CONTRASTING EXPERT ASSESSMENT OF PRIVACY WITH PERCEIVED PRIVACY: IMPLICATIONS FOR PUBLIC POLICY

Ramnath K. Chellappa

ebizlab
BRI 401G, Dept. of Information and Operations Management
Marshall School of Business
University of Southern California, Los Angeles, CA 90089

ram@marshall.usc.edu
213-740-3920
http://ebizlab.usc.edu

Abstract

The increasing use of the Internet as medium for personal, business and government transactions has ignited the debate on standards and safeguards for protecting privacy of parties involved in the transaction. Since 1995, the government has taken an active role in the form of the Federal Trade Commission's (FTC) involvement. An expert assessment of issues surrounding privacy on the Internet has helped the FTC to develop a set of five core principles to safeguard consumer's privacy in online transactions. This research argues that while scientific assessment of privacy issues and the resulting recommendations may serve to allay liability concerns of vendors online, it has limited effects on consumer perceptions of privacy. We examine the factors that firms employ to ensure privacy such as alliances with trusted third parties, policy disclosures, etc. and find that while these factors do indeed affect a consumer's perception of privacy, their role is significantly moderated by their understanding of technology and influenced by the online vendor's reputation. Theories from risk management are used to argue that currently there exists a risk communication vacuum between expert assessment of privacy and consumer perceptions thereof. The implication of this work for public policy points toward the need for government and non-profit organizations to bridge this gap through public education initiatives.

1. Introduction

The privacy of an individual and her concerns thereof is not a new phenomenon. Individuals have always been concerned about what and how much others know about them. Similarly in commercial transactions, consumers have always been concerned about using debit cards at not so reputable merchants and have often had their privacy invaded in the form of direct marketers who somehow obtained their telephone number. However, what has changed with the advent of the electronic medium is that the scale and scope of privacy concerns has compounded many folds. Online merchants, government institutions and others with whom the public conducts its transactions, have invested millions of dollars in a plethora of security technologies and privacy mechanisms, (Lemos 2001) in the hope that their consumers will become comfortable in

conducting a transaction and parting with their private information. Many researchers have pointed out that enhancing favorable security and privacy perceptions (Friedman, et al. 2000, Shneiderman 2000), and building trust (Hoffman, et al. 1999, Keen 2000) are very important for sustained activity in the electronic frontier. These investments have primarily been in the form of technologies that aim to safeguard information and in creating alliances with third parties such as TRUSTe (http://www.truste.org) that specialize in enforcing privacy safeguards.

In this research, I examine the effectiveness of these investments from a public policy perspective. First, I analyze evidence and theories from prior research that have helped formulate ideas for protecting privacy. Second, I propose that while these solutions maybe effective in protecting businesses from liability issues, they are not as effective in alleviating consumer concerns of privacy. This research argues that this difference between legal definitions of safeguarding privacy and perceptions of privacy in the online environment is essentially a function of public unawareness and unfamiliarity with the electronic medium. I employ theories from risk management to show that this gap is analogous to a risk communication vacuum seen in many other situations where governmental organizations are involved in ensuring public welfare. Based on this research I propose an active role for governmental and non-profit institutions in educating the public on the nature of electronic transactions.

2. Privacy – Real and Perceived

Privacy has always been important to individuals. It has been argued to help maintain status divisions and to help sustain individual needs in structured groups (Schwartz 1968). Schwartz has also argued that privacy is an object of exchange meaning it can be ensured for a certain price and others have proposed that it has always been a luxury (McGinley 1959). In fact the ability to invade someone's privacy can even be construed to be a sign of superior status in earlier societies (Goffman 1958). So clearly it can be argued that different classes of people have different expectations of privacy and its definition may further depend on the nature and type of situation. What an individual discusses with his doctor may not be what she discusses with her insurance agent. This could be attributed to negative repercussions or even a fear of non-conformance to existing group structure and behavior. It has been recognized quite early that any assurances of privacy are very important for social orders to function. Schwartz observes that,

> *"Guarantees of privacy, that is, rules as to who may and who may not observe or reveal information about whom, must be established in any stable social system."*

It can only be gleaned from these early arguments that there is no such thing as absolute privacy in a social order, it is obviously contextual and can be defined to be dependent on the parties involved in the exchange of information and the domain where the transaction takes place. In this research we are interested in the context of electronic transactions, particularly those that use the Internet as the infrastructure. The issue of privacy concerns in this domain has primarily stemmed from the growth of electronic commerce and the resulting business transactions. This can be construed as a social order involving a customer and merchant and while the consumer has no concern in sharing information with the merchant, she maybe concerned by other factors such as who else has the ability to view the transaction and what are the subsequent and future uses of the information. From a commercial transaction point of view, privacy of individuals has been defined as an "assessment that their personal information will subsequently be used fairly and they will not suffer negative consequences" (Culnan and

