"We Know What You Like": Online Behavioral Advertising and the New Focus On Data Privacy

By Mark Sableman

From the dawn of the computer and information age, privacy prophets like Alan Westin (author of *Privacy and Freedom (1967)* and *Databanks in a Free Society (1972)*) and Arthur Miller (*The Assault on Privacy (1971)*) have warned us that information technology was—or soon would be—invading our privacy. But for 50 years, privacy protection laws were enacted only gradually and piecemeal, industry by industry, situation by situation: for example, HIPPA for health care information, and state data breach laws to protect against identity theft. That is, until recently at least, as to broad data privacy concerns, experts were worried (or, perhaps, overreacting), while citizens and their representatives were content (or, perhaps, complacent).

Data privacy moved to center stage recently, however, largely because of the emerging technique of online behavioral advertising. Behavioral advertising caught public and legislative attention in late 2008. The resulting scrutiny led to a legislative focus on data privacy generally—a focus that seems likely to lead in turn to the kind of comprehensive data privacy regulations that the privacy prophets have long sought. This article will discuss online behavioral advertising, how its examination has opened the door to broader data privacy legislation or regulation, and the issues raised by such regulation.

What is Online Behavioral Advertising?

Online behavioral advertising ("OBA" for short), broadly speaking, refers to tracking an individual's online activities in order to deliver advertising tailored to the individual's interests.[1] During the last four years, regulators have addressed four different kinds of online tracking for behavioral advertising purposes, ranging from the mildest (contextual advertising, which is simply placing advertising adjacent to related editorial content) to the most intrusive (deep packet inspection, discussed below).

Deep Packet Inspection

The traction that the OBA/data privacy public controversy has attained may be due in part to the way in which OBA was first publicized—through the so-called "deep packet inspection" technique. In this process, a user's service provider allows an advertising network access to all of the user's activities. The advertising network thus learns all of the user's interests, by seeing the websites and other Internet services that the user patronizes. Then, using that information, the advertising network can directly target ads to the user's interests. The ISPs and advertising providers obtain consent from ISP customers through various notices and agreements—though, of course, as with many such agreements, consumers don't read them and hence aren't really aware of them.[2]

Two companies, NebuAd in the United States and Phorm in the United Kingdom, championed this technology.[3] Deep Packet Inspection (DPI) became the first face of the behavioral advertising industry to the public. And it was not a pretty face. As described in a decision in one of the after-the-fact class action suits,

1. *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (February 2009) [hereafter, "*2009 FTC Report*"] at 2, n.3.

2. *See Mortensen v. Bresnan Communication, LLC*, 2010 WL 5140454 at *5 (D. Mont. 2010) (finding that ISP gave its customers multiple notice "of its monitoring and possible transmission of [customers'] electronic activities to a third party [deep packet inspection advertising provider NebuAd]").

3. "ISP Ad Partners NebuAd and Phorm Eye Overseas Expansions," Clickz, March 5, 2008, available at http://www.clickz.com/clickz/news/1706755/isp-ad-partners-nebuad-phorm-eye-overseas-expansions.

Mark Sableman is a partner at Thompson Coburn where he concentrates his practice in the litigation of trademark, copyright, patent, advertising, libel, privacy, unfair competition and trade secret cases, as well as technology and internet issues. He has written one book and more than a dozen law review articles on communications. He has also taught Internet Law (2001-2008) and Censorship and Free Expression (2006 – present) at Washington University School of Law. He has been listed in *Best Lawyers in America* since 1996. He received his J.D. *cum laude* from Georgetown University Law Center.

NebuAd contracted with internet service providers ("ISPs") to install devices on their networks that monitored ISP subscribers' internet activity and transmitted that data to NebuAd's California headquarters for analysis. That data was used to sell advertising tailored to subscribers' interests, which appeared in place of more generic advertisements on web pages visited by subscribers. The advertising profits were split by NebuAd and its ISP partners.[4]

Data collection under DPI most likely exceeded most Internet users' expectations. In deep packet inspection, in contrast to first party and third party OBA discussed below, every aspect of the user's browsing activity is open to tracking, whether or not the visited sites have arrangements with ad networks and whether or not the user has configured his settings to refuse cookies. Essentially, solely because a user obtains Internet access through a service provider that has contracted with an advertising network using DPI, every aspect of that user's Internet browsing activity would be examined and used to produce targeted advertising.

