2002

Protecting privacy in today's knowledge based society

Jack Cook

Kristin Kinsella

David Pang

Recommended Citation

Journal of Global Competitiveness. Protecting Privacy in Today's Knowledge Based Society, with Kristin Kinsella, David Pang, and Jennifer Reginelli, 251-259, 2002

Protecting Privacy in Today's Knowledge Based Society

Jack Cook
Kristin Kinsella
David Pang
Jennifer Reginelli

ABSTRACT

With the growing use of the Internet in everyday life, consumers are increasingly concerned about personal privacy. This paper examines issues concerning consumer privacy and provides solutions available to protect that privacy.

INTRODUCTION

Internet usage is at an all-time high. Consumers regularly provide personal information while surfing. Businesses seldom actively inform consumers how this information is used. Furthermore, web sites collect information on browsing patterns and shopping habits via cookies, and use this and other gathered information to personalize the web surfing experience. Two thirds of respondents agree or strongly agree that web sites should be allowed to analyze web site traffic on an anonymous, aggregate level (Han & Maclaurin, 2002, p. 36). Although some users are not concerned about privacy, others would prefer to remain anonymous. Oftentimes, anonymity is not an option and this greatly concerns consumers. In fact, a study showed that approximately 62 percent of Internet users have privacy concerns (Han & Maclaurin, 2002). A recent Forrester study showed that online businesses lost $15 billion last year due to consumer privacy concerns (Gaudin, 2002).

Are companies devoting adequate resources to protecting privacy? Are laws that punish those who violate someone's privacy too lax or nonexistent? Are consumers too cautious or not cautious enough? Half of online purchasers allow privacy concerns to affect their purchasing on a selective basis (Han & Maclaurin, 2002, p. 36). Merriam-Webster dictionary defines privacy as "freedom from unauthorized intrusion." In general, privacy can be defined "as people's ability to control the terms under which their personal information is acquired and used" (Culnan, 2000, p. 20). More specifically, others define an invasion of privacy as "...the unauthorized collection, disclosure, or other uses of personal information as a direct result of electronic commerce transactions" (Wang, Lee, & Wang, 2002, p. 64).

Negative publicity concerning privacy dramatically increases consumer paranoia. One of the biggest challenges is ignorance. Many consumers do not know how to protect their privacy and securely transmit information. Consumers do not realize that information theft or improper information usage is a big problem on the Internet (McGinity, 2000). Whether they understand the problems or not, oftentimes they are either unaware that solutions exists or do not understand how to implement them. This paper examines both the problems associated with privacy and potential solutions that exist. Potential solutions are assessed with respect to their feasibility and ease of use for average Internet users.

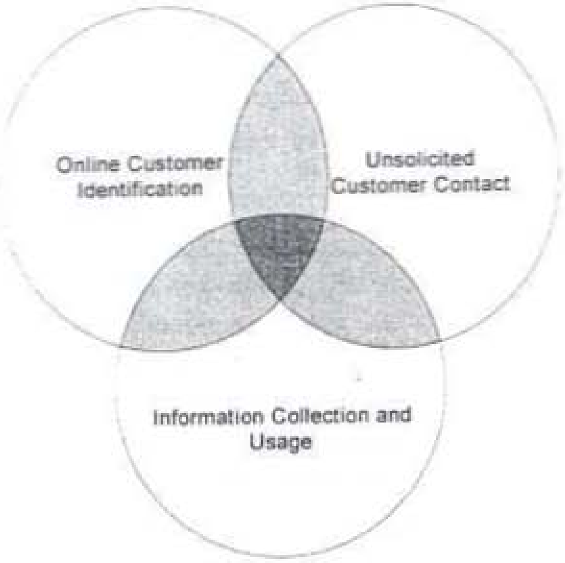
PRIVACY CONCERNS

Is it reasonable for consumers to assume that they should always have control over their personal information on the web? Some primary consumer privacy, issues online include customer identification, unsolicited consumer contact, and the distribution and sale of customer information. These three issues are interrelated, as shown in Figure 1. For example, when a web site collects information from a user, it can be used to personalize a web site (customer identification), send the user emails about related topics (unsolicited consumer contact), or be sold to third parties (information distribution and sales). Businesses must address privacy concerns if they want to successfully attract and retain customers.

