Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising

Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang
Carnegie Mellon University, Pittsburgh, PA
{pedrogln,bur,balebako,lorrie,rshay,yangwan1}@cmu.edu

ABSTRACT
We present results of a 45-participant laboratory study investigating the usability of nine tools to limit online behavioral advertising (OBA). We interviewed participants about OBA and recorded their behavior and attitudes as they configured and used a privacy tool, such as a browser plugin that blocks requests to specific URLs, a tool that sets browser cookies indicating a user's preference to opt out of OBA, or the privacy settings built into a web browser. We found serious usability flaws in all tools we tested. Participants found many tools difficult to configure, and tools' default settings were often minimally protective. Ineffective communication, confusing interfaces, and a lack of feedback led many participants to conclude that a tool was blocking OBA when they had not properly configured it to do so. Without being familiar with many advertising companies and tracking technologies, it was difficult for participants to use the tools effectively.

Author Keywords
Usability; Privacy; Online Behavioral Advertising; Cookies

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: Miscellaneous

General Terms
Human Factors; Experimentation; Security

INTRODUCTION
The United States Federal Trade Commission (FTC) and other groups have voiced privacy concerns about online behavioral advertising (OBA) for over a decade [8]. The FTC defines *online behavioral advertising* as "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests" [9]. Industry organizations have developed self-regulatory principles that call for companies to empower consumers to control targeted advertising. [1] [2]

[1] http://www.networkadvertising.org/networks/principles_comments.asp
[2] http://www.aboutads.info/principles/

CHI'12, May 5–10, 2012, Austin, Texas, USA.

Consumers may control OBA using a number of tools. However, to use these tools successfully, users must be able to install a tool, configure it to match their preferences, and effectively use it. While these tools have the potential to satisfy the concerns of consumers and regulators, there has been little rigorous evaluation of their usability and effectiveness.

In this paper, we present results of an in-depth study investigating the usability of tools that limit OBA. We found serious usability flaws in all nine tools we examined. The online opt-out tools were challenging for users to understand and configure. Users were confused by technical jargon and complicated settings in some tools. Users also struggled to install and configure Tracking Protection Lists (TPLs) and other blacklists to make effective use of blocking tools. They often erroneously concluded the tool was blocking OBA when they had not properly configured it to do so.

In the next section, we present background and related work. We then describe the privacy tools that we tested, present our testing methodology, and discuss our results. We conclude with a discussion and design recommendations.

BACKGROUND AND RELATED WORK
Online advertisers track users as they navigate the Internet to construct profiles for targeting advertisements. They typically use third-party HTTP cookies to track users [13]. Unlike first-party cookies, which are placed by the domain a user is visiting, third-party cookies are placed by another domain, such as an advertising network. Other tracking mechanisms, such as Flash Local Shared Objects (LSOs) and HTML 5 local storage, enable tracking even when the user clears cookies or switches browsers [1].

User concerns about behavioral advertising
According to a 2009 study [19], if given a choice, 68% of Americans "definitely would not" and 19% "probably would not" allow advertisers to track them online even if their activities would remain anonymous. McDonald and Cranor found that only 20% of their respondents prefer targeted ads to random ads, and 64% find the idea of targeted ads invasive [17].

Industry self-regulation and browser-based solutions
The Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA) self-regulatory principles require that companies allow users to opt out of targeting. Both organizations host websites where users can set opt-out cookies, signaling that they do not wish to receive targeted ads. However, Komanduri et al. found many instances of non-compliance

with the NAI and DAA requirements [12]. A 2010 FTC staff report stated that "industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection" [10].

Another example of attempted industry self-regulation is the Platform for Privacy Preferences (P3P), a computer-readable privacy policy standard published by the World Wide Web Consortium (W3C) in 2002. P3P compact policies (CPs) are a set of tokens that summarize a website's privacy policy regarding cookies. Internet Explorer 9 (IE9) uses CPs to evaluate websites' data practices and can reject cookies based on user preferences [4]. Leon et al. found that more than 20 of the 100 most-visited sites have inaccurate CPs and discovered "thousands of sites using identical invalid CPs that had been recommended as workarounds for IE cookie blocking" [15].

Two recent browser-based methods for controlling OBA are Do Not Track (DNT) and Tracking Protection Lists (TPLs). Users can configure their web browser to send a DNT header with HTTP requests, signaling that they do not want to be tracked. However, there is not yet a consensus on how to define tracking or what websites should do upon receiving a DNT header. In IE9, Microsoft introduced TPLs, lists of filter rules that block content and scripts from specified domains.

