

November 22, 2000

## Software to Track E-Mail Raises Privacy Concerns

By AMY HARMON

It was during a recent job search that Donald Bell gave in to the temptation to bug his own e-mail. Mr. Bell, 55, had e-mailed dozens of résumés to prospective employers and received scant response. Naturally he wondered: was he being rejected, or had his messages gone unread?

Anyone who has been left hanging knows it is the sort of nagging question that is rarely answered. But thanks to a furtive application of a feature common to the latest e-mail programs, Mr. Bell was able to learn, undetected, that the intended recipients were indeed opening his messages. With a service he found on the Internet, he could even tell precisely when a recipient read his e-mail messages and if the message was sent on to anyone else.

"It feels a little naughty, because you can't do this with postal mail," said Mr. Bell, who has since started his own company in San Francisco and sometimes uses the e-mail service to check whether colleagues forward messages that he considers confidential. "But e-mail is a different animal. You have to just reach into your heart and decide what you're going to do."

Mr. Bell is not alone in taking advantage of new e-mail software that makes certain kinds of monitoring easy and nearly imperceptible. At a time when many Internet users have come to grips with advertisers' tracking their anonymous trail of clicks across the World Wide Web, the frontier of the electronic privacy wars is shifting to the more personal realm of the e-mail "in" box.

Marketing companies now regularly keep tabs on which prospective customers open their e-mail solicitations, and at what time of day, arguing that consumers benefit because the information is used to devise more personalized promotions. Individuals who have used e-mail tracking services say they feel entitled to monitor their own correspondence in a medium where it is so easily passed along or ignored.

But privacy advocates contend that such practices open a new window of surveillance on a traditionally private sphere of communications. They compare it to having



Dan Krauss for The New York Times  
Donald Bell sorts through "snail mail" at his office in San Francisco. He is a user of new software that monitors e-mail messages he sends.

### Related Articles

[Wiretapping System Works on Internet, Review Finds](#) (November 22, 2000)

[Ruling Says Parents Have Right to See List of Sites Students Visit](#) (November 10, 2000)

[Lessons in Spam: A Nordstrom E-Mail Goes Astray](#) (October 30, 2000)

[Group Objects to F.B.I. Release of Carnivore Information](#) (August 18, 2000)

[Ongoing Coverage of Digital Privacy](#)

### Forum

[Can Privacy Be Protected Online?](#)

### Audio

• [AP Business Report, Updated Twice Each Hour](#)

### Business Home

• [Return to Business Page](#)

### Technology Home

• [Return to Technology Page](#)

### GET QUOTES

[Look Up Symbol](#)

Enter Multiple Symbols

[Portfolio](#) | [Stock Markets](#) | [Mutual Funds](#) | [Bonds](#) | [Currencies](#)  
| [Bank Rates](#) | [Industries](#)

ADD YOUR THOUGHTS

someone who leaves a message on your answering machine — a telemarketer, say, or your mother — alerted the moment you listen to it. More troubling, they say, is that the same technology can be used to match a recipient's e-mail address with previously anonymous records of the Web sites visited from that person's computer.

Invasion of Privacy?  
Should people be entitled to find out if the recipient of their e-mail has read it?  
[Add your thoughts](#) in Abuzz. Or [start your own discussion](#) about Technology News.

Connecting the data collected through files known as cookies with an e-mail address, the privacy advocates argue, will be irresistible to marketers seeking to identify the buying habits and personal tastes of individual consumers. The linked databases, they say, could also be consulted by law enforcement agencies, insurance companies, employers and others who would need only an e-mail address to look up a record of an individual's activities on the Web.

"You can buy 50,000 addresses of people who subscribe to The New Yorker," said Richard M. Smith, chief technology officer of the Privacy Foundation. "But you don't know what articles they're reading in it, or what books they've bought or what medical problems they've been researching lately. That's very much a possibility within this technology."

The technology in question is seemingly innocuous: the ability of the latest e-mail programs to send and display images. E-mail senders use the feature, based on the Web's computer language, to create colorful messages known as HTML mail.

But many also use it to embed tiny images that are invisible to the recipients. Marketers call them pixel tags and say they are used to gauge the success of e-mail campaigns. Privacy advocates prefer a more ominous name — Web bugs.

The instant someone opens an e-mail message that contains instructions to display a graphic file, his or her computer automatically fetches the image from a specified location on the Internet. By adding a unique identifying code to those instructions, a sender can record when a particular recipient retrieves the image, and, thus, when the e-mail message is opened.

Subsequent retrieval of the image can tell the sender how often the message is reopened, and sometimes whether it has been forwarded (though not the precise forwarding address).

Direct marketers, the most frequent users of the technique, say it is akin to the standard practice among Internet advertisers of tracking which banners Web surfers click on.

"I don't see any privacy issues there because the data is secure and never sold," said William Park, chief executive of **Digital Impact**, an e-mail marketing company that has designed campaigns for dozens of clients. "From the marketing perspective, if you're not opening that e-mail it might be we're sending it on the wrong day of the week, or the subject line is really boring, or the subject line is really cryptic."

The emergence of HTML mail may well make reading e-mail messages more like visiting a Web site, with all the attendant privacy risks. But for many Internet users, such risks may seem more acceptable on the Web than they do in their "in" box.

