Editors: Michael Lesk, lesk@acm.org | Jeffrey MacKie-Mason, jmm@umich.edu

Can Users Control Online Behavioral Advertising Effectively?

Lorrie Faith Cranor | Carnegie Mellon University

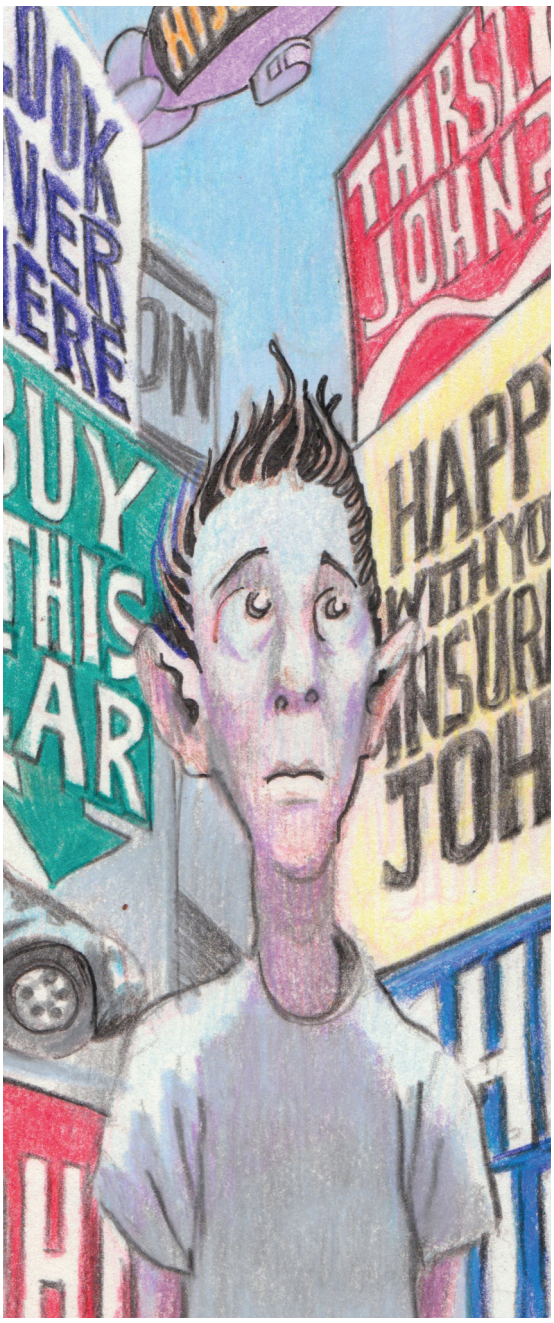
Online behavioral advertising (OBA) is the increasingly widespread practice of targeting users with specific online ads on the basis of a user's previous online behavior. Advertisers pay a premium for targeted ads because users are more likely to make purchases after viewing relevant ads.[1] On the other hand, whereas some users might appreciate seeing more relevant advertisements, many say they find targeted advertising creepy and don't like the idea of companies tracking their online activities.[2,3] Many tools empower users to control whether and when they're tracked for behavioral advertising; however, whether users can effectively control tracking and OBA using these tools is unclear.

Current Efforts

The US Federal Trade Commission has pressured companies to allow users to easily opt out of OBA.[4,5] In response, the Digital Advertising Alliance (DAA) developed self-regulatory guidelines that require companies to notify users about behavioral advertising and allow them to opt out.[6] The DAA created a standardized OBA icon for companies to place on their behavioral advertisements along with the clickable tagline "AdChoices." It also offers a website (www.aboutads.info/choices) where users can opt out of targeted ads from dozens of companies. When a user opts out, ad companies typically place an opt-out cookie on the user's computer instead of the tracking cookie that uniquely identifies the user. Companies can continue to track users, but they're prohibited from delivering targeted ads to users who have opted out.

Web browser vendors have also taken steps to help users opt out. All major browsers let users selectively block cookies, which can effectively reduce tracking. In addition, Microsoft lets users install tracking protection lists (TPLs) in Internet Explorer 9, which specify domains from which Web requests should be blocked as well as exceptions to blocking rules. Users who want to avoid OBA can download a TPL that blocks requests to known tracking companies. These are available from several organizations, including TRUSTe, PrivacyChoice, and Abine.

In February 2012, in conjunction with the White House announcement of a Consumer Privacy Bill of Rights, the DAA announced plans to include browser-based choice mechanisms, such as Do Not Track, as part of its self-regulatory program. Internet Explorer and Firefox also have a setting that sends a Do Not Track header with every HTTP request, and the World Wide Web Consortium has convened a working group to develop its specifications. In the meantime, there's no standard interpretation of what



1540-7993/12/$31.00 © 2012 IEEE Copublished by the IEEE Computer and Reliability Societies

activities the word "track" denotes, and most companies ignore Do Not Track headers.

Several browser add-ons help users avoid tracking. These tools can set opt-out cookies, block advertising cookies, block requests to tracking domains, or notify users about which trackers are present on the websites they visit.

