THE PROGRESS & FREEDOM FOUNDATION

Progress Snapshot

Volume 4, Issue 19 September 2008*

Online Advertising & User Privacy: Principles to Guide the Debate

by Berin Szoka & Adam Thierer

Since the fall of 2008, a debate has raged in Washington over "targeted online advertising," an ominous-sounding shorthand for the customization of Internet ads to match the interests of users. Not only are these ads more relevant and therefore less annoying to Internet users than untargeted ads, they are more cost-effective to advertisers and more profitable to websites that sell ad space. While such "smarter" online advertising scares some—prompting comparisons to a corporate "Big Brother" spying on Internet users[1]—it is also expected to fuel the rapid growth of Internet advertising revenues from $21.7 billion in 2007 to $50.3 billion in 2011—an annual growth rate of more than 24%.[2] Since this growing revenue stream ultimately funds the free content and services that Internet users increasingly take for granted, policymakers should think very carefully about what's really best for consumers before rushing to regulate an industry that has thrived for over a decade under a layered approach that combines technological "self-help" by privacy-wary consumers, consumer education, industry self-regulation, existing state privacy tort laws, and Federal Trade Commission (FTC) enforcement of corporate privacy policies.

In an upcoming PFF *Special Report*, we will address the many technical, economic, and legal aspects of this complicated policy issue—especially the possibility that regulation may unintentionally thwart market responses to the growing phenomenon of users blocking online ads. We will also issue a three-part challenge to those who call for regulation of online advertising practices:

1. Identify the harm or market failure that requires government intervention.
2. Prove that there is no less restrictive alternative to regulation.
3. Explain how the benefits of regulation outweigh its costs.

Berin Szoka is a Fellow at The Progress & Freedom Foundation (PFF) and Director of the Center for Internet Freedom. Adam Thierer is a Senior Fellow and Director of the Center for Digital Media Freedom at PFF. The views expressed in this report are their own, and are not necessarily the views of the PFF board, fellows or staff.

* This Snapshot was last updated in February 2009.

1. Peter Whoriskey, Washington Post, FTC Wants to Know What Big Brother Knows About You, May 22, 2008, at http://www.washingtonpost.com/wp-dyn/content/article/2008/05/21/AR2008052102989.html.

2. Mark Walsh, Online Media Daily, "Study: Internet Ads Will More Than Double By 2011," MediaPost.com, January 21, 2008, at http://mediapost.com/publications/index.cfm?fuseaction=Articles.san&s=74685&Nid=38464&p=472752.

The Online Advertising Market

While there are other forms of targeted advertising based on *who* you are ("demographic") or *where* you are ("locational"), the most important varieties are based on *what* you're searching for, seeing or doing online at any particular moment ("contextual") and the *pattern* of what you're searching for, seeing or doing over time ("behavioral"). The bulk of Internet advertising falls into one or both of these last two categories, with behavioral advertising growing rapidly.

Search engines deliver contextual ads on search results pages based on the search keywords entered by a user, while third-party advertising networks (some of which also run search engines) deliver contextual ads on behalf of website operators who sell ad space to the network, with the ads displayed on each page chosen according to keywords on that page. Contextual advertising is far "smarter" than displaying the same "dumb" untargeted banner ads to every user, because the contextual ad uses keywords to "guess" what the user is interested in based on the context of each page. But the purely contextual ad network doesn't "remember" what the user has looked at in the past, so its insights into what the user would find relevant are very limited, especially for some websites. Online behavioral advertising (OBA) solves this problem and increases the value of advertising space on *all* websites by targeting ads based on a "profile" of the user created by tracking websites the user has visited—as well as limiting the number of times a user is shown a particular ad.

The Perceived Harm Driving Calls for Regulation

For a decade, the basic technology behind OBA has changed little: When a user visits the typical webpage, he or she downloads not only the webpage contents but also a small piece of code that allows the website to distinguish that user's browser from other browsers (a "cookie")—without personally identifying the user. Some cookies are required to make sites work properly ("site cookies") while others ("tracking cookies") are used by the third-party ad network in which that site participates to recognize that browser across multiple sites participating in the ad network, and thus create a "profile" of what the user might be interested in. Even though such profiles themselves are anonymous, many privacy advocates have pointed to four reasons why online profiling is becoming "too invasive:" (i) it is sometimes possible to infer the actual identity of the user; (ii) though all browsers allow users to opt-out of tracking by "cleaning out" their tracking cookies, a website may be able to restore deleted tracking cookies through the use of cookie alternatives such as "Flash cookies"; (iii) certain vulnerabilities in current browser design make it theoretically possible to "sniff" a user's browsing history, cache or bookmarks; and (iv) the use of "packet inspection" by Internet Service Providers (ISPs) (instead of the use of cookies) to track online browsing amounts to illegal wiretapping.