Neither consumer advocacy organizations nor Congressional leaders liked DPI. Not long after the deep packet inspection technology and practice was publicized, in 2008, Rep. Edward Markey (D.-Mass.), then chair of the House Subcommittee on Telecommunications and the Internet, held hearings on the practice.[5] Although the hearings did not lead to any legislation, they sent a clear message to the service providers who represented the customer base for companies like NebuAd and Phorm, which were offering such services—that use of such services would get critical scrutiny from Congress and could well lead to liabilities.[6] As a result, NebuAd and Phorm could not sell their services on any significant scale. Less than a year later, NebuAd's directors filed to liquidate the company,[7] and Phorm was under investigation in its home country.[8]

DPI, however, was only one technique for online behavioral adverting. Once DPI faded away, the focus shifted to the more prevalent first-party and third-party online behavioral advertising programs.

First Party Behavioral Advertising

In the case of *first party* online behavioral advertising, an Internet user who browses a trusted website will likely, in the course of that browsing, find that the website generates one or more "cookies." "Cookies" are data phrases, essential to the smooth workings of the Internet from the standpoint of a typical user, which gather and save information about a user's preferences, so that different web applications can tailor their information to those preferences. They allow users to save particular designs and content, to save and correctly place usernames and passwords, and to utilize "shopping cart" programs at e-commerce sites.[9]

Cookies are central to most OBA. To take an oversimplified example, a user of the mythical usasports.com website who checks baseball scores and articles may prompt that website to post a cookie to the user's computer, noting that interest. Or, particularly if the user made purchases through the website's e-commerce application, cookies may be generated and posted based on those purchases.

A lot of cookies have nothing to do with advertising; they simply affect how the website displays user preferences on the user's return visits. But the first party website that places cookies on the browsers of its users could also use those cookies in tailoring ads specifically targeted to the user. Let's say that our user is a St. Louis Cardinals fan, as evidenced by his browsing activity on, or merchandise purchases from, usasports.com. Cookies may help present the user with Cardinals related scores and articles whenever he or she visits that website. The website operator may use those cookies, on the user's next visit, to post ads that advertise Cardinals merchandise (and certainly not Chicago Cubs merchandise). That's basic first party online behavioral advertising.

First party OBA has been generally viewed as acceptable. In its February 2009 report, the FTC staff defined OBA (*i.e.*, the activities that it felt needed supervision and possible regulation) to exclude first-party behavioral advertising. The FTC staff noted that in first-party OBA no data is shared with any third parties, and it found the practice generally appropriate and permissible: "The staff agrees that first party behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites."[10]

4. *Valentine v. Nebuad, Inc.*, 2011 WL 129611, ___ F.Supp.2d ___ (N.D. Cal. 2011).

5. U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, Hearing on What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies (Thursday, July 17, 2008.)

6. "NebuAd Faces Class Action Suit, Phorm's ISPs Drop Like Flies," *Marketing Vox*, Nov. 14, 2008; found at http://www.marketingvox.com/nebuad-faces-class-action-suit-phorms-isps-drop-like-flies-041972/.

7. *Valentine v. Nebuad, Inc.*, 2011 WL 129611, ___ F.Supp.2d ___ (N.D. Cal. 2011).

8. Christopher Williams, "BT and Phorm escape prosecution for secret wiretaps," THE TELEGRAPH, April 8, 2011.

9. Accepted uses of cookies, at least on first party websites, include "product recommendations, tailored content, shopping cart services, website design and optimization, fraud detection, and security." *2009 FTC Report* at 26.

10. *Id.* at 26.

Put simply, users generally are assumed to trust the websites they frequent, and to understand that that trusted websites will monitor their activities, and post related content in response to the user's apparent interests.[11]

Third Party Behavioral Advertising

Third party online behavioral advertising goes a step beyond first party OBA. This practice has been the focus of regulatory and Congressional attention since late 2008. In third party behavioral advertising, the suppliers of behavioral advertising (chiefly advertising networks) collect and use consumer information *across various websites* by placing "cookies" on user computers, and then generating ads in response to those cookies and what they know about the consumer identified by the cookies. As a consequence of information about a user's activities on website A, ads may be placed to that user weeks later, when he or she is visiting unaffiliated website B.

