Internet Search Terms: Embedded Privacy Issues

THOMAS R. BURKE

Reaction to subpoenas issued by the Justice Department to commercial search engines has highlighted privacy issues surrounding their growing popularity. The controversy is educating users about information Web site owners collect about their users and may invariably lead to subpoenas being issued to any Web site offering a search function.

In its ongoing defense of a federal anti-pornography law, in August 2005, the U.S. Justice Department issued subpoenas to the major private search engine companies asking them to produce, among other things, millions of records involving search terms entered by users.[1] Although the subpoenas have drawn criticism by civil libertarians and privacy advocates, the department's subpoenas did not seek information linking search terms with the users' identities.[2] Users' computer Internet Protocol (IP) addresses were not requested. Google objected to the Justice Department's request largely on the grounds that compliance would jeopardize its trade secret information. Google also insisted that the requests threatened its users' privacy rights—a stance that the American Civil Liberties Union ("ACLU") has echoed in papers filed in support of Google's opposition. Defending its subpoenas, the Justice Department insists that the data is necessary to evaluate the effectiveness of technology currently available to screen online users from pornographic materials.

Thomas R. Burke is a partner with Davis Wright Tremaine LLP in San Francisco and a member of the firm's Privacy and Security practice group. Mr. Burke's Internet practice concentrates on content liability and privacy issues. Mr. Burke can be reached at *thomasburke@dwt.com*.

This article appeared in Vol. 1, No. 5, (April 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

Google publicly announced it would resist the Justice Department's subpoena in January, at a time of growing public criticism of the Bush administration's domestic surveillance activities, including congressional debate over renewal of controversial portions of the U.S. Patriot Act. Indeed, in response to the department's subpoenas, U.S. Senator Patrick Leahy (D - Vt.) asked U.S. Attorney General Alberto R. Gonzales to explain what information was being requested and how the federal government would use it. Senator Leahy declared the government's collection and use of the information created "the specter of excessive government surveillance that may intrude upon important privacy interests and chill the exercise of First Amendment-protected speech and associational rights."[3] It is the concern about the government's interest in Internet search information - the perception that Americans' Internet searches may become a tool of government surveillance—that is the source of much concern.

The situation raises several important Internet privacy issues:

- To what extent can personal information currently be linked to a user's Internet search activities?
- What privacy expectations do Internet users hold regarding their Internet search activities?
- What steps can Internet users take to protect their online search activities?
- What policies or laws currently govern access to a users' online search activities?

INFORMATION WEB SITES LEARN ABOUT THEIR USERS

Virtually every Web site owner has analytical tools that reveal a variety of information about their users available to them, including the Web site address that the user came from (and that the user is leaving to), what internal pages are viewed, as well as the search terms a user has entered during a visit to the site.[4] Most Web site owners keep track of this information because it tells them how visitors found their Web site and what they are interested in reading. However, unless the user is required to register with the site or makes an online purchase while vis-

This article appeared in Vol. 1, No. 5, (April 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

iting the site, the only identifying information that will be collected by the Web site is the unique IP address of the user's computer. Although this information can ultimately be linked to an individual, it does not, on its face, reveal information that personally identifies the individual making the online search.

The situation is, however, quite different for Web sites in which user registration is required. On these sites, a user's search term information can potentially be linked to any personally identifying information the user has volunteered—assuming the information is not bogus—including the user's e-mail address, name, date of birth, mailing address, phone number, and credit card information. Most commercial Web sites will also transmit a "cookie" file to the user's computer—the method by which an Internet user's repeat experience with a Web site becomes customized—that also allows the Web site to track the user's visits to the site. However, a user need not accept a cookie file to use a search engine. Google, for example, allows users to reject cookie files.[5] Web sites will also embed the search terms used by a user into the Internet address (referred to as the uniform resource locators ("URLs") of Web sites that a user ultimately visits. This "referrer" information is also invaluable to Web sites because it allows them to learn how users got to their site. Again, Google and other search engines disclose this practice and allow users to opt out of providing such information.[6]

