Protecting Your Privacy in Online Transactions

Brenda J. Cude and Sherry Neal, University of Georgia

Growth in electronic commerce has been impressive. Starting from virtually nothing in 1995, total electronic commerce is predicted to reach $330 billion in 2001-02. However, experts also note that *business-to-business* electronic commerce accounts for 80% of the total value of all electronic commerce activity (Office of Economic Cooperation and Development [OECD],1998).

Availability and cost of access as well as the complexity of using a personal computer seem to be important inhibitors to *business-to-consumer* electronic commerce (OECD, 1998). Another inhibitor is consumer concern about lack of control over personal information. In Georgia Tech's Graphics, Visualization, and Usability Center (GVU, 1998) survey of online users, over one-half of respondents were very concerned about online privacy and security issues. Most (85%) said that privacy and security features would be deciding factors in choosing whether to buy online.

Resolving basic consumer concerns about online privacy and security is important to both consumers and industry. The purpose of this article is to outline the primary consumer concerns and some possible solutions.

Privacy and Security Concerns in Online Transactions

As Hoffman, Novak, and Peralta (1998, p. 2) state, "Consumers simply do not trust most Web providers enough to engage in relationship exchanges with them." Their research indicates lack of trust is related to consumers' perceived lack of control over the access others have to personal information they give in online transactions. Ninety-four percent of Web users have declined to give personal information to Web sites at one time or another when asked (Hoffman, et al., 1998).

Goodwin (1991) describes two dimensions of information control. One is environmental -- the concern that because of the nature of the Web, the consumer cannot know who might "sniff" personal information sent online. Another way to describe this dimension of control is *security* -- how are data protected from unintended users as they are transmitted and after they reach the merchant?

Goodwin (1991) describes the second dimension of information control as secondary use of information or *privacy*. Regardless of the retail channel, many consumers, including those buying online, want to know if the seller has asked only for the information needed to complete the transaction, will use that information only for the purpose intended, and will not give or sell that information to others without the consumer's consent.

There is also evidence that consumers hold online sellers to a higher standard than merchants in the traditional marketplace. For example, while almost one-fifth of Web users believe that magazines have a right to sell their demographic information to other firms for direct-marketing purposes, only 12% think that Web sites have the same right (Hoffman, et al., 1998). This higher standard may be appropriate since Web sites can collect much more detailed consumer behavior information than would be possible in the traditional marketplace. For example, a Web merchant can collect information such as the consumer's electronic address, the specific history of goods and services searched for and requested, and other Web sites visited -- all without the consumer's knowledge or consent (Hoffman, et al., 1998). In addition, it is possible to get an overall picture of a consumer's Web activity. When consumers visit Web sites, they leave an electronic "marker" at each site. These markers or "clickstream" can be aggregated, stored, and reused (FTC, 1996).

Solutions

Stringent regulation to protect consumers' privacy or to guarantee the security of their online transactions appears unlikely in the near future. Industry representatives typically take the stance that regulation would be both "inappropriate and counterproductive," infringe on First Amendment rights, and discourage the growth of commercial applications of the Web (FTC, 1996, p. 27). To date, regulators have agreed, leaving market pressures to define the best privacy protections. Thus, online consumers must take matters into their own hands. How can consumers check the security of online transactions? How can they protect personal information?

Security

At its most basic level, concern about the security of an online transaction means knowing that the business behind the Web site actually exists and will deliver what it promises. Consumers might use several strategies to limit their exposure to fraudulent online merchants. They could choose to do business online only with merchants that also exist in the traditional marketplace. However, using that strategy would eliminate many of the largest online merchants, including Amazon.com and E-Trade.

Another approach would be to check for the BBB*Online* Seal of Approval (http://www.bbbonline.org). To display this seal, companies must meet several criteria including belonging to a local Better Business Bureau; giving the BBB information about company ownership and management as well as the street address and telephone number (which the BBB verifies); being in business a minimum of one year (with limited exceptions); and having a satisfactory complaint handling record with the BBB.

A third approach to assessing the legitimacy of an online business would be to read others' reviews of that business. For example, several "scorecards" rate financial services, including Money.com's Broker Scorecard (http://www.money.com) and Gomez' Scorecards for Internet brokers, banks, and insurers (http://www.gomez.com).

With confirmation that an online business is legitimate, a second level of security relates to how information is protected as it is transmitted online and after it reaches the merchant. Use of a secure browser by both the consumer and the merchant is an essential component of this protection. A secure browser encrypts data or translates them into secret code so that they make sense only to the intended recipient and are unintelligible to anyone else.

There are currently two types of encryption available in the U.S. -- 40-bit and 128-bit. The higher number of bits means stronger encryption; the larger the number, the more complex the algorithm, and the harder the code will be to crack. Most Web sites that collect personal information such as credit card or bank account numbers require that the consumer's Web browser use 128-bit encryption before he or she can begin the transaction. Currently, 128-bit encryption provides the highest level of security for Web transactions in the U.S. The most recent versions of both Netscape Navigator and Internet Explorer are capable of 128-bit encryption (http://www.netscape.com/security/basics/glossary.html#crypt).[1]

An easy way for the casual Web user to know if a Web site uses encryption is to look at the Uniform Resource Locator (URL) in the address or location box in the Web browser. If the URL begins with https, the page viewed is running a secure Web server (noted by the "s" after http) (http://webopedia.internet.com/TERM/S/SSL.html).

In a secure environment the data are encrypted while they are being transferred. Data may not be encrypted once they reach the merchant and are stored. This is an important point since theft of data from the merchant's server also poses a risk to consumers' privacy (FTC, 1996).

