-commerce: Emerging Trends and Research Issues' *Industrial management & Data Systems*, 104(9): 744-755.
- Galanxhi-Janaqi, H., and Fui-Hoon Nah, F. 2006. 'Privacy Issues in the Era of Ubiquitous Commerce' *Electronic Markets*, 16(3): 222-232.
- Gefen, D. 2000. 'E-Commerce: The Role of Familiarity and Trust'. *Omega: The International Journal of Management Science*, 28(6): 725—737.
- Genesis 3:7, Good News Bible, Deuterocanonical Books/Apocrypha, The Bible Societies, 1979.
- Goldberg, I.A. 2000. 'A Pseudonymous Communications Infrastructure for the Internet'. PhD Dissertation. U.C. Berkeley, C.A.
- 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.
- Harris Poll. 2003. Harris Interactive [online]. Available from: http://www.harrisinteractive.com/harris_poll/index.asp?PID=365
- 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.
- Hong, J.I., and Landay, J.A. 2004. 'An Architecture for Privacy- Sensitive Ubiquitous Computing'. *IN: International Conference on Mobile Systems, Applications & Services, Proceedings of the 2nd International Conference on Mobile Systems, Applications & Services*, Boston MA USA pp177-189.
- Hong, J.I., Ng, J.D., Lederer, S., and Landay, J.A. 2004. 'Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems'. *Symposium on Designing Interactive Systems. Proceedings of the 2004 Conference on Designing Interactive Systems: Processes, practices, methods & techniques*, Cambridge MA USA pp91-100.
- Hong, D., Yuan, M., and Shen, V.Y. 2005. 'Dynamic Privacy Management: A Plug-In Service for the Middleware in Pervasive Computing'. *IN: MobileHCI*, ACM International Conference Proceeding Series; Vol. 111 Proceedings of the 7th international conference on Human computer interaction with mobile devices & services, Sept 19-22. Salzburg, Austria.
- Johansson, B. 2004. 'An Introduction to RFID – Information Security and Privacy Concerns'. *TDDC03 Projects*, Spring 2004.
- Jones, P., Clarke-Hill, C., Shears, P., Comfort, D., & Hillier, D. 2004. 'Radio Frequency Identification in the UK: Opportunities and Challenges'. *International Journal of Retail and Distribution Management*, 32(3): 164-171.
- Karjoth, G., & Moskowitz, P.A. 2005. 'Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced'. *IN Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society WPES'05* Alexandria, Virginia, November.
- Karthikeyan, S., & Nesterenko, M. 2005. 'RFID Security without Extensive Cryptography'. *IN Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks SASN '05*, Alexandria, Virginia, November.
- Keen, P., Balance, C., Chan, S. & Schrupp, S. 2000. 'Electronic Commerce Relationships: Trust by Design', Prentice Hall.
- Kostakos, V., & O'Neill, E. 2004. 'Extending Traditional Design Approaches for Pervasive Computing'. Prep 2004, 5-7th April, University of Hertfordshire, UK.
- Kostakos, V., O'Neill, E., Little, L., & Silience, E. 2005. 'The Social Implications of Emerging Technologies'. *Editorial/ Interacting with Computers*, 17: 475-483.

- Kostakos, V., O'Neill, E., & Penn, A. 2006. 'Designing Urban Pervasive Systems'. *IEEE Computer Society*, September 2006, 30-37.
- Kouw, M., Pater, L. & Schreuders, E. 2004 'No fear or hope but new weapons: a deconstruction of privacy'. *The ETHICOMP E-Journal*, Volume 1.
- Landry, B.J.L., Mahesh, S., & Hartman, S.J. 2005. 'The Impact of the Pervasive Information Age on Healthcare Organizations'. *Journal of Health and Human Services Administration*, 27(4): 444-464.
- Langheinrich, M. 2001. 'Privacy by Design – Principles of Privacy – Aware Ubiquitous Systems'. IN: *Proceedings of the 3rd International Conference on Ubiquitous Computing*, Atlanta, Georgia. Springer-Verlag LCNS 2201, pp273-291.
