likelihood, be comprehensively destroyed. WikiLeaks will vanish.

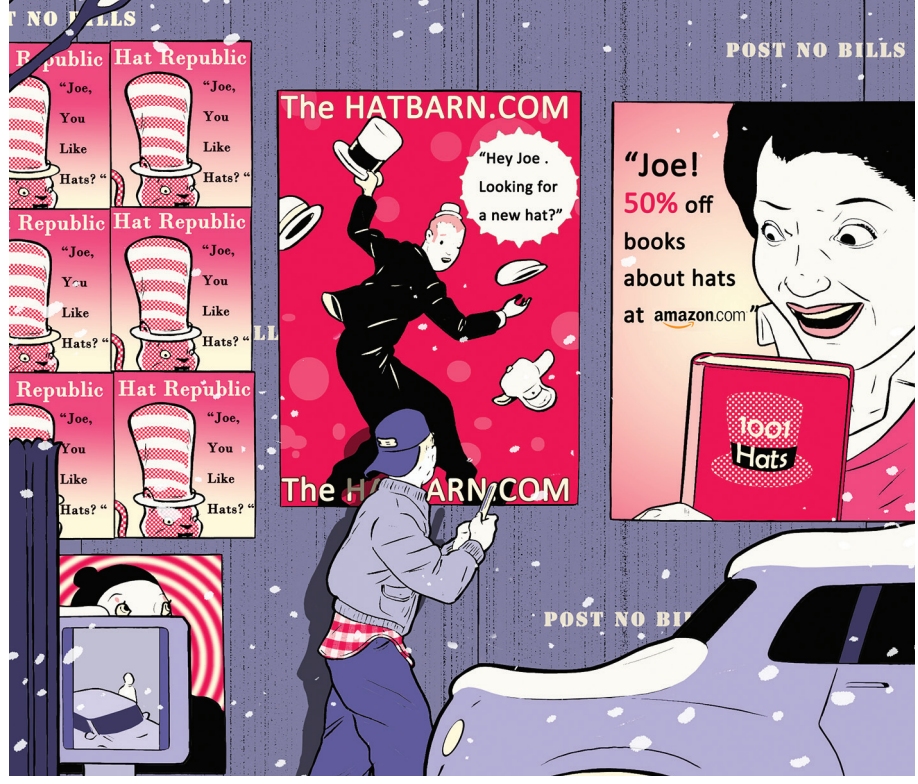
Once imagined, however, the technology of WikiLeaks cannot be forgotten and can easily be imitated. Other organizations, less radically activist, will create secure drop boxes for anonymous leaking. Already, the disgruntled former WikiLeaks volunteer, Daniel Domscheit-Berg, has said he will create a less threatening platform called OpenLeaks. It will, he says, publish nothing but, instead, function as a pipeline where sources designate the media organization to which they wish to leak: "We want to be a neutral conduit. That's what's most politically sustainable." Still more leak platforms are sprouting, including GreenLeaks, which will publish "information of environmental significance"; Brussels Leaks, which will expose the European Union; and Rospil, which will uncover Russia's secrets.

Predictably, media organizations want to replicate WikiLeaks's secure drop box, too. Recently, Al Jazeera launched a "Transparency Unit," which encourages its audience to submit "all forms of content" for "editorial review and, if merited, online broadcast and transmission on our English and Arabic-language broadcasts." The first product came in January, when Al Jazeera published the "Palestine Papers," 11 years' worth of secret documents created by the Palestinian Authority, describing negotiations with the Israeli government. The impression that emerges from them is that the Israeli government is no longer interested in securing a Palestinian state: it is a scoop that could not have existed without the Transparency Unit's drop box. Now other publications are considering their own. Bill Keller, the executive editor of the *New York Times*, is pondering how he can make it easier for sources to leak to his journalists.

WikiLeaks may not be with us for the long haul, but others will imitate its innovations, and they are likely to be more constrained and more responsible. tr

JASON PONTIN IS *TECHNOLOGY REVIEW*'S EDITOR IN CHIEF.