Consumers who use computers in a public setting should take other precautions to keep their private information secure. They should:

- Completely finish a secure transaction before leaving the computer.
- If personal information has been entered, log off from the Web site and close all windows of the browser before leaving the computer.
- Clear the *cache* before leaving the computer. The cache is a set of files stored to avoid having to download the same information again (Web pages, images, and other files).[2]
- Delete *cookies* on a regular basis. Cookies let the Web site's server put information about a user's visit to the site on the

consumer's machine in a text file that only the Web site's server can read. Because of cookies, on each return visit, the site can call up user-specific information, which could include the user's preferences or interests (FTC, 1996).[3]

Privacy

How does one evaluate the threat to personal privacy posed by dealing with an online merchant? Unfortunately, an estimated 86% of commercial Web sites give no information of any kind about how any demographic data will be used, or even if data are being collected (Landesberg, Levin, Curtin, & Lev, 1998).

When a merchant's privacy policy is available, a consumer could apply the standards of TRUSTe to evaluate the policy. TRUSTe, an organization created by a coalition of industry representatives, is an independent, non-profit initiative whose mission is to "build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent" (http://www.truste.org). A Web site displaying the TRUSTe mark has agreed to notify the consumer about personal information being gathered; how the information will be used; who the information will be shared with, if anyone; the choices the consumer has (if any) about how collected information will be used; how the merchant will protect stored data from loss, misuse, or alteration; and how the consumer can update or correct inaccuracies in information.

BBB*OnLine* also has a program through which it issues a Privacy Program seal to participating businesses. BBB reviews a company's online privacy policy and conducts a "very comprehensive Compliance Assessment review, evaluating the processes that a company has in place to live up to the privacy policies they are posting" (http://www.bbbonline.org).

For a variety of reasons, experts agree that parents should monitor their children's online activity. Explaining to children why they should not provide personal information in online transactions is critical. In addition, some of the software designed to give parents the ability to monitor and filter information their children receive online can also be used to prevent children from disclosing certain information online (FTC, 1996). Also, both BBB*Online* and TRUSTe have programs in which merchants pledge to adhere to special privacy guidelines if the target audience is children under age 13 (http://www.bbbonline.org; http://www.truste.org).

Implications for Consumer Educators

Both industry representatives and government regulators agree that consumer education is an essential part of protecting consumer privacy online (FTC, 1996). Key components of a consumer education unit on privacy and security would include:

- a review of related terminology, including encryption and cookies. Webopedia (http://webpoedia.internet.com) is one good resource;
- hands-on experience to prepare consumers to recognize when they are entering and leaving a secure environment;
- a review and evaluation of Web sites' policies related to online privacy and security; and
- a review and evaluation of the various organizations that provide seals of "approval" regarding online privacy and security, such as BBB*Online* and TRUSTe.

The FTC (1996) has suggested four elements as centrally important in effective protection of online consumers' privacy: notice, security, choice, and access. Implementation of each element depends on informed consumers. Consumers must look for notice about Web sites' policies concerning privacy and security and refuse to do business with sites that do not have adequate safeguards in place or do not post their policies. When given choices, consumers must make decisions that communicate the value they place on protecting their personal information. Finally, when consumers have the right to access the personal information that Web merchants know about them, consumers must exercise that option and correct errors they may discover. Consumer educators play a vital role in preparing consumers to assert their rights in the online marketplace.

References

Federal Trade Commission (FTC). (1996, June). *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure*. Retrieved September 28, 1999 from the World Wide Web: http://www.ftc.gov

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing, 12*, 106-119.

Graphics, Visualization, and Utilization Center (1998). *GVU's 10th WWW User Survey*. Retrieved September 28, 1999 from the World Wide Web: http://www.gvu.gatech.edu/gvu/user_surveys/survey-1998-10

Hoffman, D.L, Novak, T.P., & Peralta, M. (1998). Building consumer trust in online environments: The case for information privacy. *Project 2000 Working Paper*. Retrieved September 28, 1999 from the World Wide Web: http://ecommerce.vanderbilt.edu/papers.html

Landesberg, M.K., Levin, T.M., Curtin, C.G., and Lev, O. (1998, June). *Privacy Online: A Report to Congress*. Washington, DC: Federal Trade Commission.

Office of Economic Cooperation and Development. (1998). *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and*

Research Agenda. Retrieved September 28, 1999 from the World Wide Web: http://www.oecd.org

Endnotes

[1] You can check whether your browser is using encryption by looking for an image of a locked padlock in the lower right- (in Internet Explorer) or left- (in Netscape Navigator) corner of the browser window.

[2] To clear your cache in Netscape Navigator, go to Edit>Preferences>Advanced>Cache> and click on "Clear Disk Cache." In Internet Explorer, go to Tools>Internet Options>General>Temporary Internet Files and click on "Delete Files."

[3] In Netscape, cookies are stored in a file called cookies.txt, which contains all of the cookies on the computer's hard drive. Internet Explorer puts cookies in a folder called "cookies." You can delete the entire file or folder, or select individual cookies to delete.

Brenda J. Cude is Professor and Dept. Head, Department of Housing and Consumer Economics, University of Georgia, 215 Dawson Hall, Athens, GA 30602-3622; (706) 542-4857; e mail: bcude@arches.uga.edu.

Sherry Neal, Web Site Administrator, Terry of College of Business, Brooks Hall, University of Georgia, Athens, GA 30602.