Customer Identification

Customer identification can be accomplished in a variety of ways. Retailers can track visitor information using Internet cookies. Collected data from online forms can be combined with transaction records to follow users as they browse the Internet. The transaction records yield a personal profile of the user that includes personal information, online behavior, patterns of exploration, products and information looked at or bought, all of which can be used for target marketing.

FIGURE 1
The interrelationship between major consumer privacy concerns


Online Customer Identification
Unsolicited Customer Contact
Information Collection and Usage

Sometimes customers are identified through improper access, improper collection, or improper monitoring (Wang *et. al*, 2002). Improper access is the invasion of a user's computer without his/her prior consent. Improper collection occurs when a web site gathers information about a user without notifying him/her that the data is being collected. Improper monitoring conducts surveillance on a user's computer activities without his/her acknowledgement. All three fall under the category of improper acquisition (Wang *et. al*, 1998, p. 65). Table 1 describes the relationships between Internet marketing activities (rows) and privacy concerns (columns). As shown in Table 1, both preference tracking and unwanted eavesdropping fall under improper acquisition.

Unsolicited Customer Contact

Unsolicited customer contact, which is "the practice of collecting information for one purpose and then using the information to make unsolicited contacts..." (Miyazaki *et. al*, 2000, p. 56) includes the transmission of "...information to potential consumers without their acknowledgement or permission. Such privacy invasions include junk mail, mass direct email, and junk Internet push channels" (Wang *et. al*, 2002, p. 66).

TABLE 1
A Taxonomy of privacy concerns

		Improper Acquistion			Improper Use		Privacy Invasion	Improper Storage
		Improper Access	Improper Collection	Improper Monitoring	Improper Analysis	Improper Transfer	Unwanted Soliciation	
Internet Marketing Activities	Direct Mailing				P		E	
	Preference Tracking	E	E	E				
	Unwanted eavesdropping	P	E	E				
	No opting-out				E			P
	Third-party distribution				E	E		P

E: Explicit P: Probable

Why are consumers worried about unsolicited contact? The main concern is that they do not know what a company is going to do with their information. Refer to Table 1, which points out that activities such as direct mailings are considered a privacy invasion and unwanted solicitation. When a user receives unsolicited email, it is time consuming and annoying to sort through. Web sites could potentially use personal information without a user's understanding, knowledge, and consent. Consumers want control over what is done with their personal information. Most often web sites do not give users options about how their information is used. Users want notice and choice when it comes to their personal information. "Control is a key concern for consumers, who have stated that they believe that they have lost all control over what marketers do with their information" (Sheehan & Hoy, 2000, p. 69).

An example of unsolicited contact occurred with the Microsoft Media Player (New York Times, 4/2/2002). The version of Media Player released with Windows XP keeps a log of all music and movies played. The information is stored on the user's computer and then sent back to Microsoft, who uses the information to match people with their corresponding choices in entertainment, all without consumers' knowledge and permission. Furthermore, this tracking was not mentioned in the privacy statement. When the issue was publicized, Microsoft amended the privacy statement, but did not tell users how to turn off the logging.

An integral concern with unsolicited contact is that it leads to information being sold to third parties. In February 1999, the information sharing practices of financial institutions were analyzed. As a result, legislation was passed to prohibit sharing of information. Medical sites are controversial as well since the information that is shared is extremely private, but the sale of this information could be lucrative for a web site. For instance, a web site finds out that a user has a certain medical problem, and then sells that person's name and information to a company who provides a solution to that problem. The user is bombarded with emails about his/her problem, which he/she thought was private. Legislation relating to certain industries has been passed to protect consumer privacy, but it is not widely enforced online.

Information Distribution and Sales

How do companies collect personal information about consumers? Every time a consumer fills in a form on a web site, it is submitted to a database. If a user's computer stores cookies, personal information and browsing patterns could be collected. Most consumers are willing to supply online companies with information as long as they know the exact intent of the information. When consumers receive unsolicited marketing, such as emails and telemarketing phone calls, they know their privacy has been compromised, increasing their privacy concerns. In Table 1, information distribution and sales would be considered improper use and improper storage. Direct mailing, no opting-out and third-party distribution are all examples of information distribution and sales.