The online-advertising industry has trumpeted these efforts to demonstrate to regulators that they can effectively self-regulate. Although these tools might be a good first step, we can't conclude that self-regulation is effective without empirical data on whether users who want to limit OBA are able to use the tools effectively.

User Studies

A series of studies at the CyLab Usable Privacy and Security (CUPS) Laboratory at Carnegie Mellon University assessed the effectiveness of tools to limit OBA. These include studies of users' perceptions of OBA and users' ability to use opt-out tools.[7]

Last summer, our research team, which included my students Pedro Leon and Blase Ur, recruited 48 Internet Explorer 9 and Firefox 5 users from the Pittsburg area to our laboratory for individual semistructured interviews and an opportunity to learn more about online privacy tools. They screened out participants with computer science or IT degrees or jobs. The interviews each lasted approximately 90 minutes. Interview sessions began with questions focusing on participants' prior knowledge and attitudes about OBA and industry advertising icons. Participants viewed an informational video on OBA produced by the *Wall Street Journal*, then discussed their understanding of and attitudes about OBA and several online advertising companies.

Then Leon and Ur gave participants information on an opt-out tool and asked them to install it on our laboratory computer. They asked participants to configure the tool according to their personal preferences, then describe the configurations they chose. Then they asked participants to configure the tools to match a set of provided specifications. Finally, they asked participants to perform several browsing tasks using the tools configured with fairly protective settings. Some of these tasks required third-party content, cookies, or scripts to function properly and thus couldn't be completed when some of the tools were set to block tracking. Participants were advised that they could adjust the tools' settings if needed to complete the tasks.

User Knowledge and Perceptions

When asked about the first thing that comes to mind when they hear "Internet advertising," many participants mentioned popups, said they found Internet advertising annoying, or said they routinely ignored it. However, when asked whether Internet advertising was useful, more than half the participants said yes, but many wished it was less obtrusive. Most participants also said that receiving ads tailored to their interests was useful. Before watching the video, few participants knew how ads were tailored, and some had misconceptions about how OBA worked. After watching the video, most participants were upset that companies track them without their knowledge and consent and said they wanted to be able to control OBA. Several described OBA as "scary" or "creepy." Their misconceptions were often fueled by their dislike of popup ads and mistrust of the advertising industry. Some were concerned that their contact information and financial records might be collected during OBA.

Most participants said they were willing to allow targeted advertising while they conducted some types of searches, but not others. In addition, they tended to be most comfortable being targeted by ad companies whose names they were familiar with, and most wary of ad companies they'd never heard of.

When shown the industry advertising icons out of context, 41 out of 48 participants didn't recognize them. When shown the icons in context next to an advertisement with the accompanying tagline, most participants didn't recognize them and couldn't figure out what they indicated. Five participants realized that the icons indicated that ads were being tailored, but none of them understood that the icons were also supposed to inform them that data was being collected for targeting. Some participants thought the icons were intended for people who wanted to advertise on websites. Many didn't expect the icons to be clickable or had misconceptions about what would happen if you clicked them. Some feared that clicking the icon would lead to more ads or popups. These results suggest that the icons and tagline are failing to effectively communicate their purpose to users.

Before discussing opt-out tools, Leon and Ur asked participants, "Are you aware of any ways that can help you stop receiving targeted ads?" About half the participants mentioned deleting cookies, something the video mentioned. Twelve participants didn't think they could do anything to stop receiving targeted ads. None mentioned opt-out cookies, industry opt-out websites, Do Not Track, or TPLs, providing further evidence that consumer awareness of opt-out options is fairly low.

Opt-Out Tool Evaluation

Successful use of opt-out tools requires that users can install a

tool, configure it to match their preferences, and use the tool effectively. Leon and Ur tested the usability of nine representative tools from three broad categories for controlling OBA:

- three tools that set opt-out cookies—the DAA opt-out website, a similar website hosted by Evidon that includes opt-outs from more companies, and the PrivacyMark bookmark tool that sets opt-out cookies for more than 160 companies whenever it's clicked;
- two built-in browser settings—Internet Explorer 9 and Firefox 5; and
- four blocking tools—Ghostery, TACO (Targeting Advertising Cookie Opt-Out), Adblock Plus, and Internet Explorer Tracking Protection.

None of these nine tools empowered study participants to effectively control tracking and behavioral advertising according to their personal preferences.

Users Couldn't Distinguish between Trackers

The opt-out websites and the Ghostery and TACO browser add-ons provided users with lists of companies that they can block or from which they can opt out. However, participants didn't recognize the majority of these companies and generally chose the same settings for all companies on the list. They couldn't set opt-out or blocking preferences meaningfully on a per-company basis.

Inappropriate Defaults

The default settings for most of the tools weren't appropriate for users interested in protecting their privacy. Once a user enables a privacy feature, a protective default for that feature seems reasonable. However, Internet Explorer doesn't guide users to subscribe to a TPL, which is necessary for the TPL feature to provide protection. Furthermore, if users proactively download a browser add-on, such as Ghostery or TACO, or visit an opt-out website, they likely intend to block tracking. However, Ghostery and TACO don't automatically block any trackers.

