

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit [www.djreprints.com](http://www.djreprints.com)  
 See a sample reprint in PDF format. Order a reprint of this article now

WHAT THEY KNOW | November 23, 2010, 11:31 p.m. ET

# Shunned Profiling Technology on the Verge of Comeback

By **STEVE STECKLOW** and **PAUL SONNE**

One of the most potentially intrusive technologies for profiling and targeting Internet users with ads is on the verge of a comeback, two years after an outcry by privacy advocates in the U.S. and Britain appeared to kill it.

## A History of Phorm



[More interactive graphics and photos](#)

The technology, known as "deep packet inspection," is capable of reading and analyzing the "packets" of data traveling across the Internet. It can be far more powerful than "cookies" and other techniques commonly used to track people online because it can be used to monitor all online activity, not just Web browsing. Spy agencies use the technology for surveillance.

Now, two U.S. companies, Kindsight Inc. and Phorm Inc., are pitching deep packet inspection services as a way for Internet service providers to claim a share of the lucrative online ad market.

Kindsight and Phorm say they protect people's privacy with steps that include obtaining their consent. They also say they don't use the full power of the technology, and refrain from reading email and analyzing sensitive online activities.

Use of deep packet inspection this way would nonetheless give advertisers the ability to show ads to people based on extremely detailed profiles of their Internet activity. To persuade Internet users to opt in to be profiled, Kindsight will offer a free security service, while Phorm promises to

provide customized web content such as news articles tailored to users' interests. Both would share ad revenue with the ISPs.

Kindsight says its technology is sensitive enough to detect whether a particular person is online for work, or for fun, and can target ads accordingly.



The Daily Telegraph

CEO Kent Ertugrul outside Phorm's office in London. The company studies people's interests based on websites they visit to show them ads.

"If you're trying to engage in one-stop-shopping surveillance on the Internet, deep packet inspection would be an awesome tool," says David C. Vladeck, director of the Federal Trade Commission's Bureau of Consumer Protection. When deep packet inspection is used for targeted ads, the FTC has made it clear that broadband providers "should, at a minimum, notify consumers that the ISP was mining the information and obtain clear consumer consent," Mr. Vladeck says.

Kindsight, majority owned by telecommunications giant Alcatel-Lucent SA, says six ISPs in the U.S., Canada and Europe have been testing its security service this year although it isn't yet delivering targeted ads. It declined to name the clients.

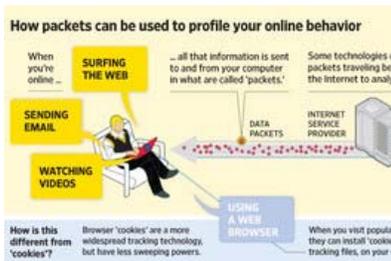
"These are tier-one ISPs we're working with," says Mike Gassewitz, Kindsight's chief executive. He says his company also has been placing ads on various websites to test the ad-placement technology and build up a base of advertisers, which now number about 100,000.

Two large ISPs in Brazil—Oi, a unit of Tele Norte Leste Participacoes SA, and Telefonica SA—currently have deals with Phorm. Oi, Brazil's largest broadband provider with about 4.5 million customers, has launched the product initially with about 10,000 people in Rio De Janeiro.

"We want to grow that," says Pedro Ripper, Oi's strategy and technology director.

A spokesman for Telefonica says it is testing the service on about 1,000 broadband customers and will evaluate the results before deciding whether to roll it out. "The user has the choice to enable or disable the service anytime he or she wants to," the company said in a statement.

Phorm is hoping to introduce its service in South Korea and eventually in the U.S. "It is designed from the ground up to ensure one thing and that is privacy," says Kent Ertugrul, Phorm's chief executive.



Kindsight and Phorm say the ISPs don't provide them with subscribers' real identities. Both also say they don't collect any personal information, read email, store users' browsing histories or monitor sensitive sites such as health blogs. Subscribers must "opt in," or give their consent to participate, both companies say.

Both the Kindsight and Phorm systems study people's behavior and interests based on the websites they visit to show them relevant ads. Mr. Gassewitz says that unlike web-based tracking methods, which generally create a single behavioral profile no matter how many people share a computer, Kindsight can "generate multiple characters per human."