PRIVACY EXPECTATIONS OF AMERICANS AND THEIR INTERNET SEARCHES

A national survey of 800 Americans conducted by the Center for Survey Research at the University of Connecticut recently found that 60 percent opposed the storage of users' search queries, while 32 percent of those surveyed were not opposed.[7] Of those surveyed, 65 percent felt that the government should not monitor the Internet searches of "ordinary Americans"—46 percent of the respondents said that they "strongly" opposed such monitoring—and only 30 percent said the government should be involved. Once again, the partisan beliefs

that surround this issue is reflected by the survey's finding that 67 percent of Democrats believe that the companies should not turn over search information to the government, compared to 30 percent of Republicans.[8]

Eighty-five percent of the respondents in the Connecticut survey also reported that they haven't searched for a Web site using a word or phrase that they wouldn't want others to know about, while only 13 percent expressed this concern. Of course, few users are like the North Carolina man who prosecutors say searched for the words "neck," "snap," "break," and "hold" shortly before killing his wife,[9] but they may not be entirely candid when surveyed about their online search habits. At bottom, undoubtedly many people who search online are comfortable with the trade-off—whatever personal information their search might reveal is worth the free and instantaneous information they receive.

MASKING THE IDENTITY OF AN INDIVIDUAL'S SEARCH TERMS

There are few fool-proof options available to users who want to remain completely anonymous while conducting an online search. Anonymizing software is available that allows an individual to surf the Internet—and conduct Internet searches—without disclosing their computer's unique IP address.[10] However, even using this software, unless all of the user's information remains encrypted, an individual's online activities can still potentially be monitored through his or her Internet Service Provider (ISP). Quite apart from data that might be subpoenaed from a commercial search engine, depending on the terms of the user's privacy agreement with his or her ISP, this same user data can also be mined and marketed by other private companies. Consequently, these commercial companies are also potentially ripe for subpoena requests for users' search-term data. In short, because the information that a user sends through the Internet is captured and potentially stored by a variety of systems that are interconnected, there is currently no easy solution that ensures the complete privacy of a user's online search activities.

This article appeared in Vol. 1, No. 5, (April 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

POLICIES AND LAWS REGULATING ACCESS TO AND USE OF USER'S SEARCH-TERM INFORMATION

Web sites are restricted in how they use data collected from their users by the promises they make in their privacy policies. If a privacy policy is posted online—and in California, by law, commercial Web sites that collect personal information on California residents are required to "prominently post" such a policy[11]—the Federal Trade Commission is empowered to enforce the policy's terms.[12] Nevertheless, in a privacy policy, a Web site owner need only disclose what the Web site owner does with a visitor's data. Providing the user agrees to the terms of the policy, there is no legal prohibition, per se, against selling or sharing search-term information that a user has consented to be disclosed.

Although some Web sites promise not to share any "personally identifiable" data with others without the user's consent, many other commercial sites disclose that such data is shared with other companies, unless the individual user expressly opts not to provide such information. Users whose information is governed by the European Directive on Data Protection enjoy greater privacy rights. Virtually every commercial Web site now offers a search engine function that is capable of generating search-term data. Owners of all Web sites - as well as the vendors they do business with—should anticipate that this user search information will increasingly be subject to discovery requests by lawyers involved in civil and criminal disputes.

In February 2006, U.S. Representative Ed Markey (D - Mass) introduced legislation that would impose European-style privacy regulations to every Web site in the United States. Representative Markey's bill, H.R. 4731, the Eliminate Warehousing of Consumer Internet Data Act of 2006, would force all Web sites in the United States to delete users' personal information, defined as "information that allows a living person to be identified individually."[13] However, currently nothing in this legislation seeks to explicitly regulate a user's search terms or Internet addresses.

A legal argument in Google's dispute with the Justice Department offers an additional potential legal protection for users' search terms. In its dispute with the Justice Department, Google contends that the

This article appeared in Vol. 1, No. 5, (April 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

Electronic Communications Privacy Act ("ECPA")[14] protects its users' search terms from disclosure without a court order.[15] In its Opposition to the Government's Motion to Compel, Google argues that its users' ability to initiate recurring searches and to have those results sent to their e-mail accounts triggers the protections of ECPA which regulates any service that "provides users thereof the ability to send or receive wire or electronic communications." Google distinguishes its operations from other commercial Web sites in which users do not have the same ability to communicate.[16]

If Google's interpretation of ECPA is accepted, the Justice Department's subpoena may be quashed because the procedures outlined in Section 2703 require information to be withheld absent the users' consent, or in response to a search warrant or a court order. Because Google's dispute arises in the context of a third-party subpoena issued by the Justice Department's Civil Division in a civil lawsuit, the district court's ruling on this issue will be closely watched by lawyers who increasingly issue subpoenas in cases to obtain access to individuals' online searches.

CONCLUSION

Concern by Americans about the domestic surveillence activities of their government is likely to continue to have a strong influence on whether government inquiries into Internet users' search terms will be tolerated and whether additional legal safeguards will be enacted. Given the increasing popularity of search engine technology, many of the legal issues faced by the commercial search engines are no different that what other Web site operators offering a search function will soon encounter. As more and more social and commercial activities move online, Web site owners will increasingly encounter more third-party demands for their users' data.

NOTES

[1] A copy of the U.S. Justice Department's subpoena issued to Google is *available at* http://news.com.com/Feds+take+porn+fight+to+Google/2100-1030_3-6028701.html?tag=nl.

This article appeared in Vol. 1, No. 5, (April 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

[2] See Dan Mitchell, "WHATS ONLINE; The Crumbs You Leave Behind," *The New York Times*, January 28, 2006, Section C, page 5.
[3] *See* http://leahy.senate.gov/press/200601/012506.html.
[4] *See* www.clicktracks.com.
[5] *See* www.google.com/privacy_faq.html#cookie.
[6] *See* www.google.com/intl/en/privacy_faq.html#personalinfo ("Some Google services (such as Google Toolbar) enable you to opt in or opt out of sending URLs to Google, while for others (such as Google Web Accelerator) the sending of URLs to Google is intrinsic to the service. When you sign up for any such service, you will be informed clearly that the service sends URLs to Google, and whether and how you can opt in or opt out.").
[7] *See* http://www.uconn.edu/newsmedia/2006/February/rel06011.html. In another poll conducted by the Ponemon Institute, a privacy research group documented users' concerns about personal search data falling into the hands of the government. *See* http://www.computerworld.com/security-topics/security/privacy/story/0,10801,107993,00.html. According to the Computerworld report, "89 percent of respondents to the Ponemon poll believe that their Web searches are kept private, and 77 percent believe that Google Web searches do not reveal their personal identities."
[8] *Id.*
[9] *See* www.wral.com/print/528726/detail.html.
[10] *See*, *e.g.*, www. tor.eff.org; www.anonymizer.com; www.steganos.com; www.the-cloak.com.
[11] *See* Cal. Bus. & Prof. Code §§ 22575-22579.
[12] 15 U.S.C. § 57a(a)(1)(B).
[13] *See* http://www.govtrack.us/congress/bill.xpd?bill=h109-4731.
[14] 18 U.S.C. §§ 2701-2712.
[15] *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Dep't of Justice, Computer Crime and Intellectual Property Section Criminal Division (July 2002), *available at* www.Cybercrime.gov/s&smanual2002.htm.
[16] *See Crowley v. Cyberspace Corp.*, 166 F. Supp.2d 1263, 1270 (N.D. Cal. 2001); *In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp.2d 310 (E.D.N.Y. 2005).

This article appeared in Vol. 1, No. 5, (April 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,