JASON SCHNEIDER



PRIVACY

How to Stop the Snoopers

Getting advertisers to quit tracking you may be harder than you think.

By SIMSON L. GARFINKEL

Most of us depend on free Web services, from Google searches to Facebook updates. Unless you're careful, though, using them has a price: your privacy. Web advertising pays for almost all such services, and this business has become very efficient, delivering ads to grab your attention. That requires tracking who you are and what you do online. Your Web browser reveals a surprising amount about you, and advertisers are keen to find out even more.

The government's principal consumer protection agency, the Federal Trade Commission, has taken the first major step toward addressing this situation with a new draft report that recommends the creation of a "Do Not Track" mechanism that would let Internet users choose, with the click of a button, whether to allow advertisers to track them online. This would offer better privacy controls than exist currently. But ultimately, the FTC's approach falls short of what's needed. That's because tracking technology is interwoven into our most popular websites and mobile services. Without tracking, they simply don't work.

Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers
Preliminary FTC staff report
December 2010

Few people realize that many of today's Web ads are tailored using huge amounts of personal data collected, combined, and cross-referenced from multiple sources—an approach known within the industry as "behavioral advertising." This tracking goes far beyond offering product recommendations based on your purchase history. Behaviorally targeted ads reflect which sites you have visited over the past month (or longer) and what you've done on those sites. Web advertisers employ a bewildering variety of tracking technologies. Perhaps the best-known involves small text files, or "cookies," that are invisibly downloaded to your computer when you visit a site; other sites then access the cookies to determine where you've been. This can provide advertisers with clues to where you live, where you work, which sports teams you follow, which TV shows

you watch. Advertisers can then refine their ads accordingly.

Behavioral advertising works. Two years ago a team of scientists at Microsoft Research Asia and two Chinese universities analyzed 17,901 Web advertisements shown to more than six million search-engine users over a seven-day period in June 2008. They found that users were up to seven times likelier to click on behaviorally targeted ads. It's hardly surprising, then, that these ads earn much more for websites—an average of $4.12 per thousand views versus $1.98 per thousand for regular ads, according to a study of 2009 data commissioned by the Network Advertising Initiative, a trade group that promotes self-regulation.

There's just one problem: most people find the very idea of behavioral advertising offensive—at least, they do once they learn it's happening. A recent survey of 1,000 U.S. adults conducted by professors at the University of Pennsylvania and the University of California, Berkeley, found that 73 percent of respondents thought it was "not okay" for advertisers to tailor ads on a website according to what they did on that site. And 84 percent said it was "not okay" for the advertisements they saw on one website to reflect what they had done on another site.

While many are simply opposed on principle to unrestricted tracking, there are real risks to data aggregation that we are just beginning to understand. Without safeguards, the tracking techniques used by advertisers could be exploited to steal identities or to devise ways to hack into computers. And the big databases that advertisers are building could be misused by unscrupulous employers or malicious governments.

Over the past 15 years the United States has developed a peculiar approach to protecting consumer privacy. Companies publish detailed "privacy policies" that are supposed to explain what information they collect, how, and what they plan to do with it. Consumers can then choose whether they want to provide their information—and they're welcome to avoid certain websites entirely.

The FTC draft report says that this model no longer works (if it ever did). "Many companies are not disclosing their practices," FTC chairman Jon Leibowitz said at a press conference in December when the report was released. "And even if companies do disclose them, they do so in long, incomprehensible privacy policies and user agreements that consumers don't read, let alone understand." Behavioral advertising makes this notion of "choice" even more dubious, since information collected on one site may be used on countless others.

The FTC is trying to rein this in. It recommends, for example, that companies collect information only when there is a legitimate business need to do so, and asks them to destroy that information when they no longer need it. But many U.S. companies operate the opposite way: collect everything possible and store it indefinitely in the hope that the data might prove useful someday.

The report says that companies need to do a better job of explaining their policies to consumers. One possible alternative to lengthy and hard-to-read privacy notices would be a simplified "privacy label," modeled on nutrition labels. A privacy label would present a website's policies in an easy-to-understand, easy-to-compare format. But requiring privacy labels on commercial websites would probably require an act of Congress—something that seems unlikely to happen.

