
Watch Your Back for ISP-Targeted Ads

Kelly D. Talcott
New York Law Journal
April 17, 2008

Internet access is a necessity for all but the tiniest businesses. Most connect online via Internet service providers, which typically offer standard terms and conditions as part of a package of services directed to business users. These agreements are frequently ignored, but deserve closer attention.

Many ISPs reserve broad rights to monitor not only how much of an ISP's bandwidth their customers are using, but also what customers are doing with that bandwidth. Businesses need to be aware to what extent their ISPs have reserved these rights, and in certain cases may want to modify their online activities because of the level of access ISPs reserve for themselves.

Until recently, disclosures by ISPs of detailed information about a user's Internet access habits, such as what sites were visited or the contents of e-mails that were sent, were limited to aiding law enforcement efforts. There are, however, new advertising delivery tools that some ISPs are incorporating into their systems that take advantage of the ISP's ability to have significant access to information about customer behavior.

These tools deliver targeted ads to the ISP's customers based on the customer's monitored Web use, and seek to leverage information about a customer's browsing habits. While current providers of these tools claim they are careful to maintain individual users' anonymity, as the tools become more prevalent it will become increasingly important to pay close attention to whether and how they protect customer information.

A typical agreement between a business customer and an ISP will make it clear that, while the ISP has no obligation to monitor the content that passes to and from the customer, it nonetheless has the right to do so. It will also reserve the right for the ISP to disclose the information it gathers to comply with the law or for a wide variety of business-related purposes.

These broad rights have paved the way for these new advertisement-delivery services that piggyback on the ISP's reserved right to monitor use and that attempt to deliver finely targeted ads to users based on their perceived interests. To determine what those interests are, these services monitor in detail what the users are transmitting to and receiving back from the Internet.

Two such services are Phorm and NebuAd. Phorm is perhaps the more recently notorious of the two, due to a series of discussions and tests conducted with ISPs in the United Kingdom that have caused British privacy advocates some concern. Both Phorm and NebuAd work from within the ISP and attempt to monitor, with some exclusions, all Web pages that each of the ISP's customers visit as well as the search terms those customers use. They use various proprietary means to correlate the information they gather about a customer's surfing habits with ads that are likely to interest them.

Phorm generates its own identifying script, or cookie, that it attaches to requests coming from customers' computers. It works at the individual computer level, using this cookie to build a profile of information about Web sites accessed by that computer as well as the information delivered by the accessed sites. This information in turn is used to provide ads to that computer that, in theory, are consistent with the interests of the user.

NebuAd provides a similar service, but works at the Internet Protocol address level. NebuAd tracks user behavior coming from that IP address, which for an IP address that is shared by more than one computer may be a composite of the searches being conducted by that set of computers. The NebuAd system records not only the addresses of Web pages visited, but also the search terms that were used and the keywords associated with the returned pages. This allows NebuAd to categorize the users' behavior in a way that facilitates delivery of targeted ads.

There are a number of benefits to these systems. Advertisers benefit because, in theory, their ads are reaching a higher percentage of consumers who may respond by making a purchase. Consumers benefit because they are receiving ads that are more likely to be of interest to them. ISPs benefit because advertisers are willing to pay a higher rate for ads that are better targeted. With such benefits all around, the practice of monitoring and leveraging the details of how people are using the Internet is going to increase.

On the other hand, the very idea of these information mining systems generates significant questions about privacy and the potential for abuse. It is one thing for ISPs to retain the right to monitor how their customers are using the Internet; it is another when that right is exercised.

Both Phorm and NebuAd take great pains to assure that the user's privacy is respected. Phorm employs an "anonymizer" that assigns a random number to the computer being tracked. In addition, according to Phorm's Web site, it will not view any information on secure pages; it ignores strings of numbers longer than three digits to minimize the chance of collecting credit

card, phone or Social Security numbers; it does not store IP addresses or browsing or search histories; and it does not integrate with systems (like the ISP's log-in system) that could identify the user.

NebuAd makes similar promises, and in addition, its CEO recently stated in an interview that it does not monitor Web behavior in certain sensitive categories, such as those relating to health or sex.

That may satisfy many users as far as Phorm or NebuAd are concerned. For businesses and individuals who have strong privacy concerns, however, even these assurances may not be enough. And given the terms of use in place with most ISPs, there is nothing to prevent another information mining service from being put in place that may collect even more sensitive information than do Phorm or NebuAd.

The problem is not an abstract one. Information has value, and collected information can have substantially more value than discrete bits of information. As that value increases, so does the potential for abuse. Fifty thousand hospital patient records -- a class of information that is supposed to be highly protected from disclosure -- were recently stolen, allegedly by an employee of the hospital, apparently to be sold to identity thieves. State Department employees were caught looking at the passport records of presidential candidates. As more personal information is collected, the temptation for insiders to take and exploit that information will increase.

ATTENTION VIGILANCE

The answer, as it is with so many privacy-related questions, is attention and vigilance. Internet users need to read and think about the privacy implications of their ISP's terms of service, acceptable use and privacy policies. When an ISP introduces a new service that claims to personalize the browsing experience (that's the key promise), users must make a real effort to determine what type of personal information that service is collecting and how it works.

If the ISP does not provide the user with the ability to "opt out" of the experience, then it may be time to change ISPs. Ideally, the feature requires an affirmative decision by the user to "opt in," since many users will not pay attention to ISP notices.

Even where the user can opt not to take advantage of the information mining service, the question that will remain is whether the service will monitor user behavior anyway. Unfortunately, to answer this question one may need to know more about the structure of the information mining system than either the ISP or the information mining service may be willing to disclose.

E-mail is one area where businesses can take immediate action to enhance privacy. The time may be approaching, if it is not here already, where businesses that regularly transmit sensitive information over the Internet need to consider encrypting those messages. There are a number of methods of encrypting e-mails, some more complex and secure than others. While they add a layer of complexity to the communications process, where a business is relying on keeping its

communications in confidence -- and may have contractual obligations to do so -- such systems may be well worth the expense and aggravation.

Kelly D. Talcott, a partner in the New York office of K&L Gates, practices intellectual property and technology law.

RELATED LINKS

ISP Contracts: Be Careful What You Sign

Do Behavioral Ads Endanger Your Privacy?