- Langheinrich, M. 2002a. 'A Privacy Awareness System for Ubiquitous Computing Environments'. IN: *4th International Conference on Ubiquitous Computing (Ubicomp)*, Spring-Verlag LNCS 2498, pp237-245.
- Langheinrich, M. 2002b. 'Privacy Invasions in Ubiquitous Computing' *Paper presented at UbiComp*, 2002, Goteborg, Sweden.
- Laudon, K.C. 1996. 'Markets and Privacy'. *Communications of the ACM*, 39(9): 92-104.
- Laudon, K.C. 2005. 'Essentials of Management Information Systems : Managing the Digital Firm'. 6thed. New Jersey: Prentice Hall.
- Lederer, S. 2003. 'Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing'. *M.S Report*, Computer Science Division University of California at Berkley December 2003.
- Lee, M. & Turban, E. 2001, 'A Trust Model for Consumer Internet Shopping', *International Journal of Electronic Commerce*, 6(1): 75-91.
- Litman, J. 1999. 'Information Privacy/Information Property'. *Stanford Law Review*, 52: 1283-1313.
- Locke, J. 1698 'Two Treatises of Government: In the Former, The False Principals and Foundation of Sir Robert Filmer, And His Followers are Detected and Overthrown. The Latter is an Essay concerning The True Original, Extent, and End of Civil Government', London. Available at <http://socserv.mcmaster.ca/econ/ugcm/3ll3/locke/government.pdf> accessed 09/02/07 at 22:55.
- Louis Harris poll. 1999, Louis Harris and Associates [online]. Available from: <http://www.natlconsumersleague.org/FNLSUM1.PDF>
- Lyon, D. 1994. 'The Electronic Eye – The Rise of Surveillance Society'. Polity Press: Cambridge.
- Lyytinen, K., & Yoo, Y. 2002. 'Issues and Challenges in Ubiquitous Computing'. *Communications of the ACM*, 45(12): 63-65.
- Machiavelli, N. 'The Prince'. Translated with Notes by George Bull, Introduction by Anthony Grafton. Penguin Classics, 2003.
- 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.
- Miller, A.R. 1971. 'The Assault on Privacy'. University of Michigan Press.
- 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.
- Molnar, D., & Wagner, D. 2004. 'Privacy and Security in Library RFID Issues, Practices, and Architecture'. IN: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society WPES'05*, Washington, DC October.
- 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.
- Niemela, E., & Latvakoski, J. 2004 'Survey of Requirements and Solutions for Ubiquitous Software'. IN: *ACM International Conference Proceeding Series; Vol. 83 Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia*, College Park, Maryland: 71-78.
- Nohara, Y., Inoue, S., Baba, K., & Yasuura, H. 2005. 'Quantitative Evaluation of Unlinkable ID Matching Schemes'. IN: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society WPES'05*, November, Virginia, USA.
- Ohkubo, M., Suzuki, K., & Kinoshita, S. 2003. 'Cryptographic Approach to 'Privacy-Friendly' Tags'. Nippon Telegraph and Telephone, November.
- Parker, R.B. 1974. 'A Definition of Privacy'. *Rutgers Law Review*, 27(1): 275.
- Pilon, R. 2003. 'Property Rights and Regulatory Takings'. *CATO Handbook for Congress*, Policy Recommendations for the 108th Congress: 145-161.
- Platt R.G. 1995. 'Ethical and Social Implications of the Internet'. *The ETHICOMP E-Journal*, Vol. 1. Politics, 1453a 25-30 – Aristotle 1984. Politics, English translation, in Barnes, J. (ed.), 'The complete works of Aristotle', Oxford.
- Prakhaber P.R. 2000. 'Who owns the Online Consumer?'. *Journal of Consumer Marketing*, 17(2): 158-171.

- Rao, B., & Zimmermann, H. 2005. 'Preface to the Focus Theme Section – Pervasive Computing/Ambient Intelligence'. *Electronic Markets*, 15(1): 3.
- 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.
- Satyanarayanan, M. 2001. 'Pervasive Computing: Vision and Challenges'. To appear in IEEE Personal Communications.
