Lawmakers Probe Web Tracking
Panel Examining Ad Technology for Privacy Concerns

By Ellen Nakashima
Washington Post Staff Writer
Thursday, July 17, 2008; D01

An Internet provider based in Kansas used a monitoring technology earlier this year to track sites visited by its users, apparently without directly notifying them, according to a congressional panel investigating the action.

Embarq, which serves 1.3 million Internet customers in 18 states, including Virginia, acknowledged that it used "deep packet inspection" technology provided by the Silicon Valley firm NebuAd to direct targeted advertising to users.

Some lawmakers and others question whether such actions violate users' rights to keep their Internet behavior to themselves. The House Energy and Commerce subcommittee on telecommunications and the Internet will take up the subject at a hearing today.

"Surreptitiously tracking individual users' Internet activity cuts to the heart of consumer privacy," said Rep. Edward J. Markey (D-Mass.), the panel's chairman. "Embarq's apparent use of this technology without directly notifying affected customers that their activity was being tracked, collected and analyzed raises serious privacy red flags."

Federal wiretap laws generally require consumers to consent to the collection and use of their communications. There has been ongoing debate over whether the technology's use for behavioral targeting violates these laws.

Developed to speed the routing of Internet communications, deep packet inspection has evolved to include such uses as detecting viruses. Recently it has been turned toward the lucrative online advertising business. But the move into marketing has raised privacy concerns that could slow its adoption by large service providers, industry experts said.

Online ad companies like Google can track users' browsing behavior only on Web pages that host its ads. In contrast, deep packet inspection technology installed in an Internet service provider's network permits a window into potentially all of a consumer's online activity, from Web surfing and search terms to any unencrypted Web communication, experts said.

"We see virtually every site that you go to. This gives us much greater reach, relevance and results for our advertisers," NebuAd chief executive Bob Dykes told an audience of online media and advertising executives in New York in February. "We actually see not only that you went to all these sites, we know what you did on the sites. For example, if you went to a travel site, we know that you're looking to go to Las Vegas or the south of France."
In an interview yesterday, Dykes said that NebuAd does not collect or keep a person's name or other "personally identifiable information" but rather tracks the sites he visits, linking them to an encrypted, anonymous identifier.

NebuAd can, but does not, monitor e-mail, instant messages or Internet phone calls, a spokeswoman said.

"Our position is well-supported," Dykes said, "that we operate within the law."

But Alissa Cooper, chief computer scientist for the Center for Democracy and Technology, said that what NebuAd and similar firms are doing is akin to wiretapping without the subject's permission.

"This is an obvious privacy violation even when the eavesdropper does not know your identity," she said. "The issue we have is with the interception itself. We think people simply do not expect a middleman to be sitting between them and the Web sites they visit."

This week, Markey, committee Chairman John D. Dingell (D-Mich.) and Rep. Joe L. Barton (R-Tex.) sent a letter to Embarq seeking to know, among other things, where the firm tested the technology, with how many subscribers and why it chose to proceed without first asking customers whether they wanted to opt in.

A "minuscule" subset of customers was targeted in the test, which ended in March, said a source familiar with the test who spoke on condition of anonymity.

Embarq spokeswoman Debra Peterson said company officials "are reviewing [the letter] for an appropriate response."

Last month, Charter Communications of St. Louis, the country's fourth-largest cable operator, backed off a plan to partner with NebuAd, citing "questions about this service" from customers.

Dykes said that "clearly quite a few" service providers have suspended their arrangements, which proves the need to "better educate the public" about NebuAd's privacy policies. For instance, he said, providers can offer consumers direct online notice that their browsing activity will be tracked for ad purposes and that they may opt out of this.

The new technology, said Emily Riley, online advertising analyst with Jupiter Research, "is almost too exciting for marketers to resist" but also is "a minefield" for privacy because of what she calls the creepiness factor.

"If you remind people that you're tracking them -- 'Hey, I know that you recently started wearing medium T-shirts instead of large. Did you lose weight?' That's creepy," she said.

Staff researcher Madonna Lebling contributed to this report.
Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the full rules governing commentaries and discussions. You are fully responsible for the content that you post.

© 2008 The Washington Post Company

Ads by Google

Congress v. Your Privacy
Warrantless spying bill passes Support the ACLU lawsuit
www.aclu.org/fisaaction

Spy Tools for Cell Phones
Listen remotely to Calls & Read SMS ANY Distance, NO Range Limitation
www.Phone-Spy.net

Cell Phone Cheating
9 Out of 10 Cheating Spouses Exposed by Cell Phone Use!
www.ReversePhone123.com