washingtonpost.com

Every Click You Make

Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising

By Peter Whoriskey
Washington Post Staff Writer
Friday, April 4, 2008; D01

The online behavior of a small but growing number of computer users in the United States is monitored by their Internet service providers, who have access to every click and keystroke that comes down the line.

The companies harvest the stream of data for clues to a person's interests, making money from advertisers who use the information to target their online pitches.

The practice represents a significant expansion in the ability to track a household's Web use because it taps into Internet connections, and critics liken it to a phone company listening in on conversations. But the companies involved say customers' privacy is protected because no personally identifying details are released.

The extent of the practice is difficult to gauge because some service providers involved have declined to discuss their practices. Many Web surfers, moreover, probably have little idea they are being monitored.

But at least 100,000 U.S. customers are tracked this way, and service providers have been testing it with as many as 10 percent of U.S. customers, according to tech companies involved in the data collection.

Although common tracking systems, known as cookies, have counted a consumer's visits to a network of sites, the new monitoring, known as "deep-packet inspection," enables a far wider view -- every Web page visited, every e-mail sent and every search entered. Every bit of data is divided into packets -- like electronic envelopes -- that the system can access and analyze for content.

"You don't want the phone company tapping your phone calls, and in the same way you don't want your ISP tapping your Web traffic," said Ari Schwartz of the Center for Democracy and Technology, an advocacy group. "There's a fear here that a user's ISP is going to betray them and turn their information over to a third party."

In fact, newly proposed Federal Trade Commission guidelines for behavioral advertising have been outpaced by the technology and do not address the practice directly. Privacy advocates are preparing to present to Congress their concerns that the practice is done without consumer consent and that too little is known about whether such systems adequately protect personal information.

Meanwhile, many online publishers say the next big growth in advertising will emerge from efforts to offer ads based not on the content of a Web page, but on knowing who is looking at it. That, of course, means gathering more information about consumers.

Advocates of deep-packet inspection see it as a boon for all involved. Advertisers can better target their pitches. Consumers will see more relevant ads. Service providers who hand over consumer data can share in advertising revenues.

And Web sites can make more money from online advertising, a $20 billion industry that is growing rapidly.

With the service provider involved in collecting consumer data, "there is access to a broader spectrum of the Web traffic -- it's significantly more valuable," said Derek Maxson, chief technology officer of Front Porch, a company that collects such data from millions of users in Asia and is working with a number of U.S. service providers.

Consider, say, the Boston Celtics
Web site. Based on its content, it posts ads for products a Celtics fan might be interested in: Adidas, a Boston hotel and so on.

With information about users from deep-packet inspection, however, advertisers might learn that the person looking at the Celtics Web site is also a potential car customer because he recently visited the Ford site and searched in Google for "best minivans." That means car companies might be interested in sending an ad to that user at the Celtics site, too.

For all its promise, however, the service providers exploring and testing such services have largely kept quiet -- "for fear of customer revolt," according to one executive involved.

It is only through the companies that design the data collection systems -- companies such as NebuAd, Phorm and Front Porch -- that it is possible to gauge the technology's spread. Front Porch collects detailed Web-use data from more than 100,000 U.S. customers through their service providers, Maxson said. NebuAd has agreements with providers covering 10 percent of U.S. broadband customers, chief executive Bob Dykes said.

In England, Phorm is expected in the coming weeks to launch its monitoring service with BT, Britain's largest Internet broadband provider.

NebuAd and Front Porch declined to name the U.S. service providers they are working with, saying it's up to the providers to announce how they deal with consumer data.

Some service providers, such as Embarq
and Wide Open West, or WOW, have altered their customer-service agreements to permit the monitoring.

Embarq describes the monitoring as a "preference advertising service." Wide Open West tells customers it is working with a third-party advertising network and names NebuAd as its partner.

Officials at WOW and Embarq declined to talk about any monitoring that has been done.

Each company allows users to opt out of the monitoring, though that permission is buried in customer service documents. The opt-out systems work by planting a "cookie," or a small file left on a user's computer. Each uses a cookie created by NebuAd.

Officials at another service provider, Knology, said it was working with NebuAd and is conducting a test of deep-packet inspection on "several hundred" customers in a service area it declined to identify.

"I don't view it as violating any privacy data at all," said Anthony Palermo, vice present of marketing at Knology. "My understanding is that all these companies go through great pains to hash out information that is specific to the consumer."

One central issue, of course, is how well the companies protect consumer data.

NebuAd promises to protect users' privacy in a couple of ways.

First, every user in the NebuAd system is identified by a number that the company assigns rather than an Internet address, which in theory could be traced to a person. The number NebuAd assigns cannot be tracked to a specific address. That way, if the company's data is stolen or leaked, no one could identify customers or the Web sites they've visited, Dykes said.

Nor does NebuAd record a user's visits to pornography or gaming sites or a user's interests in sensitive subjects -- such as bankruptcy or a medical condition such as AIDS. The company said it processes but does not look into packets of information that include e-mail or pictures.

What it does do is categorize users into dozens of targeted consumer types, such as a potential car buyer or someone interested in digital cameras.

Dykes noted that by a couple of measures, their system may protect privacy more than such well-known companies as Google. Google stores a user's Internet address along with the searches made from that address. And while Google's mail system processes e-mail and serves ads based on keywords it finds in their text, NebuAd handles e-mail packets but does not look to them for advertising leads.

Such privacy measures aside, however, consumer advocates questioned whether monitored users are properly informed about the practice.

Knology customers, for example, cull the company's 27-page customer service agreement or its terms and condition for service to find a vague reference to its tracking system.

"They're buried in agreements -- who reads them?" said David Hallerman, a senior analyst at eMarketer. "The industry is setting itself up by not being totally transparent. . . . The perception is you're being tracked and targeted."