Internet Providers' New Tool Raises Deep Privacy Concerns

By Rob Pegoraro
Thursday, August 21, 2008; D03

If you're reading this story on our Web site, I don't know what you did online before you reached this page.

But your Internet provider might if it engages in something called deep packet inspection.

That phrase may sound like what the Transportation Security Administration does to uncooperative airline passengers, but on the Internet it means a thorough and automatic inspection of online traffic -- not just where you've been but also what you've seen.

Peering inside the digital packets of data zipping across the Internet -- in real time, for tens of thousands of users at once -- was commercially impractical until recently. But the ceaseless march of processing power has made it feasible.

Unsurprisingly, companies have been trying to turn this potential into profit. By tracking users' Web habits this closely, they can gain a much more detailed picture of their interests -- and then display precisely targeted, premium-priced ads.

Equally unsurprising, these attempts have become a public-relations tar pit for Internet providers that experimented with this technology without giving users fair warning.

The House Committee on Energy and Commerce recently asked dozens of providers to explain whether they had done any such testing.

Most companies said they had yet to try the technology and had no plans to do so. (Although AT&T allowed that "if done properly," deep packet inspection "could prove quite valuable to consumers.")

A handful of providers -- for example, the Sprint spinoff Embarq and The Washington Post Co.'s Cable One -- said they briefly tested a deep-packet-inspection ad service provided by NebuAd, a start-up from Redwood City, Calif.

These companies said the tests guarded their customers' privacy. Cable One, for example, told the committee that it did not monitor encrypted Web traffic (such as bank transactions), e-mail, instant messages or Internet phone calls and said that NebuAd stripped out all personal references before analyzing those limited data.

The providers also said that were they to engage in deep packet inspection again, they would record data only from users who expressly allowed it.
Taking these companies at their word, what's there to worry about? We trade privacy for convenience all the time. We visit sites that keep far less detailed records of our comings and goings with "cookies" -- the small placeholder text files they drop on our hard drives. Millions of people subject themselves to more intensive scrutiny when they use Google's Gmail service, which scans the text of each message to place more relevant ads.

If deep packet inspection lives up to its promises, it might even yield a cash benefit. Internet providers using this technology could afford to offer customers a deal: Accept this scrutiny, and we'll knock $10 a month off your bill.

But systems such as deep packet inspection unnerve a lot of Internet users for sound reasons.

One is, of course, the immensely greater surveillance they allow. Tracking via cookies is the rough equivalent of a supermarket clerk noting that you spend a lot of time in Aisle 9 checking out cereal but never duck into Aisle 2 for frozen dinners. Deep packet inspection, by contrast, is more like the clerk following you to see which boxes of cereal you eyeballed -- and doing so at every store you visit, even those run by other companies.

Another concern is the difficulty of circumventing this constant tracking. You can tell your browser to reject the third-party cookies set by ad networks such as Google's DoubleClick, but the machinery of deep packet inspection hides out of reach in your provider's servers.

A third concern is the lack of competition for broadband service in much of the United States -- if your provider sets up deep packet inspection, you may not be able to protest by taking your business elsewhere.

But the worst aspect of this kind of "augmented" or "enhanced tracking" (pick a euphemism) is how badly and in how many ways it could fail.

What if a wrongly configured system records more data than intended?

What if these records aren't as anonymous as advertised? (Imagine how much your Web use would say about where you live, work and play -- even with all mentions of your name scrubbed out.)

What if the company running the inspections loses track of a laptop or a backup tape with these records?

What if businesses that feel threatened by the Internet, such as some record labels and movie studios, ask providers to use these inspection tools to screen for certain online activities?

What if government agencies make similar requests?

As an old saying goes, abuse of power comes as no surprise. But neither should neglect and carelessness.

Living with technology, or trying to? E-mail Rob Pegoraro at robp@washpost.com. Read more at http://blog.washingtonpost.com/fasterforward.