Disclosure is the primary privacy issue that concerns consumers. They want to know who is receiving their information and the intended use (Caudill, 2000). A classic example of this would be when credit card companies sell consumer data to marketers who use the information to determine shopping patterns (Sheehan *et. al*, 2000). Marketers and consumers both view the ownership of information differently. Consumers believe that they have absolute ownership of any information that is collected about them. Marketers, on the other hand, believe what they have collected is theirs.

POTENTIAL SOLUTIONS TO PRIVACY CONCERNS

Is security the same as privacy? No. Security is not privacy. Security is important to privacy and without it, information will not remain private. Privacy policies and practices help build consumers' trust, but without security measures to protect data, privacy violations will occur. Security is twofold. Data must be protected during transmissions, as well as once it is stored. Firewalls, passwords, and limiting access to data all enhance security and ultimately protect privacy.

Individual Countermeasures to Protect Privacy

Technology alone cannot help protect privacy; technology combined with awareness is required. One of the best ways for customers to protect themselves is to be aware of problems and existing solutions. Much of what is written or presented on privacy protection is not geared towards average consumers; so average consumers must put forth considerable effort to understand their alternatives. Technology combined with awareness goes a long way to alleviate privacy concerns. Consumers must use common sense. Consumers must ask themselves if the benefits of sharing their personal information outweigh their loss of privacy. Next technological alternatives are discussed.

Technological Solutions

Most consumers do not understand what cookies are or their capabilities. A user can set their browser preferences to identify cookies or specifically block them on certain sites, but many users do not know or understand why they would want to do that. Cookies are an easy way to keep certain information available to web sites, such as preferences or shopping cart contents, stored and accessible for the next time the user visits the site. "There is nothing inherently evil about HTTP cookies, although they can potentially be used in undesirable ways" (Cranor, 1998, p. 15). The problem arose when companies began using cookies to track information and browsing habits of users. "The current HTTP protocol provides minimal information to users, and cookie implementations in popular Web browsers don't make it easy for users to control which sites to accept cookies from" (Reagle & Cranor, 1999, p. 51). The Anonymizer is a web-based anonymity tool that channels consumer requests through an anonymous server so that Internet addresses are not revealed. A Crowd is another anonymity tool that consists of a system that blends a group of computers together into a "crowd" in order to scramble information. With Crowds, people must join into a group where all their requests are sent through the crowd (Cranor, 1998).

Onion Routing occurs when users submit web site requests "using an onion, a layered data structure that specifies symmetric cryptographic algorithms and keys to be used as data is transported to the intended recipient" (Cranor, 2002, p. 30). Data is passed through routers where each router removes a layer of the onion (encryption). When private information needs to be sent, the most common way of keeping it private is to encrypt it. Encryption transforms "... the data into a different form. The resulting data can be understood only by those who know how to reform it to its original form" (Artz, 2001, p. 75). The problem with encryption is that the data still exists, and just like a lock, encryption can be picked or decrypted. Rather than encrypt, steganography hides data. It hides information in obvious files like forms, images, and audio files. There are many packages that combine encryption and steganography which will create superior privacy in communication.

Regulatory and Legislative Efforts to Protect Privacy

Over the years, many legislative acts have passed to protect consumer privacy but most are limited to specific industries and government agencies. Some acts, like the Privacy Act of 1974, the Computer Matching and Privacy Act of 1998, and the Telecommunication Act of 1996 limit the behavior of government agencies. The Gramm-Leach-Bliley Act is geared toward the financial industry, and the Health Insurance Portability and Accountability Act (HIPAA) focuses on the healthcare industry (Whiting, 2002, p. 54). None of these acts specifically address the Internet though. All of these acts increase consumer privacy in the traditional business world; however, it is difficult to know how these laws apply to cyberspace. Is (more) legislation needed?

Currently, very little legislative control exists on the Internet; it mainly operates under self-regulation. There are no major laws in place right now that protect information privacy for consumers (Volokh, 2000). Businesses decide for themselves whether to rely on business practices or technology to address consumers' concerns. Business self-regulation involves three characteristics of government; legislation to "define the appropriate rules," enforcement to take "action when rules are broken," and adjudication to determine "whether or not a company has violated the privacy rules" (Culnan, 2000, p. 20). Businesses and many governments fear that enforcing tight legislation will hinder transactions and growth online. To discourage legislation, businesses are creating privacy policies and procedures. Governments are giving businesses time to adhere to and establish such policies. An added benefit of the privacy policies is that businesses hope to gain consumer trust and confidence.