Sophisticated Internet users know that when they click on a Web advertisement they are probably exposing themselves to scrutiny, and that it is possible to reject the files that record such behavior.

But few are aware of the tracking capability of HTML mail. And while some e-mail programs, like Microsoft Outlook and Eudora, give users the option of screening images out, others, like America Online 6.0 and Web-based Hotmail do not.

Some recipients of e-mail newsletters say they do not mind if the sender knows when they open a message, particularly if the aim is to alert them to a sale or a new product. But others argue that it violates their right to communicate, or not, without being observed. And particularly in a country where postal mailboxes are protected by federal law, the notion that reading e-mail messages is no longer a private act may prove disconcerting.

"We would shudder if regular letters were implanted with secret signals that alerted their senders when they were opened," said Jeffrey Rosen, author of "The Unwanted Gaze: The Destruction of Privacy in America" (Random House, 2000). "It seems to invade both the privacy of the home and in some sense the privacy of the mind."

Still, the practice is becoming more common. About 60 percent of e-mail users have software that can read HTML mail, according to the online research firm Jupiter Media Metrix, a number expected to grow significantly as America Online users install version 6.0, the first update to include the feature, released last month.

As advertising on Web sites proves increasingly ineffective, many companies like Eddie Bauer and Borders are relying more heavily on e-mail solicitations whose value lies in part in the ability to track recipient response. How many subscribers actually open e-mail has also become an important measurement by which e-mail newsletter companies like **Lifeminders** sell advertising. Companies that send unsolicited bulk e-mail use tracking to increase the value of their address lists by weeding out those who never open their messages.

And individuals can use **Postel Services**, the Korean company whose service Mr. Bell used to learn the fate of his job applications. Messages routed through its servers have tiny graphic files appended before being sent on. When the recipient opens the message, Postel is alerted and in turn alerts the sender.

Soobok Lee, the company's founder, said about 30,000 people had used the service since its introduction in May, in addition to several companies that had purchased licenses to track all of their correspondence. The first 30 messages a month are free, after which Postel charges 2 cents a message.

But whatever the utility or etiquette involved in monitoring the opening of a single e-mail message, it is the potential for that act to open a door to far more personal information that some find most unsettling.

The main object of concern is advertising companies like **DoubleClick**, **Engage** and **24/7 Media** that already track the Web travels of tens of millions of Internet users, anonymously, by way of cookies.

The first time someone visits a site where DoubleClick places advertisements, for instance, the company deposits an identifying code — No. 1234, say — on the visitor's computer. After that, every time the computer with cookie No. 1234 visits one of the several thousand sites that contract with DoubleClick, the company records the visit.

DoubleClick and others use the information gleaned from cookies to choose which advertisement from the hundreds of clients they represent is most suited to an individual's tastes. They may know, for instance, that No. 1234 has recently visited sites related to quitting smoking, sport utility vehicles and the Green Party — but they have generally had no way of knowing who No. 1234 is.

The opportunity to identify the person behind the cookie comes when one of the advertising firms sends HTML mail to a consumer on behalf of a client, tagged with a unique identifier to track when it is opened. When the recipient opens such a message, the cookie code is exposed to the sender's server computer, which can compare it with those stored in its own database. At that moment, No. 1234 could be revealed as joe@computer.com.

After drawing scrutiny this year from the Federal Trade Commission, the major advertisers have vowed to refrain from linking personally identifiable information to anonymously collected data without permission from the consumer. But privacy advocates say consumers may consent unwittingly, and they note that voluntary privacy policies are easily modified.

Another practice, which involves using e-mail as a kind of Trojan horse to deliver a cookie file, recently prompted the Michigan attorney general's office to warn that it would sue one Web site, **Evite**, under the state's Consumer Protection Act unless it began to inform consumers.

Party organizers use Evite, a San Francisco-based online invitation service, to send e-mail HTML invitations. In addition to collecting the official R.S.V.P.'s, Evite is able to tell the organizer who opened the mail without responding, and who did not open it. Those who open the invitation receive a cookie from Evite, which would not otherwise be possible unless they visited its Web site.

Privacy advocates speculate that the company could "rent" the cookie and the e-mail address it is associated with to other sites.

Evite's chief executive, Josh Silverman, declined to be interviewed, citing continuing negotiations with the Michigan attorney general. He said in a statement that the cookies Evite delivered were not linked to addresses.

But Nick Ragouzis, a technically savvy business consultant in San Francisco who discovered Evite's invisible pixel in an invitation he received recently, said that alone was enough to make him feel his privacy had been invaded.

"I don't really care that they know I opened this particular message," Mr. Ragouzis said. "But they never asked me. And there would be other messages that I would care about. I feel I should be asked."

Mr. Ragouzis said he told the host of the party, Jad Duwaik, to refrain from sending him future Evite invitations and asked that he stop using the company's services altogether. But Mr. Duwaik, who organizes networking events for entrepreneurs, said the information provided by Evite about how many of the invitees open the message helped him gauge interest in his parties.

"It's something I feel uncomfortable with as a consumer," Mr. Duwaik said. "But as an organizer it's just too useful to give up."