Usability of privacy tools

Prior studies have examined the usability of privacy tools. Cranor et al. designed and evaluated a privacy agent that fetched P3P policies and indicated whether they were consistent with configured preferences [6]. Ha et al. conducted focus groups to examine users' awareness of cookies and asked participants to evaluate two cookie-management tools, finding cookie management to be confusing to users [11].

A number of authors have offered guidance for the developers of privacy tools. Lederer et al. described five pitfalls in the design of privacy tools. They cautioned against designs that "require excessive configuration to manage privacy" [14]. Brunk offered recommendations for developers of privacy software including giving "the user feedback that preventative features are operational" [2]. Cranor advised privacy software developers to avoid privacy jargon, ease configuration, educate users, and use persistent indicators to convey information about the tool's capabilities and current state [5].

PRIVACY TOOLS TESTED

We tested the usability of nine tools from three broad categories for controlling behavioral advertising. This list includes three *opt-out tools*, two *built-in browser settings*, and four *blocking tools*. The tools we selected are representative of the range of tools currently available. Where we were aware of multiple similar tools, we selected those that we judged most comprehensive or easiest to use. Tests of IE 9 were conducted on Windows 7. All other tools were tested with Firefox 5.0.1 on Windows 7 or Mac OS X Leopard.

Opt-out tools

Opt-out tools allow users to set opt-out cookies for one or more advertising networks. If a user sets an opt-out cookie for a particular advertising network, that network should not show a user advertising based on his or her browsing behavior, but may continue to track and profile that user.[3] A separate opt-out cookie must be set for each network. To simplify this process, some opt-out tools let users opt out of dozens or hundreds of networks all in one place.

DAA Consumer Choice is a web-based opt-out tool hosted by the DAA. Consumers can go to the DAA website's "Consumer Choice" page,[3] select some or all of the participating companies, and click a button to set opt-out cookies. At the time of our testing, there were 79 participating companies.

Evidon Global Opt-Out is an opt-out tool hosted by Evidon, a company that provides technology to help advertisers comply with industry self-regulatory programs.[4] Similar to the DAA opt-out site, Evidon's opt-out page allows consumers to select companies from which to opt out of OBA. In addition, Evidon provides links to other companies from which a consumer may opt out through other means. At the time of testing, Evidon provided direct opt-out for 184 companies and links to opt-out information for 118 others.

PrivacyMark is a JavaScript bookmark tool that sets opt-out cookies. PrivacyMark[5] is offered by Privacy Choice, a company that sells privacy-related services to companies and offers free consumer privacy tools. At the time of our testing, the tool set opt-out cookies for over 160 companies.

Browsers' built-in settings

All major web browsers include privacy options among their built-in settings. We tested the privacy settings on Internet Explorer and Firefox, the browsers that currently have the highest market share.[6] These browsers offer the ability to block cookies selectively based on a variety of factors, including whether they are first-party or third-party cookies.

Internet Explorer 9 (IE9) includes an Internet options panel with a privacy tab that displays a six-level privacy slider. These levels restrict or block cookies based on a website's P3P CP. A user can also choose advanced settings that block all first-party or third-party cookies, setting exceptions on a per-site basis. IE9 offers additional privacy features, which we discuss with the *blocking tools*.

Mozilla Firefox 5 includes a privacy panel with a check box to "Tell web sites I do not want to be tracked" by sending a DNT header to each website a user visits. In addition, the privacy panel allows users to select options to delete browsing history automatically or choose to accept no cookies, accept cookies except from third-parties, or accept all cookies, including the option to set exceptions on a per-site basis.

Blocking tools

We tested four blocking tools, which allow users to choose domains or patterns to block. When using a blocking tool, users rely on the scope of a list of blocking rules rather than

[3] http://www.aboutads.info/choices/
[4] http://www.evidon.com/consumers/profile_manager#tab3
[5] http://www.privacychoice.org/privacymark
[6] http://gs.statcounter.com/

on the good faith of the advertising networks. When a site is blocked, the browser will not communicate with that site, preventing that site from tracking the user.

Adblock Plus 1.3.9 is an open-source tool that relies on subscription lists to determine what to block. When a user installs Adblock Plus,[7] he or she chooses one or more filter subscriptions maintained by third parties.

IE9 Tracking Protection is a mechanism built into IE9 that blocks websites based on TPLs, which are blacklists of domains. Users may subscribe to TPLs curated by third parties.

