# An Investigation of Privacy Tradeoff on the Internet

**By**

**Fei Lee**

Prepared for BADM 590

Trustworthy Computing: Information Security and Management

Professor Michael Shaw

May 2006

The University of Illinois at Urbana-Champaign

**Abstract:**

Privacy on the Internet may be considered as an economic tradeoff. Online consumers are willing to tradeoff private personal information with benefits or rewards such as a personalization user interface and product discounts. Organizations are willing to risk their reputations in order to collect as much customer information as possible. However, little is known regarding how to strike a balance between the tradeoffs that could satisfy both consumers and online firms. This paper aims to examine the relationship between online privacy, trust, and firms' reputation. We propose that consumers' trust towards online firms is associated with firms' self-regulated privacy policies. In addition, online firms' reputation can be enhanced if firms offer privacy awareness information or technical support regarding privacy concerns on their websites.

## Introduction

Privacy is an economic problem and often is associated with an economic tradeoff. From an individual's perspective, people want to share enough information to have a more customized and personalized online shopping experience but at the same time, they are reluctant to share too much personal information to other parties due to privacy concerns. More and more customers are aware of the fact that online firms have monitored and collected information regarding their purchases and other activities conducted on the Internet. "The main danger to privacy for people who live in free democratic societies comes from the private sector, not the government; Big Bucks, not Big Brother" (Etzioni, 2000, p. 91). In 2001, the U.S. Federal Trade Commission (FTC), being pressured by consumer-protection organizations, held a conference to examine how companies exchange personal data and create profiles of consumers. The FTC conducted its own survey and the results indicate that 92% of respondents do not trust online firms to keep their personal information confidential, and 82% agreed that the government should take actions by regulating how online firms use consumers' personal information (Thibodeau, 2001).

From an organization's perspective, firms want to collect as much information as possible about their customers but they do not want to put their firms' reputation at risk by violating any privacy regulation. Another survey conducted by the Federal Trade Commission shows that 99% of online firms collect personal information from customers visiting their websites--a practice that is integral to many enterprises but largely invisible to their consumers (Seligman and Taylor, 2000). Firms claim that detailed consumer

profiles can be used not only to establish relationships with consumers but also to reduce corporate costs by allowing firms to target their marketing campaigns more effectively and efficiently. In addition, consumers' previous purchasing histories can be used to predict their future purchasing patterns since past behavior is viewed as the strongest indictor of future behavior (Thibodeau, 2001). However, consumers' personal information (i.e., purchasing history, income and education level, size of family, or lifestyle interests) can also be used as a customer-tailored-made price strategy allowing online retailers to increase profits by charging different prices to different customers. The strategy was unknown to many consumers until Amazon's Internet privacy scandal exploded in 2000.

**Amazon Case of Privacy Intrusion**

In September 2000, Amazon randomly offered a 30%, 35%, or 40% discount for the same DVD movie to different consumers based on their previous buying histories. When the public found out what they had really done, consumers who had received comparatively smaller discounts were outraged by the company's action. To make things worse, some customers who had bought the limited-edition copy of the "Men in Black" DVD movie also noticed that Amazon charged different prices on the DVD movie depending on customers previous shopping patterns (new customers versus repeat customers); the types of web browsers used (e.g., Netscape versus Microsoft's Internet Explore), and the brands of Internet Service Provider (ISP) subscribed (e.g., different ISP addresses). Amazon finally claimed that the whole scenario was only a 'random' price test to study how different prices affect sales and insisted that buyers' demographic

information was never used in the test. After receiving an enormous number of complaints, the Seattle-based company finally canceled its price testing policy and refunded approximately $3.10 each to about 7000 customers (Baker, Marn, and Zawada, 2001; Melillo, 2000; Rosencrance, 2000).

In the same September 2000, Amazon changed its Internet privacy policy (i.e., information sharing practices) to acknowledge to the general public that its customer data will be considered a marketable asset if the online firm is ever acquired, or sells off operations. In its original online privacy policy, Amazon claimed that it did not sell, trade, or share consumers' personal information to outside parties, but it reserved the right to do so in the future. The revised policy justified the claim that Amazon considers customer information as one of the transferred business assets during the firm's selling or buying stores or assets processes. Amazon then admitted that it does exchange data with other parties in instances where it is seeking "fraud protection and credit risk reduction". Amazon's revised privacy policy has raised serious concerns from privacy advocates who later filed a petition requesting the Federal Trade Commission to investigate whether Amazon deceived its consumers about privacy and the circumstances under which it might disclose consumers' personal information. Even though the FTC staff concluded that Amazon's revised privacy policy does not materially conflict with representations Amazon made in earlier renditions of its privacy policy, Amazon's action might seriously jeopardize the trust between buyer-seller relationships (Jones, 2001).

