Cyberprivacy in the New Millennium

Hal Berghel, University of Nevada at Las Vegas

Because the Constitution does not clearly and explicitly articulate a right to privacy, a legal standard of what constitutes privacy remains elusive in the United States. In 1965, Supreme Court Justice William O. Douglas declared that a penumbra within the wording of the First, Fourth, and Fifth amendments entitles each of us to a "zone of privacy." The extent of this zone, however, is unclear. Public officials and celebrities alike can testify that the penumbra shades some more than others.

US courts have generally operated under the principle that the right to privacy is tantamount to the right to be left alone, but everyday experience confirms that this right isn't absolute, even when we are in the comfort of our homes or offices. Mass marketers invade our privacy by calling us during mealtime, filling our mailboxes with junk mail, and spamming our personal computing space. Many employers read our e-mail and check the Web sites that we visit.

THE ELECTRONIC AUDITORIUM

Through the medium of e-mail, modern networking technology is slowly transforming our private sanctuaries into an electronic auditorium. I reflected on this trend some years ago in "E-mail: The Good, the Bad and the Ugly" (http://www.acm.org/~hlb/col-edit/digital_village/apr-97/dv_4-97.html), and my observations then remain true today.

E-mail lets us schedule our own communication interrupts, easily dismiss geographical transmission delays, and integrate seamlessly into our digital desktops. While e-mail is indispensable for most of us, its convenience is not without penalty. The collective streams of consciousness from our well-intentioned friends and associates can easily exceed our personal bandwidths, resulting in communication exhaustion. E-mail's ubiquitous, no-cost ease of use encourages "bombing," "flaming," and other forms of abuse. E-mail messages that bear embedded and attached viruses, or ill-behaved or malevolent executables, can wreak havoc on computers.

E-mail is indispensable for most of us, but one penalty of its convenience is its negative impact on individual privacy.

Cyberprivacy at work

The most worrisome aspect of e-mail, however, is its negative impact on individual privacy. An overt example of this concern is the famous 1996 case of *Smyth v. The Pillsbury Company*, in which the Philadelphia federal district court ruled that an employer's reading of employee e-mail does not "tortiously invade" the employee's right to privacy. Unlike telephone conversations, e-mail is considered corporate property because it relies upon corporate computer systems and inhabits corporate storage facilities.

The speciousness of this argument does not lessen its societal impact. Most of us simply refuse to organize our lives around server backup schedules, encryption technologies, disk housekeeping, and secure offsite storage to protect our privacy in the workplace.

Cyberprivacy at home

More subtly, e-mail has conditioned us to accept an unprecedented level of privacy invasion that extends into our most personal space, the home. Because unwanted e-mail has no volume, it is easy to discard and thus normally falls below our abuse threshold. How many of us would willingly accept the amount of snail mail we get if it came in physical form?

When we click on banners, respond to advertisements, or use the "mail to" autoreply embedded in Web sites and e-mail, we reveal something personal about ourselves—even if it's only the contents of the environment variables within our IP packets (visit my "CGI-Bin Bin" site at http://www.uark.edu/wrgx for more about how this technology works). Once a cottage industry, indexing personal identifiers such as e-mail addresses, IP numbers, fax numbers, server names, and other personal or transaction-oriented information is now a big business.

HANDS IN THE COOKIE JAR

The Web accelerated the digital assault on personal privacy begun by e-mail. In a process known as "profiling via click-throughs," modern "dynamic marketers" maintain huge databases of sundry personal data that they correlate with names, phone numbers, e-mail addresses, IP addresses, client- and server-side environment variables, and—most regrettably—Social Security numbers.

The cookie monster

The primary security hole for penetrating our zone of privacy is the cookie: digital information stored on the client computer by the browser software or network application (see http://www.cookiecentral.com). Originally intended as a harmless Web extension to overcome a deficiency in the statelessness of the hypertext transfer protocol, the cookie has become a bête noire of Internet privacy zealots and informed cybernauts.