Ad networks place their behavioral ads based on information about particular users' browsing activities. More precisely, they use cookies to identify users with certain interests, as revealed by past browsing activity. In an example presented by the Center for Democracy and Technology, a consumer advocacy group, an ad network initially saw that a particular user visited a hotel review website (sf-hotel-review.com).[12] The ad network placed a cookie on that user's computer. Then, as the consumer visited other websites (dogz-blogs.com and social-network.net), the ad network learned more about that user's interests, by tying that cookie to the visited websites. By the time the user visited the third website, the ad network was able to place a travel-related ad there, knowing that travel was one of the consumer's interests. Although oversimplified, this example describes how advertising networks work—they take note of user interests as found on various websites, and they then arrange for posting of targeted ads when those users visit websites where the ad networks have contracts to place ads.[13] The FTC has so far concluded that this kind of cookie-based behavioral advertising across unaffiliated websites should be subject to either government regulation or robust self-regulation.[14]

The New Focus on Data Privacy

The national debate over behavioral advertising and data privacy seemed to reach a crucial turning point in mid-2010. In May, U.S. Rep. Rick Boucher, a Democrat from Virginia whose House subcommittee considered Internet laws, announced, at the annual meeting of American Business Media, a proposed omnibus data privacy bill—that is, a federal law that would not only cover OBA, but all aspects of data privacy, in every industry. And during the summer of 2010, the *Wall Street Journal* began running a series about OBA and data privacy, under the ominous series title, "What They Know."

The *Journal* series dramatized behavioral advertising, making both consumers and policymakers better aware of what had until then been something of an insider debate. A *Journal* animated graphic, "A Short Guide to Cookies," for example, portrayed cookies as little animated animals that carry information back and forth between a user's computer, the Internet, and third party ad networks. More importantly, the *Journal* series described research concerning flaws in the tracking system. For example, while users can, in theory, delete (or refuse to accept) normal cookies if they do not want to be tracked, in many cases, Flash cookies (often associated with online videos) were dropped on to user computers, even if the user had attempted to refuse cookies.[15] Even worse, Flash cookies sometimes "respawned" traditional cookies that the users had attempted to delete. The *Journal's* series raised eyebrows. Forty-nine of the top 50 United States websites used a total of 3,180 tracking files, the *Journal* reported.[16] (The *Journal's* own website used trackers, too, the series acknowledged.) The *Journal* similarly found and described re-

11. The 2009 FTC Report explains that in first-party behavioral advertising, "given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it." *Id.* at 26-27.

12. *CDT's Guide to Behavioral Advertising*, Behavioral Advertising Across Multiple Sites, http://www.cdt.org/content/behavioral-advertising-across-multiple-sites.

13. *See generally* Imran Kahn et al., *The Rise of Ad Networks: An In-Depth Look at Ad Networks*, JP Morgan Chase, North American Equity Research, October 11, 2007, found at http://www.mediamath.com/docs/JPMorgan.pdf.

14. *2009 FTC Report*, pp. 27, 28; Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Dec. 1, 2010 [hereafter *2010 FTC Report*], p. 55, available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

15. Julia Angwin, *How to Avoid the Prying Eyes*, WALL ST. J., July 30, 2010. The Flash cookie issue initially came to light through an academic study at University of California, Berkeley. A. Soltani, A.Canty, Q Mayo, L. Thomas & C.J. Hoofnagle, *Flash Cookies and Privacy*, Summer Undergraduate Programing Engineering Research at Berkeley (SUPERB) 2009. *See also*, Jennifer Valentino-DeVries, *Adobe Aims to Improve Privacy Settings in Flash*, WALL ST. J., Jan. 12, 2011.

16. Julia Angwin and Tom McGinty, *Sites Feed Personal Details To New Tracking Industry*, WALL ST. J., July 30, 2010 (reporting that in study of largest 50 U.S. websites, a total of 3,180 tracking files were installed).

search regarding "referrer header tracking," which it described as "history tracking."[17] Class action lawyers responded with various suits alleging that use of Flash cookies and referrer header tracking was illegal.[18]

The *Journal* series popularized understanding of behavioral advertising, but also carried the subtext that consumers, and policymakers, needed to address data privacy in general. Indeed, as the *Journal* series proceeded, it probed data privacy issues outside of behavioral advertising—for example, GPS tracking used in connection with cell phones, Google's ability to profile its customers, and data scraping from public sources on the web. At least in part because of these revelations, by late 2010, the privacy focus had shifted in Washington from just online behavioral advertising to data privacy in general, and more proposals for broad data privacy regulation followed.