"If I come online and I'm in work mode, I will show up as a very different character than when I go online Saturday morning and I'm in recreation mode," he says. The targeted ads would reflect which "character" is online.

Mr. Gassewitz calls that some of Kindsight's "secret sauce." The company this year filed a patent on its "character differentiation" technology.

A new revenue source would mark a welcome change for ISPs. The companies have been under pressure to offer ever-faster Internet services at lower prices, while Google Inc. and other companies raked in billions of dollars selling ads. Targeted ads based on people's interests or behavior generally fetch higher fees.

ISPs "feel like they have data and they ought to be able to use it," says Tim McElgunn, chief analyst at Pike & Fischer Broadband Advisory Services. "They really desperately want to."

This isn't the first time ISPs have tried this. Two years ago, ISPs in the U.S. and Britain signed deals with companies offering deep packet inspection services and a cut of ad revenue.

Those pacts fell apart after a privacy outcry. In the U.K., an uproar ensued after BT Group PLC admitted it had tested Phorm's technology on some subscribers without telling them. Last year, BT and two other British ISPs that explored deploying Phorm's service—Virgin Media Inc. and TalkTalk—abandoned it.

#### More From the Series

- [A Web Pioneer Profiles Users by Name](#)
- [Web's New Goldmine: Your Secrets](#)
- [Personal Details Exposed Via Biggest Sites](#)
- [Microsoft Quashed Bid to Boost Web Privacy](#)
- [On Cutting Edge, Anonymity in Name Only](#)
- [Stalking by Cellphone](#)
- [Google Agonizes Over Privacy](#)
- [On the Web, Children Face Intensive Tracking](#)
- ['Scrapers' Dig Deep for Data on Web](#)
- [Facebook in Privacy Breach](#)
- [Insurers Test Data Profiles to Identify Risky Clients](#)
- [The Tracking Ecosystem](#)
- Follow [@whattheyknow](#) on Twitter
- [Complete Coverage: What They Know](#)

In the U.S., controversy erupted in 2008 over the practices of a company called NebuAd Inc., which planned to use deep packet inspection to deliver targeted advertising to millions of broadband subscribers unless they explicitly opted out of the service. At a congressional hearing, Bob Dykes, the company's founder, was grilled over its policy. NebuAd stopped doing business last year; several U.S. ISPs who signed deals with NebuAd have been hit with class-action lawsuits accusing them of "installing spyware devices" on their networks.

In an interview, Mr. Dykes said, "If I had to do things over again, I would have figured out how to architect an opt-in model."

The companies now offering ad services based on deep packet inspection believe they have learned how to make the services acceptable to privacy advocates and Internet users. This includes asking for permission up front and offering people incentives to receive targeted ads, such as Kindsight's free security service, which includes identity-theft protection. Customers can pay a monthly fee to receive no ads.

In Brazil, Phorm is emphasizing customized content on partner websites if people agree to opt in. For example, users visiting a sports website might see articles about their favorite teams (gleaned from an analysis of their surfing habits), providing an online experience different from other people.

"Receive your favorite content in an easy and practical way and without spending money!" says Oi's main opt-in screen for the Phorm service, called Navegador. "We guarantee your privacy! No personal information is input in the program, so your privacy is guaranteed!"

Oi's Mr. Ripper says more than half the subscribers offered the service in the initial launch have opted in to date. "We were very happy with it," he says. He says two outside auditors verified Phorm's privacy-protection settings.

Until 2007, Phorm was known as 121Media Inc. It delivered targeted ads, particularly pop-ups, to users who downloaded free software. The ads were "based on an anonymous analysis of their browsing behavior, which is likely to indicate their commercial and lifestyle interests," according to corporate filings.

Several Internet security companies, including Symantec Corp., flagged part of 121Media's adware system as "spyware." Microsoft's Malware Protection Center called it a "trojan," or malicious software disguised as something useful.

Facing "a combination of public perception and legal and technological challenges," 121Media said it shifted its focus in 2005 from the desktop-adware business to ISPs.

It eventually shuttered its adware business and renamed itself Phorm. The company is led by Mr. Ertugrul, a Princeton-educated, former investment banker who in the early 1990s formed a joint venture with the Russian Space Agency to offer joy rides to tourists in MiG-29 fighter jets. The venture was later sold.