- Schieck, A.F., Penn, A., Kostakos, V., O'Neill, E., Kindberg, T., Fraser, D.S., & Jones, T. 2006. 'Design Tools for Pervasive Computing in Urban Environments'. *DDSS*.
- Schmandt, C. & Ackerman, M. 2004. 'Personal and Ubiquitous Computing – Issue on Privacy and Security'. *Pers Ubiquit Comput* (2004) 8(6): 389-390.
- 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: pp21-32.
- Shih, D.H., Lin, C.Y., & Lin, B. 2005. 'RFID Tags: Privacy and Security Aspects'. *IN: Proceedings of Southwest DSI 2006 Annual Conference, Dallas TX:332-44*.
- Simpson, R.L. 2004. 'Where will be in 2015?'. *Nursing Management*, 35(12): 38-44.
- Singh, S., Puradkar, S. & Lee, Y. 2005. 'Ubiquitous Computing: Connecting Pervasive Computing through Semantic Web'. Springer-Verlag.
- Smith, A.D. 2005. 'Exploring Radio Frequency Identification Technology and its Impact on Business Systems'. *Information Management and Computer Security*, 13(1): 16-28.
- Stone, E.F, D.G. Gardner, H.G. Gueutal and S. McClure. 1983. 'A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations'. *Journal of Applied Psychology*, 68(3): 459-468.
- Subirana, B., and Bain, M. 2006. 'Legal Programming'. *Communications of the ACM*, 49(9): 57-62.
- Taghaboni-Dutta, F., & Velthouse, B. 2006. 'RFID Technology is Revolutionary: Who Should be Involved in this Game of Tag'. 20(4): 65-78.
- Tavani, H.T. 2001. 'Privacy Protection, Control of Information and Privacy Enhancing Technologies'. *Computers and Society*, March 2001.
- Tavani, H.T. 1999. 'Internet Privacy: Some Distinctions between Internet Specific and Internet-Enhanced Privacy Concerns'. *The ETHICOMP E-Journal*, Volume 1.
- The Great American Privacy Makeover. 2003. PC World [online]. Available from: <http://www.pcworld.com/article/id,112468-page,1/article.html>
- Turban, E., McClean, E., & Wetherbe, J. 2004. 'Information Technology for Management – Transforming Organisations in the Digital Economy'. *John Wiley & Sons Inc, USA*.
- Turow, J., Feldman, L., and Mettler, K. 2005. 'Open to Exploitation: American Shoppers Online and Offline. A Report from the Annenberg Public Policy Centre of the University of Pennsylvania.
- UN and CoE see Vasiliu *et al.*, 2002 'Personal Information Privacy Issues in B2C eCommerce: A Theoretical Framework.
- Wang, H., Zhang, Y. and Cao, J. 2006. 'Ubiquitous Computing Environments and its Usage Access Control'. *IN: ACM International Conference Proceeding Series, Vol.152 Proceedings of the 1st International Conference on Scalable Information Systems*, Hong Kong Article No.6 2006.
- Want, R. 2004. 'The Magic of RFID'. *Intel Research*, Queue, October 2004: 41-48.
- Warren, S., and Brandeis, L.D. 1890. 'The Right to Privacy'. *Harvard Law Review*, 4:193.
- Watson, R.T., Pitt, L.F., Berthon, P, Zinkhan., G.M. 2002. 'U-Commerce: Expanding the Universe of Marketing'. *Journal of the Academy of Marketing Science*, 30(4): 333-347.
- Weiser, M. 1991. 'The Computer for the 21st Century'. *Copyright by Scientific American, Pervasive Computing* (2002): 19-25.
- Weiser, M. 1993. 'Hot Topics- Ubiquitous Computing'. *Computers*, 26(10): 71-72.
- Weiss, A. 2003. 'Me and My Shadow'. *Networker*, Sept 2003, 7(3): 25-30.
- Westin, A. 1967. 'Privacy and Freedom'. Ateneum, New York.
- Young, J.B.1979. 'Privacy'. *John Wiley & Sons Ltd*.