Ghostery 2.5.3 is a browser plugin available for all major web browsers. When a user visits a website, Ghostery[8] finds and disables cookies, scripts, and pixels that are used for tracking. It notifies users about which companies have been blocked and gives users the option of selectively unblocking these companies. Ghostery is owned by Evidon.

TACO 4.0 by Abine blocks tracking by particular advertising companies, sets opt-out cookies, and deletes LSOs. In addition, TACO[9] offers other privacy features, including disposable email addresses. The version of TACO we tested has since been rebranded as Privacy Suite.

METHODS

We conducted a 45-participant, between-subjects laboratory study in which each participant tested one of nine tools that control OBA. The study took place on Carnegie Mellon University's Pittsburgh campus during August 2011.

Recruitment

We sought nontechnical participants who were not knowledgable about privacy enhancing tools, but who were interested in trying them. Since we were using IE9 on Windows 7 and Firefox 5 on Windows 7 and Mac OS X as our testing platforms, we recruited participants who had experience using one of these operating system and browser combinations. Participants, who received $30 Amazon gift cards, were recruited from the Pittsburgh region using Craigslist, flyers, and a university electronic message board. Recruitment material directed prospective participants to a screening survey. We recruited five participants for each of the nine tools we tested, for a total of 45 participants. Prior research has shown that many usability problems that are likely to occur in a given population can be identified with only five participants [16].

Testing protocol

Each 90-minute individual session was moderated by one of two researchers who had jointly moderated 11 pilot sessions. We used audio recording and screen capture to document each session. Participants were randomly assigned to the tools considering their browser and OS preferences. We began each session with a semi-structured interview to gather perceptions, knowledge, and attitude about online advertising. We then showed the participant an informational *Wall Street Journal* video about OBA.[10] Following the video, we probed the participant's attitudes and perceptions about behavioral advertising. Next, we asked participants to perform three types of tasks using a computer in our laboratory configured with their preferred Internet browser and operating system. We reset the browser settings both between participants and between tasks. We asked participants to think aloud as they performed each task and to work as though they were using their own computer.

Installation and Initial Configuration. We provided a simulated email from a friend recommending the assigned tool. The email linked to a website from the tool provider where the participant could download, use, or learn about the tool. After the participant installed and configured the tool to match his or her personal preferences, we asked an After Scenario Questionnaire (ASQ) [16] and open-ended questions to measure his or her perceptions and understanding of the tool.

Configuration of Specified Settings. We next asked participants to configure the tools to match specifications we provided. Tools in the same category had similar specifications. Evidon and DAA participants were asked to opt out of 13 specific companies. Ghostery and TACO participants were asked to block the same 13 companies, which were selected from the pool of companies common to these tools. Participants also chose specific settings for the tool's notification messages. AdBlock Plus participants were asked to subscribe to a specific filtering list and add a specific filtering rule. IE-TPL participants installed a specific TPL and also blocked a specific domain. IE and Firefox participants blocked third-party cookies, allowed first-party cookies, and added two exceptions. Participants using PrivacyMark did not perform this task since that tool cannot be configured. Participants then answered another ASQ survey and verbal questions.

Fine Tuning Settings to Resolve Problems. We then configured the tool to a fairly protective setting and asked the participant to perform five typical browsing tasks with the tool installed and active. Three of these tasks required third-party content, cookies, or scripts to function properly, and thus could not be completed when some of the tools were set to block tracking. We advised the participant to change the tool's settings if he or she faced difficulty completing these tasks. In one task, we asked participants to watch a video on nytimes.com. Participants testing AdBlock Plus or Ghostery could only see the video after unblocking brightcove.com, disabling the tool on nytimes.com, or completely disabling or uninstalling the tool. Similarly, we asked participants to shop for a laptop on dell.com. When participants testing Ghostery or TACO clicked a button to proceed to the checkout page, nothing happened unless they unblocked omniture.com, disabled the tool on dell.com, or uninstalled the tool. Finally, we asked participants to log into Facebook, using an account we provided, and invite a friend to play Farmville. Participants testing Ghostery and TACO saw whitespace where the game should have been. Participants then answered questions and filled out a System Usability Scale (SUS) questionnaire [7].