Consumers are increasingly raising their concerns for the privacy and security of electronic commerce (e-commerce) transactions (e.g., FTC 1998; Gilbert, 2001). Consequently, the general public is asking for increased regulations to protect personal privacy, while enterprises have countered by proposing self-regulatory guidelines or a single national standard that would preclude individual states from setting more stringent requirements (Thibodeau, 2001). The fundamental question remains unanswered: "is there any combination of economic incentives and technological solutions to privacy issues that would satisfy the interests of both consumers and enterprises?"

## Online Privacy, Security, and Trust

Numerous issues regarding security and privacy intrusion have made many consumers hesitate to perform any kind of transaction online because of uncertainty about retailer behavior or the perceived risk of having their personal information stolen by hackers (e.g., Meeks, 2000; McKnight, Choudhury, and Kacmar, 2002). Therefore, trust plays a critical role in helping consumers overcome perceptions of risk and insecurity. *BusinessWeek*'s (2000) survey shows that 61% of the respondents would consider conducting transactions on the Internet only if the security and privacy of their personal information could be adequately protected. In addition, researchers indicate that enhancing favorable security and privacy perceptions (e.g., Friedman et al., 2000; Shneiderman, 2000) and building trust (Hoffman and Novak, 1996; Keen, 2000) are essential for sustained activities in the electronic business environment. Marketing literature has long recognized that consumer trust in the transacting vendor is the most importance factor for the consumer to accept the risk of transaction, financial or otherwise and the vendor's reputation and branding are known determinants of this trust (Doney and Cannon, 1997; Ganesan, 1994). Trust is

further defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” and can be conceptualized as three-dimensional: ability, benevolence, and integrity (Mayer, Davis, and Schoorman, 1995, p.712).

From an information system research perspective, the trust construct has been studied in the e-commerce context, but primarily from the perception of trust in the transacting online store (Jarvenpaa, et al., 1999; Jarvenpaa, et al., 2000). Recently, McKnight et al.’s (2002) study suggests that trust in Internet shopping may indeed be affected by infrastructural contextual factors such as security and privacy. Chellappa (2002) examined whether information technology characteristics themselves contribute to the variability of overall consumer trust in a transaction. The empirical findings show that consumers’ perception of privacy and security, in addition to known factors of trust such as online retailers’ reputation, influence their trust in e-commerce transactions. In particular, the author proposed that perceived privacy and perceived security are antecedents of trust developed due to the nature of the institutional infrastructure such as the Internet.

Chellappa’s (2002) survey results also show that consumers report differences in their perceptions of privacy, security and trust between online and offline transactions even if the transactions involve the same store. While perceived security directly acts upon trust in e-commerce transactions, perceived privacy’s effect on trust is mediated by perceived

security. The study suggests that online firms should engage in efforts to positively influence consumer perceptions of privacy and security that inevitably affects firms' trust and reputation. To better understand consumers' future purchase preferences, firms need to obtain "consumers' permission" to collect and use personal information. If consumers perceive the sharing of this information to be not so secure or private, they are unlikely to allow the acquisition and use of their personal information. Consequently, low perceptions of privacy and security will lead to low perception of trust and jeopardize firms' reputation in the long run.

**Perceptions of Trust and Online Privacy**

The Pew Internet & American Life Project (Fox, 2000) surveyed more than 2000 Internet users in the United States about their perceptions of trust and online privacy. The results show that Internet users view online firms monitoring their web activities as privacy intrusion. However, most of the users do not use available privacy-protection tools since they do not know how firms' websites operate (i.e., most online users do not know that they are being tracked) and how existing privacy-protection tools can be deployed to protect their online privacy. For example, it is fairly common for online firms to use "cookie" to track consumers' online browsing activities. Surprisingly, even though American Internet users have high concerns about being monitored online, only 10% of the respondents reported that they have set their browsers to reject cookies.

The majority of American Internet users (84%) worry about the things that could happen online and the way in which data about them might be gathered and used. They are

concerned about commercial firms or strangers getting personal information about themselves or their families. A two-thirds majority (64%) reported that they were willing to share personal information only if they could choose when and where to give that information. For example, 27% of the respondents consider Internet tracking activity is helpful because it allows websites to tailor information for individual users. However, they do not think firms should track their online behavior without first asking users' permission. In addition, 94% of Internet users want privacy violators to be disciplined. Online users think that firms should be fined or punished if they violate their stated privacy policy and use personal information in ways that they promised they would not do so (Fox, 2000).