Industry, Regulatory and Congressional Responses

Industry, Congress, and both executive and independent agencies are now working toward solutions that will give users more understanding (in data privacy lingo, "transparency" or "notice") of data collection practices, and more control ("choices") with respect to them. Some proposals seek to move beyond traditional ways of thinking, by incorporating privacy considerations into all business conduct ("privacy by design") or by setting new national standards ("codes of conduct"). Across the board, change is in the offing for data privacy.

Industry

Four advertising industry groups (AAAA, ANA, IAB, and DMA), together with the U.S. Council of Better Business Bureaus, have created detailed principles for industry self-regulation of OBA.[19] The self-regulatory principles, based on an opt-out model, call for notifying consumers of third-party behavioral advertising practices through either in-ad notices or other notices placed on webpages containing behavioral ads. A special trademark (a small "i" and triangle design) was created as the "Advertising Option Icon," to identify behavioral ads and allow users to click for more information and choices. After clicking on the Advertising Option Icon, or other notices, users would be given various ways that they could express their preferences as to what behavioral ads they wished to receive or not receive—for example, by completing forms on the aboutads.info website used by many ad networks.

Regulatory Agencies

The Federal Trade Commission held hearings in late 2008 on behavioral advertising, and after reviewing public comments, issued a February 2009 staff report, *Self-Regulatory Principles For Online Behavioral Advertising.*[20] That report opined that contextual advertising and first party behavioral advertising did not need special regulation. As to third party behavioral advertising, the report suggested that it needed to be subject either to robust industry self-regulation, or, in its absence, governmental regulation.

The FTC staff issued another study of consumer privacy, on December 1, 2010, *Protecting Consumer Privacy in an Era of Rapid Change.*[21] As to behavioral advertising, it raised questions about the effectiveness of the industry self-regulation system, suggesting that it was not sufficiently robust and granular, and that implementation was taking too long.[22] The report suggested, in place of the industry self-regulatory program, a new government-mandated browser-based "Do Not Track" system, whereby Internet users would set their particular tracking preferences.[23] There wouldn't be a "Do Not Track" list like the current "Do Not Call" lists; instead, web browsers would be used to implement consumer preferences. The report stated that any such browser-based mechanism should offer "granular" choices (i.e., allowing consumers to pick and choose what kind of ads they will see) and yet be "understandable and simple." (Partly in response to this report, the major Internet brows-

17. Jennifer Valentino-DeVries, *Former FTC Employee Files Complaint Over Google Privacy*, WALL ST. J., Oct. 7. 2010; Jessica E. Vascellaro, *Lawsuit Targets an Online Data Collection Technique*, WALL ST. J., Dec. 5, 2010. Referrer header tracking is explained in this report: B. Krishnamurthy B. and C. E. Wills, *On the Leakage of Personally Identifiable Information Via Online Social Networks*, SIGCOMM Comput. Commun. Rev. 40, 1 (Jan. 2010), 112,117, available at: http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf.

18. *Web Media Companies Sued for Covert Flash Cookie Tracking, Deceptive Privacy Policies*, 15 BNA ELEC. COMM. & L. REP. 1317 (Aug. 25, 2010).

19. *See What is the Self-Regulatory Program for Online Behavioral Advertising?*, found at http://www.aboutads.info/how-interest-based-ads-work/what-self-regulatory-program-online-behavioral-advertising-0; "Self-Regulatory Principles for Online Behavioral Advertising," July 1, 2009, found at http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; Implementation Guide, Oct. 2010, found at http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf.

20. See note 1 *supra.*

21. *2010 FTC Report*, note 14 *supra.*

22. *Id.* at 64-66.

23. *Id.* at 66-69. The report also cast some doubt on the FTC's previous approval of first party behavioral advertising. For example, it suggested that first party behavioral advertisers should possibly be restricted in sharing information even with their affiliated companies, unless the affiliations were clear to consumers through use of common branding. *Id.* at 55.

ers have been modified to offer some "Do Not Track" options.[24])

On the broader issue of data privacy, the 2010 FTC Report suggested that a totally new legal "framework" was needed for privacy protection—a "privacy by design" framework in which privacy considerations assurances are built into a company's default mode of operations.