In February 2008, Britain's biggest ISPs—BT, Virgin Media and TalkTalk—announced plans to implement Phorm's service. Those plans quickly

unraveled.

Suspicions earlier had arisen among some BT subscribers who discovered they were being routed through an unfamiliar Internet address when they tried to visit a website. Some of them contacted BT and were advised their computer might be infected with a virus, according to a person familiar with the matter.

A BT spokesman said it is "standard procedure" to take customers through "a number of steps to try and identify the issue" if they call with a question about their service.

In fact, the subscribers were part of tests BT conducted in 2006 and 2007 using Phorm's technology. When BT disclosed the testing in April 2008, the backlash was fierce, with online protests by privacy advocates and government investigations. Four members of the board of directors later resigned, including former AT&T chief executive David Dorman and ex-Coca-Cola Co. president Steven Heyer, citing differences with Mr. Ertugrul. Messrs. Dorman and Heyer declined to comment.

The three ISPs eventually bailed out. "Phorm was bad news," says David Smith, deputy commissioner of Britain's Information Commissioner's Office, which oversees data protection. He says he's not surprised Phorm is looking for clients abroad. "It was pretty clear that no one was going to touch them in the UK."

Kindsight's roots trace to an in-house project known as Project Rialto at Alcatel-Lucent, where Mr. Gassewitz once worked as a vice president of strategic planning.

A 2007 job posting on Project Rialto's website described the company's work as developing "systems that can handle [a] massive volume of data for in-depth analysis of user behavior to enable targeted advertising."

Project Rialto eventually became Kindsight, a spinoff. At an Alcatel-Lucent conference held in September 2008 in Beverly Hills, Mr. Gassewitz spoke at a session called "Merging Technology and Advertising." A summary of his comments, posted on Alcatel's website, reads in part: "Through technologies like deep packet inspection," Internet service providers "can gather even more information about consumers" than rivals such as Google or Facebook.

Mr. Gassewitz also talked about "significant privacy concerns," the summary says, and stressed that ISPs must find a way to provide measurable value to consumers "to avoid backlash."

To win over Internet users to its services, Kindsight plans to offer what it has described as a "free, always-on, always-up-to-date security service."

"Say hello to your new best friend..." it said on its redesigned website in 2008. The company later dropped the slogan. "That was early days," says Mr. Gassewitz.

Before giving away the security service free, Kindsight plans to display an opt-in screen to ISP users that explains how its technology analyzes "web sites visited and searches conducted to assign a numerical value to various interest categories." The "score" is used to deliver relevant ads.

In market-research tests in North America, France and the U.K., Kindsight found that about 60% of users were willing to take the service free in exchange for receiving targeted ads, he says. Another 10% were willing to pay for it.

Mr. Gassewitz says six ISPs have tested Kindsight's security service on subscriber groups as big as 200,000. Mr. Gassewitz says, "There was no profiling occurring, no advertising occurring, no data collection occurring."

Oi's Mr. Ripper believes that the technology's time has come. "The Internet is becoming more and more a platform to deliver very targeted messages," he says. As for deep packet inspection, "Everyone is going to get there. It's just a matter of timing."

**Write to** Steve Stecklow at [steve.stecklow@wsj.com](mailto:steve.stecklow@wsj.com) and Paul Sonne at [paul.sonne@wsj.com](mailto:paul.sonne@wsj.com)

---

### More From 'What They Know'

[A Web Pioneer Profiles Users by Name](#)

[Web's New Goldmine: Your Secrets](#)

[Personal Details Exposed Via Biggest Websites](#)

[Microsoft Quashed Bid to Boost Web Privacy](#)

[On Web's Cutting Edge, Anonymity in Name Only](#)

[Stalking by Cellphone](#)

[On the Web, Children Face Intensive Tracking](#)

[Google Agonizes Over Privacy](#)

['Scrapers' Dig Deep for Data on Web](#)

[Facebook in Privacy Breach](#)

[Insurers Test Data Profiles to Identify Risky Clients](#)

[The Tracking Ecosystem](#)

Follow [@whattheyknow](#) on Twitter

[Complete Coverage: What They Know](#)

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com)