Communication Problems

Overall, the tools were ineffective at communicating their purposes and guiding users to properly configure them. They tended to present information at a level that was either too simplistic to inform users' decisions or too technical to be understood. For instance, Internet Explorer 9 provides a simplistic privacy slider whose six levels (for instance, "medium") don't describe their functionality. In contrast, participants couldn't understand the jargon-filled technical explanations next to the slider. Ghostery and TACO used terms that were meaningless to participants: "Web tracker," "Web bug," "Flash cookie," "Silverlight cookie," "tracking cookie," "script," "IFrame," and "targeted ad network." In addition, participants testing opt-out tools didn't understand what the tools would opt them out of. They often mistakenly believed that they were protected against tracking when they were still being tracked even though they no longer saw targeted ads. Furthermore, users thought deleting their cookies would increase their privacy, not realizing that deleting their cookies would also delete opt-out cookies (thus undoing their opt-out).

Need for Feedback

Many of the tools provided insufficient feedback. Participants were unsure of what opting out meant and how they could tell whether the opt out or cookie blocking was working. Do Not Track mechanisms also provided no feedback, and there's currently no way for tools to confirm that Do Not Track preferences are being honored. In contrast, for every website users visited, Ghostery and TACO displayed notifications about which companies were attempting to track them and whether trackers had been blocked. Users appreciated this feedback and gained an understanding of what the tools were doing.

Users Want Protections That Don't Break Websites

Participants had difficulty determining when the tools they were using caused parts of websites to stop working. In cases in which some content wasn't displayed or features stopped working, participants believed that their Internet connection was the problem. TPLs have the potential to address this problem by letting users subscribe to a curated list that blocks most trackers except those that are necessary for sites to function. However, participants were unaware that they needed to select a TPL or unsure how to decide which TPL to select. In addition, sites may bundle essential functionality into trackers to prevent their trackers from getting blocked.

Confusing Interfaces

Most tools suffered from major usability flaws. For instance, multiple participants opted out of only one company on the DAA's website, despite intending to opt out of all. Others mistook the page on which advertising companies register for the DAA for an opt-out page. Participants testing TACO never realized that they weren't blocking any trackers. Participants didn't understand Adblock Plus's filtering rules. None of the participants who tested Internet Explorer Tracking Protection realized that they needed to subscribe to TPLs until prompted in a later task.

More emphasis on tool usability is necessary to empower users to control behavioral advertising.

These studies show that users lack awareness of the tools they can use to control targeted advertising and the ability to use them effectively. Although the industry has developed guidelines and an opt-out program, users either don't recognize the opt-out icon or don't realize they can click it to get relevant information. In January 2011, the DAA announced it was launching a marketing campaign and website (www.youradchoices.com) to inform consumers about the AdChoices icon. Whether this campaign increases awareness remains to be seen.

Most of the tools examined could be substantially improved with more attention to usability. However, an underlying challenge is that users don't understand how online advertising works and are unfamiliar with online-advertising companies. When faced with choices about blocking trackers from dozens of unfamiliar companies, users can't make informed decisions. We shouldn't expect users to read dozens of privacy policies[8] or become privacy experts. Tools that let users make coarse-grained choices and translate these into the appropriate fine-grained settings (perhaps learning from other users or from users' preferences or behaviors over time) might offer a possible solution. Privacy regulations that provide a baseline level of protection offer a complementary solution that might address user concerns. ■

References

1. H. Beales, "The Value of Behavioral Targeting," Network Advertising Initiative, Jan. 2010; www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
2. A.M. McDonald and L.F. Cranor, "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising," *Proc. Telecommunications Policy Research Conf.* (TPRC 10), 2010; http://ssrn.com/abstract=1989092.
3. J. Turow et al., "Americans Reject Tailored Advertising and Three Activities That Enable It," 2009; http://ssrn.com/abstract=1478214.
4. "Protecting Consumer Privacy in an Era of Rapid Change," Federal Trade Commission, 2010; www.ftc.gov/os/2010/12/101201privacyreport.pdf.
5. J. Leibowitz, "Concurring Statement of Commissioner Jon Leibowitz: FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising," Feb. 2009; www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.
6. "Self-Regulatory Principles for Online Behavioral Advertising," Digital Advertising Alliance, July 2009; www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.
7. P.G. Leon et al., "Why Johnny Can't Opt-Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," *Proc. Conf. Human Factors in Computing Systems* (CHI 12), ACM, 2012; www.cylab.cmu.edu_cylab11017.html.
8. A.M. McDonald and L.F. Cranor, "The Cost of Reading Privacy Policies," *I/S: J. Law and Policy for the Information Society*, 2008 Privacy Year in Review issue; http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

Lorrie Faith Cranor is an associate professor of computer science and of engineering and public policy at Carnegie Mellon University. Contact her at lorrie@acm.org.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.