The survey results raise an interesting issue regarding economic tradeoff of privacy. Even though individuals' concerns about online privacy indicate that they do not want to share too much personal information with third parties, nevertheless, they are willing to trade-off the privacy for convenience, or bargain the release of personal information in exchange for small rewards (i.e., personalized and customized user interface) (Acquisti, 2004). Such tradeoffs will exist only if consumers have a certain level of trust in a firm in that they believe the firm would (1) ask for permission before sharing personal information with third parties and (2) not violate the privacy policy that the firm has published. In other words, firms' trustworthiness is of utmost important for consumers to decide as to whether share their personal information or not. Therefore,

*Preliminary Proposition 1: Consumers' trust towards online firms will increase if firms provide a privacy guarantee regarding their use of personal information data.*

## Privacy Attitudes and Privacy Behavior

Given that a large number of articles report on online privacy concerns, an unanswered question why do most consumers still take no aggressive action to protect their online privacy? The Harris Interactive (2001) conducted a survey to examine consumers' attitudes, behaviors, experiences and expectations regarding online and offline privacy. The results, consistent with The Pew Internet & American Life Project's (Fox, 2000) survey results, show that Internet users often are unaware of privacy-protection tools that are available on the Internet. Online users choose to rely primarily on their personal judgment as the driving force in protecting their privacy since they believe that they do not have enough resources or control over how to fully protect their personal information. Even though most Internet users realize that both businesses and government are also responsible for Internet privacy protection, they still have doubts about the ability of businesses and government to set and implement proper policies or regulations related to the collection and use of personal information. In other words, they do not fully trust that businesses and government can provide a reasonable level of privacy protection.

### Optimism Bias towards Privacy Intrusions

Internet users do recognize the value of personalization and customization to a modest degree. Fifty-nine percent of survey respondents reported that they are willing to exchange some of their personal information for improved services, such as product discounts and complementary products and services. Most online users (69%) who have

provided personal information over the Internet are confident in the transmission and storage of their information (Harris Interactive, 2001). The Pew Internet & American Life Project's survey in 2000 has shown similar results regarding consumers' attitudes towards online privacy. Internet users express certain levels of fears about a number of problems they might face online. They report, however, that the actual incidence of online problems is not very substantial. Surprisingly, despite those fears, online consumers behave in a fairly trusting way. Internet users are taking advantage of online services so as to simplify their lives, despite their serious concerns about Internet privacy and security risks. For example, 22% of Internet users have entrusted their personal calendar or address book to a website service (Fox, 2000). Researchers suggest that such dilemma is due to consumers' optimism bias that one's risks are lower than those of other individuals under similar situations. The optimism bias might lead consumers to believe that they will not be the ones who experience privacy intrusions (Acquisti, 2004; Weinstein, 1989).

Slovic (2000) suggests that individuals often have difficulties handling cumulative risks. For example, young smokers acknowledge the long term risks of smoking but fail to realize the cumulative effect of low risks in each additional cigarette that will eventually accumulate to a serious harm. Individuals' difficulties in dealing with cumulative risks can also apply to privacy concerns. For example, consumers might perceive as low risk by releasing a small amount of personal information over the Internet. However, they often fail to realize that the released personal information can remain available online over long periods of time. The potential privacy risk becomes serious when each small

amount of personal information data is being accumulated into a larger set of data in the future. Jehiel and Lilico (2002) indicate that it is comparatively easier for people, given their limited foresight perspective, to focus actions and effects in the short time periods. As the foresight changes, people's behaviors change even when preferences remain the same. Therefore, online consumers might want to protect their Internet privacy, but they will not actually take actions because of optimism bias. The cost of privacy protection (i.e., purchasing privacy-protection software) may be fairly instant, but the actual rewards are sometimes invisible (absence of privacy intrusions) and spread over long periods of time (Acquisti, 2004).

The optimism bias might mislead consumers to take no actual action against Internet privacy intrusion but could not ease their wariness about privacy. The Internet privacy concerns (i.e., not sure how firms process personal information) will have a stronger effect on new Internet users than on veteran users. New users are more wary and less friendly online than veteran users. This wariness is reflected in the fact that Internet newcomers are also less likely to purchase products or services online (Fox, 2000). In the long run, privacy concerns could seriously hamper online firms' profits and jeopardize e-commerce potential. Therefore, firms should not avoid the issues of privacy raised by the general public. On the other hand, there might be a positive impact on firms' reputation if online firms (1) provide more information about long term privacy risks or (2) offer a free/lower cost of privacy-protection software on their own websites.

