

"Is Your E-Mail Watching You?"

By Stefanie Olsen

Note: *This article is reprinted by permission granted from Robert Gwynn of NACL (Nat'l Anti-Cookie League)*

Watch out – the spam choking your e-mail in-box may be loaded with software that lets marketers track your moves online, and you may not even be aware that you've been bugged.

Web sites have long planted bits of code called "cookies" on consumers' hard drives to tailor Internet pages for returning visitors and better target ads. Now, enhanced messages that share the look and feel of web pages are being used to deliver the same bits of code through e-mail, in many cases without regard for safeguards that have been developed to protect consumer privacy on the web.

Consumer notice and choice have been at the heart of the Internet privacy debate for years, driving popular web companies including eBay, Yahoo and DoubleClick to write tough-sounding web privacy policies. Playing offense, civil libertarians and privacy groups for years have stalked web sites for violations of their stated policies and have kept an eye on secretive tracking tactics. Although many of the same troubles are cutting into e-mail, disclosure of such data-gathering practices has not received anywhere close to the level of scrutiny it has had on the web.

In some cases, spammers may be able to link formerly anonymous consumers with their e-mail addresses. For example, a web site specializing in horoscopes may know a consumer only by birth date. But if that web site rents a list of e-mail addresses with that consumer's address on it, the company may be able to link the address to the individual's birth date and visits to the site.

"In many ways, e-mail tracking is more powerful because they can correlate the e-mail address with online history," said Lance Cottrell, president of Anonymizer, an Internet privacy services company. "There isn't an opportunity to be fully informed when you receive a spam with remotely loaded graphics used to track your computer," he added, "It's a bit of a loophole in the whole process."

The rise of e-mail tracking runs parallel to the adoption of "rich e-mail" or messages that incorporates the programming language most commonly used to display web pages, known as HTML (Hypertext Markup Language). Such messages may include web pages, audio and video in addition to ordinary text.

According to a recent report from the industry trade group the Direct Marketing Association (DMA), 65 percent of online marketers regularly send HTML e-mail to consumers or prospective customers. By incorporating HTML, the e-mail acts like a web page, requesting graphics and content from a web server and counting as a "hit" to the company's web site. Taking advantage of the technology, marketers can track how and when people respond to e-mail, note where they click, and track follow-up actions on their web pages. They do this by embedding cookies or clear GIF images known as web beacons, an action that isn't possible in a simple text message.

Digital Impact, an e-mail marketing company, uses a range of tactics to measure the effectiveness of campaigns for its customers, which include Citigroup, Bank of America, Wal-Mart, Target, and The Gap. Since its launch in 1998, Digital Impact has sent about 3 billion commercial e-mails. Gerardo Capiel, chief technology officer and co-founder of Digital Impact, said that while about

70 percent of the e-mail the company sends for customers is HTML, less than 30 percent of HTML e-mail includes tracking technology. Capiel said the company asks that its customers address e-mail communication in their privacy policies. "We don't set a cookie when you open the e-mail, but you might get one when you click through," he said. "It's really a questions of how aggressive the marketer wants to get to track revenue."

Experian, another e-mail marketing company, started using cookies this year to better track digital communications for its customers. According to its privacy policy, it uses cookies and web beacons to monitor when an e-mail was opened, how many times an e-mail recipient forwarded the message, and which web addresses were clicked on, among other actions.

Christine Frye, chief privacy officer of Experian's e-marketing services unit, said the company has started working with customers to educate them on updating their privacy policies to include e-mail tracking. So far, "They've been very receptive to that." She said. However, she would not name any Experian customers.

Such techniques have become pervasive enough to attract the attention of browser and e-mail software makers. Some e-mail programs already include settings allowing consumers to block cookies. Microsoft's Internet Explorer 6.0, for example, offers controls for cookies on the web and via the company's Outlook and Outlook Express e-mail programs. Turning on the "prompt for cookies" setting can reveal the stunning extent of the problem, unmasking unsolicited HTML e-mail messages that try to lay down cookies on a hard drive.

According to Microsoft, IE 6, Outlook and Outlook Express block cookies by default in HTML mail and place such mail automatically in a secure "restricted" zone. The settings have not always proven effective, however. Well-known security expert Richard Smith has reported at least one bug that allows cookies to be planted through Outlook despite the default settings.

Rajeev Dujari, development manager on IE 6 for Microsoft, countered that Outlook is designed to let consumers read e-mail in different security zones and control cookies through privacy settings, But he admitted that consumers need to better educate themselves to set a defense against increasingly invasive marketing tactics. "Our default is around cookies being part of a web experience rather than an e-mail experience," Dujari said. "When consumers get e-mail, people don't usually expect a cookie."

E-mail marketing also raises sticky questions for marketing companies who deliver ads into rich e-mail. Although these companies typically guarantee anonymous data collection, it theoretically would be easy to tie that data back to an e-mail address in an e-mail-based marketing campaign, according to privacy experts.

DoubleClick, a heavyweight in web ad delivery and e-mail marketing, offers a service called DartMail that lets companies manage, deliver and track e-mail marketing campaigns. The technology allows customers to add software such as cookies or web beacons to a campaign and track the effectiveness of a promotion. DoubleClick said that data it collects online is kept separate from data collected through e-mail.

J.Crew is a customer of DoubleClick's DartMail, but the retailer does not specifically address e-mail monitoring practices in the privacy policy published in its web site. The policy says only that "In some instances, we may use third-party companies to help us serve you better. These companies may be

given access to some or all of the information you provide to us and may use cookies on our behalf." J.Crew did not immediately respond to requests for comment.

"E-mail privacy hasn't been on the radar until recently," said Larry Ponemon, CEO of the Dallas-based Privacy Council, a knowledge management and technology company. He added that most companies still don't fully understand how e-mail plays a role in privacy and security.

One problem with the disclosure of e-mail privacy stems from the large percentage of e-mail marketing campaigns that are conducted at arm's length through third-party providers. As a result, companies that retain e-mail marketing services may not always be fully aware of the practices employed on their behalf.

Walmart.com, for example, delivers opt-in e-mail marketing through third-party providers. It does not mention e-mail monitoring in its privacy policy, however, which was last updated December 8, 2000, according to its web site. In an interview, Walmart.com spokeswoman Cynthia Lin confirmed that the company tracks customers through e-mail using "software technology." Still, she said the company's privacy policy is adequate. "Any data gathering that occurs after consumers leave the e-mail client is not technically part of the e-mail experience, even if the original web link is embedded in an e-mail."

[END]