The metaphor for HTTP, designed to minimize the bandwidth drain of persistent network connections, is "connect-process-request-respond-disconnect." Unlike Telnet, FTP, and other TCP/IP environments, HTTP enables only one request-response cycle at a time. Even something as simple as a request to change directories requires a separate connection.

The advent of electronic commerce made persistent communication connections necessary—for example, to fill "shopping carts." Because recording all this information on a server for millions of users is impractical, Netscape conceived of the client-side identifier, which they called a cookie.

A bad aftertaste

Web cookies come in two flavors, *session* and *persistent*. Session cookies, useful for transaction lists, last only as long as the browser session. Persistent cookies remain on the client until they reach an expiration date, the user manually deletes them, or a client-side cookie manager automatically deletes them. See the Resources sidebar for examples of cookie managers. To learn more about the recipe for digital cookies, see http://www.acm.org/~hlb/publications/web99/web99.html.

Persistent cookies can "remember" past navigation streams through Web sites, store account names and passwords, and personalize the appearance of a Web site based on recorded user preferences. However, not all persistent cookies are benevolent. Because the delimited "name=

Resources

Several products and services offer remedies for e-mail and Internet security problems.

Cookie managers are tools that exclusively allow you to block and control cookies. Popular utilities include

- http://www.rbaworld.com
  Cookie Cruncher enables you to view, edit, and delete Internet cookies. It includes an Internet shell and dial-up adapter.
- http://www.thelimitsoft.com
  Cookie Crusher allows refined real-time control over Web cookies, including support for multiple cookie paths and cookies in accept-from/reject-from lists.
- http://www.kburra.com
  Cookie Pal lets you decide which cookies your system will accept or reject.

Many products and services beyond cookie managers exist to protect online privacy. Examples include

- http://www.anonymizer.com
  Anonymizer.com is a subscription Internet service that prevents mass marketers, identity thieves, and others from seeing where you surf.
- http://www.xs4all.nl/~freeswan/
  Linux FreeS/WAN is an authentication and encryption service that allows Linux users to create a virtual private network.
- http://www.nsclean.com
  NS Clean and ***IE Clean*** protect your browser from FTP download sites using your e-mail address, Java and JavaScript exploits, newsgroup e-mail harvesters, ICQ chat and rogue ActiveX vulnerabilities, Visual Basic scripts, networked persistent cookies, and XML persistence.
- http://www.privacyinc.com/Browse/
  Privacy, Inc. is a membership service that maintains a cyberprivacy news archive, reveals what personal information various government agencies maintain, acts as your agent in submitting Freedom of Information/Privacy Act requests, and searches for your name in Internet databases.
- http://www.webroot.com
  Window Washer and ***MacWasher*** automatically clean your browser's cache, cookies, history, autocomplete form data, location drop-down bar, and other tracks.
- http://www.zeroknowledge.com
  Zero-Knowledge Systems provides online privacy protection technologies for both individuals and businesses.

Several Web sites provide online articles, links, and services related to the general problem of cyberprivacy. Popular sites include

- http://www.acm.org/hlb/
  Hal Berghel's Web site contains numerous articles, columns, and editorials on cyberprivacy.
- http://www.cpsr.org
  Computer Professionals for Social Responsibility is a public-interest membership organization that examines the impact of computer technology on society, including civil liberties and privacy.
- http://www.futurecrime.com
  The FutureCrime Prevention Association is a membership organization that helps prevent identity theft.
- http://www.privacyfoundation.org
  The Privacy Foundation educates the public about threats to privacy in the electronic world and resources available to combat them.

value" strings that make up the business part of a cookie have no content restrictions, they could, for example, include the user's Social Security number, telephone number, and e-mail address.

Further, cookies are inherently sharable among similar domains. Browsers match cookie lists with domain tails—the latter strings of domain names, separated by at least two dots—and can send those it detects to the server. A cookie containing "domain=widget.com" could, say, match with "sales_prospects.widget.com" or "share_with_hate-group.widget.com."

The potential for mischief doesn't end there. Modern productivity software, especially Web browsers, routinely renders multisource documents as single pages. Coalescing disparate Web resources in a single presentation window is one of HTML's great advantages. Few realize, however, that any server contributing part of a Web page can potentially retrieve, use, or share any cookie that relates to the main URL. Third parties can manipulate cookies by adding the active URL's domain tail to the end of their own in their domain ID, thereby making them difficult to block.

Third-party cookies, or "Web bugs," are less worrisome if the original page chunks are large and their source is plainly identifiable. Web bugs, however, typically measure only one pixel in size, practically invisible to the user. Because they seldom arouse suspicion, no one knows how widespread Web bug use has become for a wide variety of tracking, surveillance, and monitoring activities.

In addition to cookies, privacy threats arise from viruses, Trojan horses, Java scripts, ill-behaved HTTP servers, the identification daemon, "hit logging," spyware, the Windows 98 Registration Wizard, Internet Explorer's "phone home" feature, and public-domain utilities such as Comet Cursor. Innocuous productivity applications like Microsoft Word and PowerPoint, which embed network media just like browsers do, are in principle equally dangerous.

THE FULL MONTY

The misuse of Social Security numbers, made easier by the ability to harvest vast amounts of data inexpensively and conveniently through the Internet, represents the greatest potential threat to privacy in the new millennium.

Identity theft

Created as a unique record identifier for Social Security applicants in 1935, the SSN has, over time and through legislation, become the primary source of personal identification in the US. The reliance on a single identifier in government and commercial databases, credit reports, marketing lists, and so on makes the SSN a convenient tool for identity theft. According to a recent General Accounting Office report, losses due to this fastest growing type of white-collar crime approach $1 billion annually (GAO/GGD-98-100BR).

The misuse of Social Security numbers represents the greatest potential threat to privacy in the new millennium.

With just the SSN, an identity thief can extract enough data from the Web and other sources—such as personal items discarded in trash, intercepted mail, telephone books, subscription lists, artifacts acquired through theft and robbery, phony telemarketers, credit card carbons, calls to disreputable 8xx and 9xx telephone numbers, court records, and motor vehicle agencies—to create a duplicate, credit-worthy identity of virtually anyone. The multibillion-record database collections in cyberspace, cross-indexed and mined, do for identity theft what cookies and their sister-technology excesses do for activity tracking and computer identification.

Remedies

In addition to cookie managers, various digital appliances and software patches exist to limit online intrusion during browsing. Web anonymizers offer the ability to surf the Net in privacy by sanitizing packet headers that pass from the client to the server; pseudonym services perform a similar function for e-mail. Internet protocol security environments provide authentication and encryption services. Web monitors keep abreast of snooping. The Resources sidebar provides information about some companies that offer these services.

These products and services, however, offer only makeshift remedies to the cyberprivacy problem. Ultimately, Congress must deal with the "full monty"—the SSN and all other surrogate unique identifiers. Two such proposals are the Personal Information Privacy Act (HR 1450), introduced in 1999 by Rep. Gerald P. Kleczka of Wisconsin, and the Privacy and Identity Protection Act (HR 4857), introduced last year by Rep. Clay E. Shaw of Florida in conjunction with a similar Senate bill.

Under these proposed laws, consumers would regain considerable control over the use of their personal identifiers. Credit bureaus would be prohibited from giving out any information not available in the phone book without written consent. Businesses, especially those engaged in electronic commerce, could no longer require SSNs as a condition of doing business. "Put simply," Congressman Kleczka has stated, "protecting the SSN is to identity theft as locking the door is to burglary."

Hal Berghel is professor and chair of computer science at the University of Nevada at Las Vegas and a frequent contributor to the literature on cyberspace.

Editor: Ron Vetter, University of North Carolina at Wilmington, Department of Computer Science, 601 South College Rd., Wilmington, NC 28403-3297; voice +1 910 962 7192, fax +1 910 962 7457; vetterr@uncwil.edu