Executive Branch

The Department of Commerce also entered the data privacy debate in late 2010, with its own "Green Paper" report, generally supporting industry self-regulation but also suggesting that government could assist in helping industry participants set appropriate standards. Commerce also suggested that it could help coordinate and harmonize foreign and domestic data privacy standards—an important issue for international businesses that need to transfer data across national boundaries.[25]

Congress

The congressional focus on data privacy, initiated by Rep. Boucher in 2010, continued in 2011 even in his absence, after he lost his seat in the 2010 Republican electoral sweep. One proposal, by Rep. Jackie Speier (D-Cal.), would mandate "Do Not Track" rules for Internet browsing. A more modest bill, proposed by Rep. Clifford Stearns (R-Fla.), would require clear and full disclosures of privacy practices, and recognize the opt-out methods that are in general use today. Yet another bill, jointly sponsored by Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.), would mandate "robust" notices to consumers of Internet data collection practices, give individuals broad rights to opt-out of having information about themselves collected or sued, and impose even stronger controls (such as opt-in requirements) on sensitive medical and financial information. The Kerry-McCain bill would also seek to minimize use of data—for example, by requiring limited use, in accordance with the original purpose of the data, in cases where data is transferred to third parties.

Common Issues

As data privacy rules are considered, many issues will need to be addressed:

Who will set the rules? More specifically, will we rely on industry self-regulation, agency rules, Congressional enactments, or some combination? Industry self-regulation would likely provide more flexibility and room for techniques like OBA, but government regulation would likely give consumers stronger protections.

What data will be protected? In addition to traditional "personally identifiable information," today even Internet identifiers such as Internet protocol addresses, and geolocation data transmitted by mobile devices are sometimes claimed as personal data. How protected data is defined will have a big impact on new technologies. For example, if geolocation information is viewed as protected data, or as "sensitive" data deserving of enhanced protection, mobile marketing technologies may be stymied. That is, if your location, transmitted by your mobile phone, is "sensitive" information, your cell phone company may not be able to direct you to the nearby restaurants and attractions that its advertisers operate.

How will data be protected? The traditional "notice and choice" model (seeking only to ensure that consumers were told how data would be used, and given choices about limiting uses) generally worked on an opt-out model. Many consumer advocacy groups seek a more restrictive opt-in model, which could significantly limit data collection and use, and thereby correspondingly limit commercial collection and uses of data.

How broadly will the rules apply? Many data regulation proposals would cover even data already publicly available, or data concerning individuals in their business capacities. Businesses, media, and academic and investigative researchers are likely to object to such coverage, as overbroad and likely to limit customary and non-intrusive data usage. Particularly with business-to-business communications, protections drafted with business-to-*consumer* communications in mind may be inappropriate. Attendees at business trade shows, for example, generally desire to have their contact information shared with prospective suppliers and customers.

Who will enforce the rules? Here the choices range widely, from industry self-enforcement procedures (akin to those of the advertising industry's National Advertising Division, which regulates advertising content disputes) to civil actions and class actions. Many class actions have already been asserted in data privacy cases, typically based on federal and California statutes and on contract claims derived from privacy policy promises. Several of the proposed bills take a middle-ground approach, committing enforcement to state attorney generals and the Federal Trade Commission.

How will aggregate and anonymized data be treated? Because of the usefulness of maintaining, analyzing and using data, many entities collect and maintain data in aggregate or anonymized form, thereby protecting individual privacy while utilizing the data for business purposes. Because of recent studies concerning methods by which such data can be reconnected to individuals, however, even such data may end up following un-

24. *See, e.g.*, Jack Marshall, *Apple Adds Do-Not-Track to Safari Browser*, ClickZ, April 13, 2011, available at http://www.clickz.com/clickz/news/2043376/apple-adds-track-safari-browser.

25. U.S. Department of Commerce Internet Task Force, *Commercial Data Privacy And Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 2010).

der restrictive rules.[26] *What kind of disclosures will be mandated*? While most websites currently disclose their "privacy policies," current law requires only limited disclosures. Some privacy advocates charge that privacy policies are often too difficult for consumers to read and understand, and as a result have sought to require standardized or "plain English" privacy policies. Standardized policies, however, could prevent flexibility and impede use of new online business techniques.

Conclusion

The data privacy prophets of the 1960s and 1970s have been vindicated in one way—data privacy now stands at the center of a national debate. But much remains to be determined as to how the data privacy debate will progress, and what data privacy rules develop from it. In today's Internet and information economy, driven by data collections and exchanges, that debate calls for careful study and participation by all.

❑❑❑

26. Arvind Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, arXiv:cs/0610105v2 [cs.CR], Nov. 22, 2007 (available at http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf).