THE WALL STREET JOURNAL.

The Great Privacy Debate

It's Modern Trade: Web Users Get as Much as They Give

iStock Photo

By Jim Harper
Updated Aug. 7, 2010 12:01 a.m. ET

If you surf the web, congratulations! You are part of the information economy. Data gleaned from your communications and transactions grease the gears of modern commerce. Not everyone is celebrating, of course. Many people are concerned and dismayed—even shocked—when they learn that "their" data are fuel for the World Wide Web.

Who is gathering the information? What are they doing with it? How might this harm me? How do I stop it?

These are all good questions. But rather than indulging the natural reaction to say "stop," people should get smart and learn how to control personal information. There are plenty of options and tools people can use to protect privacy—and a certain obligation to use them. Data about you are not "yours" if you don't do anything to control them. Meanwhile, learning about the information economy can make clear its many benefits.

The Great Privacy Debate

Americans are being tracked online in new and sophisticated ways. A debate on the risks and rewards, following the Journal's What They Know investigation.

- **Nicholas Carr: The Dangers of Web Tracking**
- **Firms Resist Privacy Regulation**

It's natural to be concerned about online privacy. The Internet is an interactive medium, not a static one like television. Every visit to a website sends information out before it pulls information in. And the information Web surfers send out can be revealing.

Most websites track users, particularly through the use of cookies, little text files placed on Web surfers' computers. Sites use cookies to customize a visitor's experience. And advertising networks use cookies to gather information about users.

A network that has ads on a lot of sites will recognize a browser (and by inference the person using it) when it goes to different websites, enabling the ad network to get a sense of that person's interests. Been on a site dealing with SUVs? You just might see an SUV ad as you continue to surf.

Most websites and ad networks do not "sell" information about their users. In targeted online advertising, the business model is to sell space to advertisers—giving them access to people ("eyeballs") based on their demographics and interests. If an ad network sold personal and contact info, it would undercut its advertising business and its own profitability.

Some people don't like this tracking, for a variety of reasons. For some, it feels like a violation to be treated as a mere object of commerce. Some worry that data about their interests will be used to discriminate wrongly against them, or to exclude them from information and opportunities they should enjoy. Excess customization of the Web experience may stratify society, some believe. If you are poor or from a minority group, for example, the news, entertainment and commentary you see on the Web might differ from others', preventing your participation in the "national" conversation and culture that traditional media may produce. And tied to real identities, Web surfing data could fall into the hands of government and be used wrongly. These are all legitimate concerns that people with different worldviews prioritize to differing degrees.

"Surreptitious" use of cookies is one of the weaker complaints. Cookies have been integral to Web browsing since the beginning, and their privacy consequences have been a subject of public discussion for over a decade. Cookies are a surreptitious threat to privacy the way smoking is a surreptitious threat to health. If you don't know about it, you haven't been paying attention.

But before going into your browser settings and canceling cookies, Web users should ask another question about information sharing in the online world. What am I getting in return?

The reason why a company like Google can spend millions and millions of dollars on free services like its search engine, Gmail, mapping tools, Google Groups and more is because of online advertising that trades in personal information.

And it's not just Google. Facebook, Yahoo, MSN and thousands of blogs, news sites, and comment boards use advertising to support what they do. And personalized advertising is more valuable than advertising aimed at just anyone. Marketers will pay more to reach you if you are likely to use their products or services. (Perhaps online tracking makes everyone special!)

If Web users supply less information to the Web, the Web will supply less information to them. Free content won't go away if consumers decline to allow personalization, but there will be less of it. Bloggers and operators of small websites will have a little less reason to produce the stuff that makes our Internet an endlessly fascinating place to visit. As an operator of a small government-transparency web site, WashingtonWatch.com, I add new features for my visitors when there is enough money to do it. More money spent on advertising means more tools for American citizens to use across the web.