Armstrong 1999, Smith, et al. 1996). Other definitions also exist, such as "the ability of individuals to personally control information about one's self" (Stone, et al. 1983) and the very early "people's ability to control the terms under which their personal information is acquired and used" (Westin 1967). Privacy has also been discussed in much detail from an individual's viewpoint and as a part of organizational practices (Culnan 2000, Culnan and Armstrong 1999, Culnan 1995, Smith, et al. 1996). In essence, from a legal perspective privacy may even be considered as a distinct consumer right (Godwin 1991).

The question therefore is if the consumer understands this right, i.e., 1. If she knows that she has this right, 2. If she knows that there is a risk to this right in the online world, 3. If she can identify the factors that create this risk, and, 4. If she understands the protective/remedial measures offered by the vendors? For continued use of the Internet for personal, business and governmental purposes it is important that all of the above elements are satisfied. We argue that the adoption of the electronic medium is not only threatened by unethical vendors violating the guarantee of privacy, but also because consumers are unclear about the nature of the risks that exist. And hence any protection measure may remain ineffective unless we understand consumer perceptions of privacy. Although studies have been conducted to study consumer willingness to provide information (Phelps, et al. 2000), presence of online disclosure statements (Miyazaki and Fernandez 2000) and other issues related to use of cookies, third party advertisements, etc., few have addressed the effectiveness of all the prescribed measures for safeguarding privacy. In fact, one of the studies (Miyazaki and Fernandez 2000) finds no relationship between online privacy and security statements and perceptions of risk.

2.1 Expert Assessment of Risk to Privacy and Recommendations

A review of the recommendations and common practices is in order before any attempt is made to understand their ineffectiveness in allaying consumer perceptions. Since 1995, the Federal Trade Commission has served as the leading governmental body in setting online privacy standards. Based on various research (Culnan 2000) and expert recommendations, the FTC (FTC 1998a, FTC 1998b, FTC 2000a, FTC 2000b) has suggested a set of fair information practices that recommend a firm to provide the following to a consumer:

1. Notice regarding the firm's collection of information and usage
2. Choice regarding subsequent usage that is different from the original intent,
3. Access to review and contest the collected information,
4. Security/integrity through reasonable steps and
5. Ability to enforce/redress the above practices and provide sanctions for any non-compliance.

Typically the above practices are implemented by Web sites in two visible ways.

1. *Policy statement:* Typically a Web site will present a policy statement that indicates how it follows the fair information practices. A Web site that adheres fully to the above practices will indicate what information it collects, how it collects them (usage of cookies), names of other third parties that place cookies (advertisers, partners, etc.) and how it uses the information. Further it will offer the consumer the choice through opt-in/opt-out mechanism regarding usage and collection.
2. *Privacy Seal:* Another manner in which a site signals its conformance with the fair information practices is through a seal on its home page indicating it is affiliated with a third party such as TRUSTe, CPA WebTrust, BBBOnline

Privacy, etc. This implies that the third party has verified that the Web site collects and uses information in accordance to the FTC guidelines in addition to any other vendor specific requirements.

In fact a recently released FTC survey of popular and random Web sites (FTC 2000b), finds that over 95% display some sort of a privacy policy satisfying the above principles to varying degrees. Further 36% of the Web sites are also found to display a privacy seal indicating an alliance with one of the third party firms. Clearly if such a large number of Web sites conform to the set guidelines, it should indicate a greater consumer confidence in the online environment. However among others, a recent report from the Center for Communication Policy at UCLA, funded by the National Science Foundation (UCLA 2000) states that

> *"strong agreement among both Internet users and non-users who perceive that using the Internet creates risks to the preservation of individual privacy. When asked if "people who go online put their privacy at risk," almost two-thirds (63.6%) of Internet users and more than three-quarters (76.1%) of non-users either agree or strongly agree with that statement. Only 11.7% of Internet users and 13.1% of non-users disagree or strongly disagree that people put their privacy at risk on the Internet."*

Clearly this implies that there is a dichotomy in terms of what online etailers do to ensure privacy and how consumers perceive these measures. In order to explore the nature of this dichotomy, recent research (Pavlou and Chellappa 2001) has introduced the concept of *perceived privacy* which is defined as "the subjective probability with which consumers believe that the collection and subsequent access and usage of their private information is consistent with their expectations as set by known legal guidelines." Chellappa et al. (2000), point out that consumer trust in the ability of the Internet to act, as the business infrastructure is dependent upon perceived security and perceived privacy and that perceived security may be related to perceived privacy since privacy involves both protection (that is influenced by security) and assurance about usage.

