



ELECTRONIC FRONTIER FOUNDATION

Lee Tien, [tien@eff.org](mailto:tien@eff.org)  
(415) 436-9333 x 102David Sobel, [sobel@eff.org](mailto:sobel@eff.org)  
(202) 797-9009 x 104

## EFF's Concerns about Deep Packet Inspection (DPI) and Behavioral Advertising

Few entities in society pose as great a threat to personal privacy as one's Internet service provider (ISP). That's because your ISP has the means, motive, and opportunity to scrutinize nearly every communication departing from and arriving to your Internet-connected computer. The rise of "cloud computing"—which shifts more of people's computing from their home computers and networks to third-party computers on the Internet—will only make this problem worse.

- Opportunity:** Because your ISP serves as the gateway between your computer and the rest of the Internet, every e-mail message or IM you send and receive, every web page you visit and file you download, and every VoIP call you make travels through your ISP's routers.
- Means:** Ten years ago, your ISP couldn't efficiently analyze every communication traversing its network because computers were relatively slow and networks were relatively fast. Today, computers are fast enough to analyze those communications, and an entire industry—the deep-packet inspection industry—has emerged to provide ISPs with tools for massive, widespread automated surveillance.
- Motive:** Third parties are placing pressure on ISPs to spy on users in unprecedented ways. Advertisers are willing to pay higher rates for behavioral advertising. Furniture makers will pay more to place ads in front of people who have been recently surfing furniture websites. To enable behavioral advertising, companies like NebuAd and Phorm have been trying to convince ISPs to collect user web-surfing data that they do not collect today. Similarly, the copyrighted content industries seem willing to pay ISPs to detect, report, and possibly block the transfer of copyrighted works.

As a result, ISPs are scrutinizing more information--and different forms of information--than ever before. AT&T has begun to consider monitoring for copyright violations; Charter Communications signed up with NebuAd, sparking a firestorm of publicity and legislative interest that pushed Charter to abandon the deal; and a few British ISPs have begun to use Phorm's services.

### **Anonymization is no panacea.**

In 2006, AOL researchers released 20 million keyword searches submitted by hundreds of thousands of subscribers over a three-month period. Researchers had "anonymized" the data by replacing identifying information like AOL login IDs with another unique ID number—but any particular person's searches were all linked by that identifier. It turns out that knowing an unidentified person's search queries is often enough to breach his or her privacy. *See, e.g.,* Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006 (discovering an AOL user based on searches such as "landscapers in Lilburn, Ga" and several people with the same last name of the user). More advanced techniques for re-identification are available, *see e.g.* <http://33bits.org/2008/11/12/57>, and we urge the FTC to be skeptical of claims that personal data has been anonymized.

### **Opt-in consent is no guarantee**

Opt-in consent for ISP surveillance will likely mitigate some of these privacy problems in the immediate future. For such consent to be truly informed, however, ISPs must provide far more information about their DPI practices than has been seen thus far. Consumers cannot reasonably be expected to know about, and protect themselves from, DPI practices. *See, e.g.,* <http://arstechnica.com/news.ars/post/20080724-06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy.html>. And even if consumers opt out of the creation of behavioral profiles for use in delivering ads, they may not be opting out of the copying or inspection of their communications.