Ten years ago—during an earlier round of cookie concern—the Federal Trade Commission asked Congress for power to regulate the Internet for privacy's sake. If the FTC had gotten authority to impose regulations requiring "notice, choice, access, and security" from websites—all good practices, in varying measure—it is doubtful that Google would have had the same success it has had over the past decade. It might be a decent, struggling search engine today. But, unable to generate the kind of income it does, the quality of search it produces might be lower, and it may not have had the assets to produce and support all its fascinating and useful products. The rise of Google and all the access it provides was not fated from the beginning. It depended on a particular set of circumstances in which it had access to consumer information and the freedom to use it in ways that some find privacy-dubious.

Some legislators, privacy advocates and technologists want very badly to protect consumers, but much "consumer protection" actually invites consumers to abandon personal responsibility. The *caveat emptor* rule requires people to stay on their toes, learn about the products they use, and hold businesses' feet to the fire. People rise or fall to meet expectations, and consumer advocates who assume incompetence on the part of the public may have a hand in producing it, making consumers worse off.

If a central authority such as Congress or the FTC were to decide for consumers how to deal with cookies, it would generalize wrongly about many, if not most, individuals' interests, giving them the wrong mix of privacy and interactivity. If the FTC ruled that third-party cookies required consumers to opt in, for example, most would not, and the wealth of "free" content and services most people take for granted would quietly fade from view. And it would leave consumers unprotected from threats beyond their jurisdiction (as in Web tracking by sites outside the United States). Education is the hard way, and it is the only way, to get consumers' privacy interests balanced with their other interests.

But perhaps this is a government vs. corporate passion play, with government as the privacy defender. The Journal reported last week that engineers working on a new version of Microsoft's Internet Explorer browser thought they might set certain defaults to protect privacy better, but they were overruled when the business segments at Microsoft learned of the plan.

Privacy "sabotage," the Electronic Frontier Foundation called it. And a Wired news story says Microsoft "crippled" online privacy protections.

Getty Images

But if the engineers' plan had won the day, an equal, opposite reaction would have resulted when Microsoft "sabotaged" Web interactivity and the advertising business model, "crippling" consumer access to free content.

The new version of Microsoft's browser maintained the status quo in cookie functionality, as does Google's Chrome browser and Firefox, a product of the nonprofit Mozilla Foundation. The "business attacks privacy" story doesn't wash.

This is not to say that businesses don't want personal information—they do, so they can provide maximal service to their customers. But they are struggling to figure out how to serve all dimensions of consumer interest, including the internally inconsistent consumer demand for privacy along with free content, custom Web experiences, convenience and so on.

Only one thing is certain here: Nobody knows how this is supposed to come out. Cookies and other tracking technologies will create legitimate concerns that weigh against the benefits they provide. Browser defaults may converge on something more privacy-protective. (Apple's Safari browser rejects third-party cookies unless users tell it to do otherwise.) Browser plug-ins will augment consumers' power to control cookies and other tracking technologies. Consumers will get better accustomed to the information economy, and they will choose more articulately how they fit into it. What matters is that the conversation should continue.

—Jim Harper is director of information policy studies at the Cato Institute.

Jim Harper is the Web master of *WashingtonWatch*, a site that tracks federal spending; the editor of *Privacilla*, a Web-based think tank; and the director of information policy studies at the Cato Institute in Washington, DC. He is also a founding member of the Data Privacy and Integrity Advisory Committee for the Department of Homeland Security. Harper studied political science at the University of California at Santa Barbara and in 1994 received a law degree from Hasting College of the University of California. His articles about privacy and security have appeared in *Administrative Law Review*, the *Minnesota Law Review*, the *Hastings Constitutional Law Quarterly*, the *Blaze*, and the *Technology Liberation Front*. He has also published two books: *Identity Crisis: How Identification Is Overused and Misunderstood* (2006) and *Terrorizing Ourselves: Why US Counterterrorism Policy Is Failing and How to Fix It* (2010), coedited with Benjamin H. Friedman and Christopher A. Preble. As an expert in the legal complications surrounding new technologies, Harper has testified at several congressional hearings and lectured widely.