The goals of the current article is to identify a paradigm to understand this ineffectiveness of current safeguards in allaying consumer concerns and explain the difference between expert assessment of risk to privacy and the construct of perceived privacy.

2.2 A Risk Analysis Approach to Understanding Online Privacy

Risk has been defined as a combination of something that is undesirable and uncertain and more formally (Covello and Merkhofer 1994), "the possibility of an adverse outcome, and uncertainty over the occurrence, timing or magnitude of that adverse outcome." In the domain of public policy, the U.S. National Academy of Sciences formalized (Powell 1998) risk analysis through its National Research Council in a publication called the "The Red Book." This model clearly distinguishes between three stages of risk analysis, namely risk assessment, risk management and risk communication. In the context of online privacy and public perceptions, risk communication is of particular interest. Risk communication has been defined (Powell 1998) as "the science of understanding scientific and technological risk and how it is communicated within a socio-political structure." It has been in existence from the days of nuclear power concerns in the 1970's to recent food related risks such as E-Coli outbreaks. An important element of risk is the fact that experts define risks in the language of science and it is often mired quantitative and probabilistic terms (Groth 1991, Pollak 1996, Sandman 1987) that is

often indiscernible to the common public. Powell and Leiss (1997) make the argument that while experts use scientific and statistical language, the common public uses an intuitively grounded one, i.e., population averages of experts matter little to the public which values personal consequences. They further refer to the emergence of a risk information vacuum between scientific assessment and public perception of risk, particularly when the fundamental assumptions are grounded differently for the two parties. Communication of privacy risks apparently suffers from the same problem. While researchers and the government have evaluated the causes of risk and come up with recommendations, it is apparent that the average public does not understand the causes of these risks and hence the recommendations. If new guidelines are proposed for the online medium, the public must first be made aware of the nature of this medium before they could understand the recommendations. This is especially true in case of risks created by technological changes. The information vacuum can be a cause for further concern since vacuums hardly remain as such for long periods. It has been known to be filled by information from other sources some of which may be from intuitive explanations, albeit incorrect, and some possibly even from vested sources (Powell 1998).

Online vendors do not fall in the category of the public. In fact they may be considered to be part of the expert population, although biased towards their own profit maximization objectives. Thus the fact that there is great vendor compliance with FTC guidelines can be explained by the market mechanisms at work. The element of privacy online can be argued to have two opposing dimensions, the first being the contextual sensitivity of information from the consumer perspective and the other being the contextual liability for the vendor. Interestingly, these two dimensions co-exist very well due to the fact that both parties benefit from the exchange of information. Consumers online, greatly value personalization of products and services. However in order for a vendor to personalize, they need to provide personal information. Vendors online also benefit from collecting this information as it could generate advertising revenues, allow them to tailor their inventory, etc. Thus there is a equilibrium (Chellappa and Sin 2001), in the online world as a result of a utility maximization behavior exhibited by both parties. Consumers make implicit assumptions about privacy risk when making product-purchasing decisions, and are therefore influenced by exogenous factors such as reputation of the stores, prior experience, satisfaction etc. However, ideally these perceptions should be due to their awareness or knowledge of how the online world functions. This argument can also be inferred from earlier research on perceived privacy that showed a weak albeit significant correlation with prior experience and a strong relationship with reputation (Pavlou and Chellappa 2001). This explains the fact that when controlled for reputation and satisfaction, disclosure statements and privacy seals can contribute towards enhancing perceptions of privacy but in ungrounded surveys (i.e., surveys not connected to specific stores/transactions) consumers exhibit great concern. The online merchant is not particularly concerned about privacy, however he is clearly concerned about his liability and legal responsibility and therefore compliance with recommendations of a body such as FTC clearly serves to enhance his legal position. And hence the relatively quick and easy adoption of the recommendations can be observed at the business end, while they still fail to allay consumer concerns.

3. Implications for Public Policy and Conclusions

The existence of risk to privacy of individuals and their transactions in the online world is real. It is also important to encourage expert assessment of these risks in order to obtain reasonable remedial measures. However an expert analysis of risk alone is

insufficient to understand consumer perceptions of privacy and therefore a study of the effectiveness of the measures suggested by the experts is warranted. The consumer perceptions of risk can be studied in two ways. From a market perspective, it can be shown that consumers may implicitly include reputation and past experiences with stores in order to evaluate their privacy risk. The implication of this argument being that some stores may fare better than others due to their reputation even if they do not take explicit measures to protect consumer privacy. The message to businesses online is therefore to invest in reputation enhancing activities.