The other concerns expressed by the advocates of regulation vary significantly. Some fear that browsing profiles could be captured by hackers, somehow associated with personally identifying information, and used for identity theft. These advocates demand limits on data retention as well as data security mandates. Others demand that users have access to their own profiles—a goal inherently in tension with data security. Most share a vague queasiness

about “being tracked” and about advertising in general, while downplaying the effectiveness of self-regulation or user self-help.

Perhaps most legitimately, others fear that the *real* “Big Brother”—government—will gain access to a “honey pot" of surveillance data that might be associated with individual users. A variety of solutions have been proposed to what is, for the most part, a poorly defined problem, including: a government-run “Do Not Track” registry to make it easier for users to block tracking cookies; mandating opt-in for some or all forms of profiling; and banning completely the collection of tracking data about sensitive subjects, cross-referencing of data sets, and use of packet inspection data for OBA.

The Less Restrictive Means: A Layered Approach

But how should policymakers decide which, if any, of these interventions are really necessary—or would even be effective? Ironically, those who demand immediate OBA regulation to protect user privacy are often the first to insist on less burdensome approaches whenever a policy “problem” involves purely noncommercial speech. For example, emphasizing personal and parental responsibility is often favored as the more sensible approach to dealing with free speech and child protection concerns. But, as Chapman University Law Professor Tom Bell has asked, why not apply the same standard across the board?[3] Why not expect those especially privacy-sensitive users who object to OBA to *do* something about it? To the extent effective self-help privacy tools exist, they provide a means of solving policy problems that is not only “less restrictive” than government regulation but generally more *effective* and customizable as well. Why settle for one-size-fits-all solutions of incomplete effectiveness when users can quite easily and effectively manage their own privacy? Indeed, those who advocate personal responsibility and industry self-regulatory approaches to free speech and child protection issues should be advancing the same position with regards to privacy.

Fortunately, a wide variety of self-help tools and “technologies of evasion” are readily available to all users and can easily thwart traditional cookie-based tracking, as well as more sophisticated tracking technologies such as packet inspection. While cookie management tools that allow users to delete their cookies have been standard in browsers for some time, the latest generation of browsers incorporates far more advanced control over what kind of cookies browsers will accept from websites in the first place. Furthermore, the extensible nature of modern browsers allows any freelance software developer who sees a way to improve a browser to do so by writing an add-on that "plugs in" to the browser using standard programming interfaces designed by each browser developer. Many such add-ons are wildly popular, but even those users who never install a single one benefit from the acceleration of browser evolution made possible by add-ons. We will be documenting examples of these tools in our upcoming *Special Report* and in an ongoing series of blog essays.

3. Tom W. Bell, "Internet Privacy and Self-Regulation: Lessons from the Porn Wars," Cato Institute Briefing Paper No. 65, August 9, 2001, http://www.cato.org/pub_display.php?pub_id=1504.

The Benefits of Smarter Advertising

The "free" Internet economy is based on a simple value exchange: Users get access to an ever-expanding collection of content and services at no cost from websites that are able to generate revenue from "eyeballs" on their pages by selling space on their sites to advertisers, usually through ad networks. The smarter that advertising, the more free content and services it can support. This is the same value exchange that has supported free, over-the-air television and radio content for decades. The only difference is technological: Because websites can connect directly with the user, they need not rely on crude profiling tools such as Nielsen ratings.

There are larger economic benefits of smarter online advertising. First, it makes the overall economy more open and competitive by allowing small market entrants to reach consumers with messages about their products. Second, those who attack the use of packet inspection by ISPs for OBA fail to see that it is precisely the kind of "game-changer" that could disrupt Google's currently dominant market position. Third, the involvement of ISPs in OBA could help defer broadband costs: Even if OBA revenue does not completely subsidize monthly service costs, smarter advertising could at least keep prices in check and potentially lower them significantly going forward.

But smarter advertising isn't just about selling products or services. It is ultimately about making *all* kinds of speech more cost-effective. The ability to "target" listeners more narrowly also increases the ability of political and other not-for-profit speakers to communicate their messages. In short, smarter advertising means more voices, more choices, and more speech. The line between "advertising" and "content" is already blurring rapidly, as the technologies used to customize advertising are also used to customize webpages and ad networks themselves are used to deliver content.