*Preliminary Proposition 2: Online firms' reputation will be enhanced if firms voluntarily offer complete information or technical support regarding privacy concerns, on their websites.*

## Conclusions

The enhancement of efficiency and effectiveness drives the whole world towards embracing information technology (Oliner and Sichel, 2002). Researchers have recognized that the Internet has fundamentally changed the way people live their lives (Howard, Raine, and Jones, 2001) and electronic commerce has impacted the overall economy (Willis, 2004). However, the advent of e-commerce has amplified public concern about Internet privacy and security. Internet consumers are increasingly aware of firms tracking and monitoring consumer-online activities. Cookies are bits of encrypted information deposited on a computer's hard drive after the computer has accessed a specific website. The website then stores these bits of information so when the same site is accessed again by that same computer, the website can recognize the particular computer and provide the same layout, shopping cart, search information, or user's name with the exact personalization and customization each time the site is visited (Fox, 2000).

The stored information could benefit consumers by more precisely targeting their needs (i.e., preferred product information or discount) but also could be used to their disadvantage. Amazon.com has been criticized for using a customer-tailored-made pricing strategy (i.e., charge different customers different price for the sales of a same DVD) based on customers' previous shopping information and other customer demographics. In addition, Amazon enraged many Internet users by revising its Internet

privacy policy and admitting that it does exchange its customers' personal information data with other parties. Amazon's privacy scandal places a serious doubt on buyer-seller relationship in terms of trust.

Previous research suggests that online consumers' perceived privacy and perceived security influence their overall trust towards online firms. Empirical evidence also shows that consumers are willing to tradeoff their privacy for additional online benefits (i.e., personalized user interface or product discount) only if firms promise the proper use of the personal information. Therefore, firms' trustworthiness is the crucial determinant factor for consumers to decide whether to share their personal information or not. We further propose that consumers' trust towards online firms will increase if firms provide a privacy guarantee regarding their later use of personal information data (Preliminary proposition 1).

Privacy concerns can potentially hamper the growth of e-commerce. "American consumers currently have high levels of concern about online privacy and a corresponding reluctance to shop online. A lack of consumer trust in the Internet is significant. Industry newsletter Privacy & American Business found that 61% of U.S. Internet users have at some time refused to purchase a product online because of privacy concerns" (U.S. Public Interest Research Group, 2000, p.2). In the long run, consumers might revert to traditional brick-and-mortar shopping behaviors if they do not have enough resources or control over privacy protection. As such, the full potential of e-commerce may never be realized.

Lack of information regarding privacy protection or being unaware of available privacy-protection technology might mislead consumers to think that they will not be the victims of privacy intrusions (Acquisti, 2004; Weinstein, 1989). Therefore, online consumers might take no actual action against Internet privacy intrusion even though they realize the importance and value of privacy protection. Consumers might still complain about online privacy risks and such wariness would affect new Internet users regarding their attitudes towards online transaction activities. Empirical evidence shows that Internet newcomers are less likely to purchase products or services online (Fox, 2000). Consequently, privacy concerns could seriously hamper online firms' profits and delay e-commerce development. Thus, we suggest that online firms should not only encourage their consumers to learn more about online privacy issues but also offer actual assistance to their customers to protect against Internet privacy intrusions. We propose that online firms' reputation will be enhanced if these firms voluntarily offer complete information or technical support regarding privacy concerns on their websites (Preliminary Proposition 2).

In conclusion, individual users, online firms, and the government are all responsible for privacy protection and have to work hand-in-hand with each other. It is an inseparable relationship that if one party falls short, the other members of this triad fall with it. Online users do care about Internet privacy but they simply do not trust the abilities of online firms and government in putting sufficient effort to protect their personal information data. Technology alone (i.e., privacy-protection software) or privacy awareness (i.e., privacy-related information) alone might not address the core of privacy problem. On the

other hand, a combination of both and the genuine efforts from online firms and government will help and keep consumers “stay online”.