On the other hand, the risk analysis view provides greater clarity on the role of government initiated safeguards. This view suggests that consumers are not knowledgeable about the Internet and therefore do not understand the safeguards set by FTC even though most online vendors employ them. This paradigm helps explain the fact the vendors adopt these guidelines not due to their concern for consumer privacy but rather to allay liability concerns. Further this also implies that the measures themselves may not be ineffective but rather their role has not been clearly communicated to the public. Therefore the most significant implication of this paradigm to public policy is the need to educate the average public. In concurrence with other risk communication views, this article also advocates the use of the media in making the consumer aware. Further it also re-iterates the importance of regulators and other non-profit groups in constructing effective safeguards. It is also very important to incentivize the online industry to assume a greater portion of the risk communication responsibility.

4. References

Chellappa, Ramnath K. and Raymond Sin, "Personalization versus Privacy: The Flip Sides of the Same Coin," *Working Paper*, ebizlab, Marshall School of Business, USC (2001), Los Angeles.

Covello, V.T. and M.W. Merkhofer, *Risk Assessment Methods*, Plenum Press, New York, 1994.

Culnan, Mary J, "Protecting privacy online: Is self-regulation working?," *Journal of Public Policy & Marketing*, 19, 1 (2000), 20-26.

Culnan, Mary J and Pamela K Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, 10, 1 (1999), 104-115.

Culnan, Mary J., "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing*, 9, 2 (1995), 10-19.

Friedman, B., P. H. Kahn and D.C. Howe, "Trust Online," *Communications of the ACM*, 43, 12 (2000), 34-40.

FTC, (Federal Trade Commission), "Consumer Privacy on the World Wide Web," Statement Presented to the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Committee on Commerce U.S. House of Representatives, July 21 1998a.

FTC, (Federal Trade Commission), "Fraud Could Slow Growth of Electronic Commerce," FTC Press Release FTC File No. P97-4406, Federal Trade Commission, June 25 1998b.

FTC, (Federal Trade Commission), "Online Privacy Cases," 2001, (- 2000a), -.

FTC, (Federal Trade Commission), "Privacy Online: Fair Information Practices in the Electronic Marketplace," Washington DC, (2000b), -.

Godwin, Cathy, "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing*, 10, 1 (1991), 149-166.

Goffman, Erving, *The Presentation of Self in Everyday Life*, University of Edinburgh, Edinburgh, 1958.

Groth, E., "Communicating with consumers about food safety and risk issues," *Food and Technology*, 455, (1991), 248-253.

Hoffman, Donna L, Thomas P Novak and Marcos Peralta, "Building consumer trust online," *Association for Computing Machinery. Communications of the ACM*, 42, 4 (1999), 80-85.

Keen, P. G. W., "Ensuring E-trust," *Computerworld*, 34, (March 13 2000), 46.

Lemos, Robert, "Egghead hack costs millions: Companies paid big bucks to reissue credit cards," 2001), -.

McGinley, Phyllis, "A Lost Privilege," In *Province of the Heart*, Viking Press, New York, 1959, 56.

Miyazaki, A. D. and A. Fernandez, "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing*, 19, 1 (2000), 54-61.

Pavlou, Paul A. and Ramnath K. Chellappa, "The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transactions," *Working Paper*, ebizlab, Marshall School of Business, USC (2001), Los Angeles.

Phelps, Joseph, Glen Nowak and Elizabeth Ferrell, "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing*, 19, 1 (2000), 27-41.

Pollak, R.A. . . . 545: 25-34., "Government risk regulation," *Annals of American Academy of Political and Social Science*, 545, (1996), 25-34.

Powell, D.A., "Risk Assessment," Spokane, WA, (1998),
Sandman, P.M., "Risk communication: facing public outrage," *EPA Journal*, 13, (1987), 21.

Schwartz, Barry, "The Social Psychology of Privacy," *American Journal of Sociology*, 73, 6 (1968), 741-752.

Shneiderman, Ben, "Designing Trust Into Online Experiences," *Communications of the ACM*, 43, 12 (2000), 34-40.

Smith, Jeff H., Sandra J. Milberg and Sandrea J. Burke, "Information Privacy: Measuring Individuals' Concerns About Corporate Practices," *MIS Quarterly*, 20, 2 (1996), 167-196.

Stone, E. F., D. G. Gardner, H.G. Gueutal and s. McCLure, "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology*, 68, 3 (1983), 459-468.

UCLA, Center for Communication Policy, "The UCLA Internet Report - Surveying the Digital Future," UCLA, 2000.

Westin, A. F., *Privacy and Freedom*, New York:NY, 1967.