The Larger Implications of Potential Regulation

As if reducing the advertising revenue generated by each web ad didn't do enough to reduce the total amount of funding for free web content and services, government regulation of targeted online advertising could reduce advertising revenues even further by aggravating the problem of ad blocking in two ways. First, the less relevant ads are, the more annoying users will find them, and the more likely users are to try to block them. Increased relevance is perhaps the most important remedy for ad blocking and the best way to maintain the implicit value exchange that currently supports free Internet content and services

Second, regulation could short-circuit the eternal battle of technological one-upmanship between online advertisers and those users who rely on the technologies of evasion to "opt-out" of seeing ads or being tracked. Such privacy-conscious users are "free-riding" off of those users who don't opt-out, since (at present) they generally don't lose access to the free content and services supported by the targeted advertisements that other users *do* see. The user who blocks tracking, but not ads, is still free-riding off those users who don't opt-out of tracking. On a large enough scale, such self-help has the potential to disrupt the value exchange of the Internet, just as automatic commercial-skipping has already disrupted the value exchange of television. As with all "Spy vs. Spy" battles, this long-term trend is inevitable: As more

sophisticated technologies of evasion are incorporated seamlessly into browsers and can be used without significantly degrading the browsing experience, their use will become increasingly mainstream. But ultimately, just as with television commercial-skipping, market forces can and will, if permitted, respond through technological means and the development of new business models. Today's implicit *quid pro quo* may become, of necessity, explicit: Websites and ad networks will have to find increasingly creative ways to grant access to certain content and services for users who do *not* block ads or the tracking that makes ad space more valuable. Policymakers should take care not to ban such technologies or cripple such business models (*e.g.*, through requiring opt-in), which may rely on more sophisticated forms of targeting such as the use of packet inspection data.

As users face an increasingly clear choice between (i) getting content and services for free supported by behavioral advertising and (ii) paying to receive those same services and content without tracking or even without ads altogether, policymakers will finally see whether users are really as bothered by profiling as the advocates of OBA regulation insist. Given the ongoing and widespread replacement of fee- or subscription-supported web business models with ad-supported models, it seems likely that the vast majority of consumers will continue to choose ad-supported models, including profiling.

Conclusion

The questions raised above—about the harm that supposedly requires intervention, the availability of less restrictive means, and the cost/benefit analysis of regulation—are vital considerations for the future of the Internet. Indeed, if smarter online advertising will not fund the Internet's future, what will? As both the desire for "free" services and content and the need for bandwidth expand, OBA has the potential to offer important new revenue sources that can help support the entire ecosystem of online content creation and service innovation, while also providing a new source of funding for Internet infrastructure and making ads less annoying and more informative. That would certainly seem preferable to increased user fees or other "pay-per-view" pricing models for Internet content and services.

But looming legislative and regulatory action could stop all of that by replacing the current regime—in which the FTC merely enforces industry self-regulatory policies—with one in which the government preemptively dictates how data may be collected and used. The more enlightened approach is a "layered" approach to privacy protection that combines industry self-regulation, enforcement of industry-established privacy policies, consumer education, and user "self-help" solutions. These and other issues will be addressed in greater detail in our upcoming PFF *Special Report*.

Related PFF Publications

- *Targeted Online Advertising: So What's the Harm & Where Are We Heading?*, by Berin Szoka & Adam Thierer, Progress on Point 16.2, February 2009.
- *Parental Controls and Online Child Protection: A Survey of Tools and Methods*, Adam Thierer, The Progress & Freedom Foundation *Special Report*, Version 3.1, Fall 2008.
- *Privacy Solutions*, Berin Szoka, Adam Thierer & Adam Marcus, Ongoing Blog Series.
- *Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information*, Thomas Lenard & Paul Rubin, *Progress on Point 14.15*, The Progress & Freedom Foundation, Aug. 2007.
- *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Talking About You*, Eugene Volokh, *Progress on Point* 7.15, Progress & Freedom Foundation, Oct. 2000,
- *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks For Competition and Privacy*, Thomas Lenard, Testimony before the Subcommittee on Antitrust, Competition Policy and Consumer Rights Committee on the Judiciary, U.S. Senate, Sept. 27, 2007.
- *Writ of Certiorari of PFF*, Amicus Brief, U.S. Supreme Court in the matter of *Trans Union v. FTC*, by Randy May, Feb. 22, 2002.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
202-289-8928 ■ mail@pff.org ■ www.pff.org