## References:


1. Acquisti, A. (2004), "Privacy in Electronic Commerce and the Economics of Immediate Gratification," In proceedings of the 5th ACM conference on Electronic Commerce, 21-29.
2. Baker, W., Marn, M., and Zawada, C. (2001), "Price Smarter on the Net," *Harvard Business Review*, 79(2), 122-27.
3. BusinessWeek (2000), "Business Week/Harris Poll: A Growing Threat," *Business Week*, 96.
4. Chellappa, R.K. (2002), "Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security," < http://asura.usc.edu/~ram/rcf-papers/sec-priv.pdf>
5. Doney, P.M. and Cannon, J.P. (1997), "An Examination of the Nature of Trust in Buyer-Seller Relationships," *Journal of Marketing*, 61, 35-51.
6. Etzioni, A. (2000), "The New Enemy of Privacy: Big Bucks," *Challenge*, 43(3), 91-106.
7. Federal Trade Commission. (1998), "Consumer Privacy on the World Wide Web," <http://www.ftc.gov/os/1998/07/privac98.htm>
8. Friedman, B., Kahn, P.H. and Howe, D.C. (2000) "Trust Online," *Communications of the ACM*, 43(12), 34-40.
9. Ganesan, S. (1994), "Determinants of Long-Term Orientation in Buyer-Seller Relationships," *Journal of Marketing*, 58, 1-19.
10. Gilbert, J. (2001), "Privacy? Who Needs Privacy?" *Business 2.0*, 42.

11. Howard, P., Raine, L. and Jones, S. (2001) Days and Nights on the Internet: The Impact of a Diffusing Technology, *The American Behavioral Scientist*, 45, 3, 383-407.
12. Hoffman, D.L. and Novak, T.P. (1996), "Marketing in Computer-Mediated Environments: Conceptual Foundations," *Journal of Marketing*, 60, 50-68.
13. Jarvenpaa, S.L., Tractinsky, N., Saarinen, L. and Vitale, M. (1999) "Consumer Trust in an Internet Store: A Cross-cultural Validation," *Journal of Computer Mediated Communication*, 5(2).
14. Jarvenpaa, S.L., Tractinsky, N. and Vitale, M. (2000), "Consumer Trust in an Internet Store," *Information Technology and Management*, 1(12), 45-71.
15. Jehiel, P. and Lilico, A. (2002), "Smoking Today and Stopping Tomorrow: A Limited Foresight Perspective," <http://www.enpc.fr/ceras/jehiel/SmokerWEtex.pdf>
16. Jones, J. (2001), "FTC Sides with Amazon.com in Privacy Case," *InfoWorld*, <http://www.infoworld.com/articles/hn/xml/01/05/25/010525hnepic.html>
17. Keen, P., Balance, C., Chan, S. and Schrump, S. (2000), *Electronic Commerce Relationships: Trust by Design*, Prentice Hall, Englewood Cliffs, NJ.
18. Mayer, R.C., Davis, J.H., and Schoorman, F.D. (1995), "An Integrative Model of Organizational Trust," *Academy of Management Review*, 20(3), 709-34.
19. McKnight, D.H., Choudhury, V. and Kacmar, C. (2002), "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research*, 13(3), 334-359.

20. Meeks, B.N. (2000) “Is Privacy Possible in the Digital Age,” *MSNBC*, < http://www.msnbc.com/news/498514.asp>

21. Melillo, W. (2000), “Amazon Price Test Raises Net Privacy Outcry,” *Adweek*, 41(40), 8-11.

22. Oliner, S.D. and Sichel, D.E. (2002) “Information Technology and Productivity: Where Are We Now and Where Are We Going?” *Economic Review - Federal Reserve Bank of Atlanta*, 87, 3, 15-44.

23. Rosencrance, L. (2000), “Customers Balk at Variable DVD Pricing,” *Computerworld*, 34(37), 4.

24. Seligman, T.J. and Taylor, J.D. (2000), “FTC Reverses Privacy Policy,” *New York Law Journal*, Jun. 19.

25. Shneiderman, B. (2000), “Designing Trust into Online Experiences,” *Communications of the ACM*, 43(12), 34-40.

26. Slovic, P. (2000), “What Does It Means to Know a Cumulative Risk? Adolescents’ Perceptions of Short-Term and Long-Term Consequences of Smoking,” *Journal of Behavioral Decision Making*, 13, 259-266.

27. The Harris Interactive (2001), “Consumer Privacy Attitudes and Behaviors Survey,” < http://www.bbbonline.org/UnderstandingPrivacy/library/harris2-execsum.pdf>

28. Thibodeau, P. (2001), “FTC Workshop Looks at Key Data Privacy Issues,” *Computerworld*, Mar. 13.

29. Weinstein, N.D. (1989), “Optimistic Biases about Personal Risks,” *Science*, 24, 1232-1233.

30. Willis, J.L. (2004), “What Impact Will e-commerce Have on the U.S. Economy?” *Economic Review - Federal Reserve Bank of Kansas City*, 89, 2, 53-71.