The effect of legislating privacy protections must be considered before enacting new legislation. For example, regulations and laws may give consumers a false sense of security, implicitly encouraging consumers to drop their guard. Information gathered by businesses for target marketing will be hindered. Newer companies would not be able to become established because they would be cut off from consumer information (Hall, 2001). Consumers would not be able to determine the level of privacy they wanted. Certain legislation could also be considered a violation of free speech (Caudill, 2000).

CORRELATING SOLUTIONS WITH CONCERNS

With knowledge of the solutions available to them, customers can more easily determine exactly what to do to alleviate their concerns over privacy on the Internet. The three main concerns are online customer identification, unsolicited customer contacts, and information distribution and sales. Solutions to these concerns are suggested in Table 2 as interpreted by the authors.

TABLE 2
Correlation solutions with concerns

Solutions

Concerns	Digital Signature	Anonymity Tools	Steganography	P3P	CPEX	XNS	Privacy Seals	Browsers	Awareness/ Knowledge
Online Customer Identification		X		X		X	X	X	X
Unsolicited Customer Contacts	X		X	X	X	X			X
Information Collection/ Usage	X			X		X	X		X
Consumer Effort	High	Medium	High	Medium	Medium	High	Low	Low	High

One of the most important solutions is for a customer to be aware and knowledgeable about the potential issues that can arise with privacy. If a consumer is knowledgeable about the problems and the solutions that exist, his/her concerns will be alleviated. A user who knows how to set up his/her computer with personalized privacy preferences can protect himself/herself against unwanted identification on a website, unsolicited contact, and unwanted distribution and sale of information. Also included in Table 2 is the level of consumer effort required to use each solution. A user must put in a lot of effort in order to become aware and knowledgeable about issues and solutions; he/she must seek out the information and take the time to understand it.

CONCLUSION

As each day passes, consumer information becomes less private in the eyes of government and businesses. Do we "own" information about ourselves? Is privacy online an oxymoron? Envision being watched constantly – everything you say or look at recorded. This paper has shown that many technologies exist to alleviate privacy concerns. If companies and individuals use currently available technologies along with reading and adhering to privacy policies and practices, then self-regulation should be adequate to safeguard consumers' privacy.

REFERENCES

Artz, D. (2001, May-June). Digital steganography: Hiding data within data. *IEEE Internet Computing*, 5(3), 75-80.

Caudill, E. M. & Murphy, P. E. (2000, Spring). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, 19(1), 7-19.

Cranor, L. F. (1998, June). Putting it together: Internet privacy: A public concern. *netWorker*, 2(3), 13-18.

Cranor, L. F. (1999, February). Internet privacy. *Communications of the ACM*, 42(2), 29-31.

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

Gaudin, S. (2002, April 26). Online privacy bill raising 'grave' e-commerce concerns. *Internetnews.com*, Retrieved June 8, 2002. Available at: http://www.internetnews.com/ec-news/article.php/1016831/.

Hall, M. (2001, August 13). The politics of privacy. *ComputerWorld*, 35(33), 32-33.

Han, P. & Maclaurin, A. (2002, January-February). Do consumers really care about online privacy? *Marketing Management*, 11(1), 35-38.

McGinity, M. (2000, April). Staying Connected: Surfing your turf. *Communications of the ACM*, 43(4), 19-21.

Reagle, J. & Cranor, L. F. (1999, February). The platform for privacy preferences. *Communications of the ACM*, 42(2), 48-55.

Sheehan, K. B.& Hoy, M. G. (2000, Spring). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73.

Technology's threats to privacy. (2002, February 24). *The New York Times*, 4.12.

Volokh, E. (2000, August). Personalization and privacy. *Communications of the ACM*, 43(8), 84-88.

Wang, H., Lee, M.K.O., & Wang, C. (1998, March). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, 41(3), 63-70.

Whiting, R. (2002, January 7). Companies get public with privacy. *InformationWeek*, 870, 53-54.