

Privacy on the Internet: Is Your Right to Privacy a Click Away From Being Violated?

By Elizabeth A. Corradino, Esq.

May 2003

The unprecedented growth of technology has given people access to a World Wide Web of knowledge, information, and consumerism in a way that was previously unimaginable. However, one of the negative side effects of this growth is the diminished level of privacy protection. Every personal computer, Internet service provider, and Web site can now create, collect, and process personal information. Personal information has become a commodity, creating a market where comprehensive database profiles of individuals can be bought, sold, and manipulated in a variety of ways.

This type of information is also gathered in a number of ways, some of which require consumer participation, such as user surveys and order forms. Others collect information without user knowledge through the use of certain types of software, the most common of which are "cookies," "Web bugs," or "Web beacons."

If one begins with the premise that information about oneself is personal property, then the unauthorized collection and subsequent distribution of personal information can seriously compromise individual privacy rights. This article will explore how this information is being collected, for what purpose and whether safeguards are being put in place to protect it.

Data, Data Everywhere

In *Privacy, Identity, Databases: Toward a New Conception of the Consumer Privacy Discourse*, Stan Karas of the Boalt Hall School of Law observes that in the networked environment in which we now live, every click of a mouse leaves a data trace, which, if one knows where to look, provides a continuous record of an individual

and his or her activities. Personal information, now more than ever before, has great value to companies interested in specifically targeting consumers based on their personal profiles.

While numerous Web sites exist principally to provide information with no e-commerce component, many more are in the business of generating revenue. It is this model where the concept of "information as commodity" has the greatest impact.

Typically, consumer information is obtained by Web site operators, who then sell that information to third parties. Consumer information can also be collected directly by third party advertisers. For the most part, this information is obtained without the consumer's knowledge.

Because those who gather information depend so heavily on consumer ignorance of their activities, the first step in controlling the information-gathering process is to familiarize consumers with the technologies that make it possible to access personal information on the Internet. A prime example of such technology is a "cookie." Many consumers with an Internet connection are familiar with the term but it would be fair to say that a majority of consumers do not know that it describes small text files, left on a user's hard drive, used to track the user's navigation of a particular Web site. Essentially, cookies make use of user-specific information transmitted by the Web server onto the user's computer so that the information is available for later access by the originating server or other servers.

Although Web browsers can be configured to block the placement of cookies, such

configuration presupposes that the user is aware that he or she is being tracked. Furthermore, as a testament to the value of personal information in today's world, many Web sites now incorporate software that circumvents the counter-technology designed to block the unauthorized collection of personal information.

A more recent technological advancement, which is by far one of the most threatening, is the emergence of Web beacons, commonly referred to as "Web bugs." Web bugs are tiny, often transparent embedded graphics in web pages that can report a visitor's IP address, cookie information, and referring URL to the site's owner or a company advertising on the site.

Web bugs can be detected by viewing the source code of a Web page and looking for IMG tags that load from a different server than the rest of the site. Disabling a browser's cookies will also prevent Web bugs from tracking the user's activity and unique information. However, both these actions require a level of awareness or technological sophistication that the average Internet user does not possess. Moreover, due to the absence of legislation requiring that all Web sites contain privacy policies or mandating disclosures of the presence of information-gathering technology, the use of Web bugs is generally not disclosed by a Web site operator.

According to the Christopher Saunders article, "Congressional Group to Study Web Bugs" (internetnews.com), Web bugs have been targeted by the Congressional Privacy Congress as being of specific concern, because Web bugs allow advertisers to build a user's profile and gain access to personal and sometimes confidential infor-

mation without users knowing that they are being tracked.

Protecting Privacy on the Web

So, what is being done to safeguard personal information on the information super-highway?

The Federal Trade Commission which considers itself "the nation's consumer protection champion," has stated that it intends to expand its Privacy Agenda over the next few years, primarily by working within the framework of existing laws.

However, it does acknowledge that new legislation specifically created to address privacy issues on the Internet would increase consumer confidence in the medium by establishing a clear set of rules about how personal information is collected and used.

One of the better known examples of this type of legislation is the Children's Online Privacy Protection Act (COPPA), which became effective April 21, 2000. COPPA targets Web sites specifically directed at children and outlines what an operator of such a Web site must include in a privacy policy, when and how to seek verifiable consent from a parent and what the operator's responsibilities are vis-à-vis the protection of children's privacy and safety online.

However, because COPPA does not provide individuals with a private right of action, neither a parent nor a child can bring suit for an alleged violation of the act. The act also protects Web sites from liability in the event of a good-faith effort to remedy the disclosure of a child's personal information. And because the act only applies to commercial websites or online services directed to children under 13 or general audience Web sites whose operators have actual knowledge that they are collecting personal information from children, many other traffickers in personal information are left unregulated.

COPPA was invoked by the Electronic Privacy Information Center and 11 other groups in a complaint recently filed with the FTC. The complaint alleges that Amazon.com violated online privacy laws by allowing children to review books and then posting the reviewers' personal information, including home addresses, on the Web site, without first obtaining parental consent. Amazon.com's initial response is that no violation has occurred because its Web site is not aimed at children, but rather to adults who make purchases for children. Whether the FTC will use this complaint as an opportunity to redefine the scope of the act or as a springboard to protect other online data remains to be seen.

The Gramm-Leach-Bliley Act was also enacted specifically to address privacy concerns. Under Gramm-Leach-Bliley, financial institutions must provide their customers with notice of their privacy rights and, with certain exceptions, allow them to opt out of having that information forwarded to third parties.

There are also several bills pending before Congress that address online privacy issues, such as the privacy bill introduced by U.S. Rep. Clifford Stearns (R-Fla.), one of the leading advocates of privacy legislation, which contains an "opt-out" standard for consumers. However, there is strong opposition by Web companies such as Microsoft Corp, VeriSign Inc., and Sun Microsystems Inc., which claim that industry self-regulation, fueled by the desire of businesses to maintain good customer relations by addressing privacy concerns, is all that is necessary.

To date, none of the bills addressing online privacy issues have been passed, and there is still no legislation setting forth comprehensive regulations on the collection of personal data online. Until that time comes, individuals will continue to be at the mercy of the private sector to regulate its own conduct and respect their right to privacy.

Elizabeth Corradino is a partner in Moses & Singer's Privacy, Intellectual Property, Advertising, Entertainment, and New Media Practice Groups. Ms. Corradino would like to thank Jennifer Romano, a recent graduate of New York Law School, for her invaluable assistance in preparing this article.

MOSES & SINGER LLP