Of course, real choice requires more than just clear information—it also requires options. At the moment, that means taking measures such as activating the "private browsing" mode built into modern Web browsers (which prevents sites from accessing cookies) or using browser plugins that automatically block advertisements and certain tracking technologies.

But there is no rule that says advertisers can't employ their own measures to circumvent private-browsing modes, and many are doing so. Browsers can be "fingerprinted," using their unique settings, allowing tracking without cookies. Advertisers can even sniff the history directly out of your

browser, by exploiting the way Web links are displayed in a different color once they have been clicked. Last summer, researchers at Stanford University's Security Lab presented a paper comparing the private-browsing modes of the four most popular Web browsers: Internet Explorer, Firefox, Chrome, and Safari. They found ways to defeat these modes, including a new type of cookie that can be accessed via Adobe's ubiquitous Flash plug-in—meaning that "private" browsing is never really private.

The FTC's solution to this problem is "Do Not Track." The idea is loosely modeled on the agency's popular "Do Not Call" list. Instead of a centralized list of consumers who don't want to be tracked, however, the report envisions a browser setting that would transmit an anonymity request to Web advertisers. If behaviorally targeted advertisements really are beneficial to consumers, most people will leave the feature switched off. Otherwise, websites better get used to $1.98 per thousand ads viewed.

Browser makers have started building tracking controls for their software. Google recently released an add-on for Chrome called Keep My Opt-Outs, and Microsoft has announced a similar feature for Internet Explorer 9 called Tracking Protection. Mozilla promises to add similar functions to Firefox. These features all tell websites when someone doesn't want to be tracked. But it's still up to companies to honor this request. And, unsurprisingly, the idea of "Do Not Track" is fiercely opposed by the advertising industry, which warns it would hamstring a booming business—especially if enabled in browsers by default.

The real problem with "Do Not Track," however, is that it derives from an earlier understanding of Web advertising—that ads are distributed by advertising networks to news sites, search engines, and other destinations that don't necessarily need to know who you are. Nowadays many popular websites are unusable unless you let them track you.

Take Facebook: the site has seen explosive growth in advertising revenue precisely because it tracks its users' interests in great detail. There's no way to turn off tracking and still let your friends see your status updates. Thanks to Facebook Connect, which lets you log on to other websites with your Facebook credentials, and the "Like" button, which sends links from external Web pages back to your Facebook profile, Facebook now tracks you across the Web. Or, more accurately, you tell Facebook where you are.

Smart phones will accelerate this trend. Already, many phone apps deliver ads based on your GPS-determined position. Future ads might depend on the applications that you've installed, whom you've called, even the contents of your address book—all information that's there for the taking. With the popular geography-based social-network game Foursquare, the only way to avoid tracking is not to play.

There is a way to resolve this conundrum, and it's disappointing that the FTC report ignores it. The report recommends continuing to try to limit what information companies can get, instead of limiting what they can do with information once they have it. In this age of Facebook, Google, and Foursquare, what we actually need are simple and enforceable policies limiting the retention and use of consumer data. These could be dictated by the government or, conceivably, built into browsers so that users could decide on the specifics. For example, you could tell Google that it may archive your searches forever, to help improve its service, but that it has to anonymize them after six months. You could tell Facebook it can keep your posts indefinitely but can use them for advertising purposes only for a year.

Unfortunately, any kind of reform will face stiff opposition from vested interests. But if the government wants to defend us from privacy-trampling advertising, it needs more than "Do Not Track": it needs to consider limitations on the use of Web data. tr

SIMSON L. GARFINKEL IS A RESEARCHER AND AUTHOR BASED IN ARLINGTON, VIRGINIA. HIS RESEARCH INCLUDES WORK ON COMPUTER FORENSICS, PRIVACY, AND PERSONAL INFORMATION MANAGEMENT. HE IS A CONTRIBUTING EDITOR TO *TECHNOLOGY REVIEW*.