[7] http://adblockplus.org/en/

[8] http://www.ghostery.com/

[9] http://abine.com/preview/taco.php

[10] http://online.wsj.com/video/92E525EB-9E4A-4399-817D-8C4E6EF68F93.html

Limitations

Due to the limited recruitment area, our participants are not representative of the general Internet population. We make no effort to draw statistically significant conclusions, but instead focus on understanding the underlying problems faced by each participant. As with any laboratory study, participants were not in their usual working environments. Participants only used their assigned tools for about an hour; an experiment over an extended time period might reveal further insights about how users interact with the tools over time and might reveal changes in behavior as users become more familiar with the tools. However, we note that a user who is dissatisfied with a tool within the first hour may opt not to continue using it. Furthermore, because most of these tools offer few visual indicators of what they are doing and do not require ongoing interaction with the user interface, users may not gain much additional familiarity through continued use.

RESULTS

We first describe our participants' demographics. Then, we present usability results for all three categories of evaluated tools. We summarize our results in Table 1.

Participants

Our participants were fairly well-educated, with some concerns about online privacy. They included 15 males and 30 females between the ages of 19 and 57 (mean age 29); each condition had both males and females. Eight were undergraduate students, 15 were graduate students, two were unemployed, and 20 were employed. None had a background in computer science or web development. The level of initial knowledge about OBA was fairly uniform across conditions. Participants' quotes are attributed to an identifier consisting of an abbreviation for the tool they tested (e.g. "EV" for Evidon) and their subject number (1 to 5) within that tool.

In our initial interview, a number of participants expressed awareness that the ads they see are sometimes tailored to their interests, though they conflated contextual and behavioral advertising. When asked how they think online advertising companies decide which ads may be relevant to users, half of the participants mentioned web browsing history or web searches, while many others mentioned social networks and email. A few participants mentioned that cookies might be involved, though they did not know how. None of the participants demonstrated an understanding of the mechanisms used for tracking. After they viewed the informational video, most participants were able to explain roughly behavioral advertising and third-party cookies. When asked about ways to stop receiving targeted ads, most participants mentioned deleting cookies, while some mentioned antivirus software. Only a few mentioned built-in browser settings.

Opt-out tools

Configuration

Participants had difficulty using the DAA's opt-out website both when attempting to navigate from the site's homepage to the opt-out page and also when choosing the companies from which to opt out. DAA-1 and DAA-4 were unable to find the opt-out page, which is linked from the homepage, until the moderator provided written instructions. Both of these participants accidentally navigated to the page on which advertising companies register to join the DAA, mistakenly believing that this was the opt-out page. DAA-1 remarked, "The application to opt out it is a bit expensive: $5,000 a year."

Once they arrived on the DAA's opt-out page, participants did not always notice that the page had three tabs: *All Participating Companies, Companies Customizing Ads For Your Browser* (the default view), and *Existing Opt-Outs.* In our test, in which each user began with a new Firefox profile, Yahoo! always appeared alone on this list of companies that had already begun tracking them. Both DAA-3 and DAA-5 only opted out of Yahoo! even though both expressed a desire to opt out of all behavioral advertising. They didn't realize that they needed to switch tabs to choose all companies. The other three DAA participants opted out of all participating companies. Since participants had difficulty navigating the DAA site, the opt-out process took a relatively long time. Participants expressed displeasure when the DAA website displayed a message stating that certain opt-outs had failed.

All five participants who tested Evidon successfully located the opt-out mechanism, although EV-2 complained that "the opt-out option is hidden." EV-1 initially had problems finding it, saying, "I am not sure where to go to opt out," and EV-3 requested assistance finding the opt-out tab once he landed on the profile page. EV-1 and EV-3 both chose to "Select All" companies whose opt-out could be completed on Evidon's page, while EV-4 chose to opt out of all companies except Google, 24/7 Real Media, AOL Advertising, and YouTube, which he identified as those he uses and trusts.

Although Evidon provides the most comprehensive list of trackers, including links to manually opt out of sites, users who wish to opt out of all companies linked from Evidon's page may expend a large amount of time doing so. Both EV-2 and EV-5 wanted to opt out of all companies available, including those that required manual opt-out. EV-5 spent 47 minutes completing the opt-out process, including landing on opt-out pages in five different languages. "How am I gonna opt-out of this one?" he remarked when he arrived on a Japanese language opt-out page. He completed these non-English opt-outs by using Google Translate.

The installation process for PrivacyMark requires dragging an icon to a browser's bookmarks toolbar, an unfamiliar process. PM-1 was initially confused about where the bookmarks toolbar was located. PM-4 remarked, "Usually software goes through a different installation process." The instructions provided incorrectly assume that the user has previously enabled the bookmarks toolbar. This toolbar is not enabled by default in recent versions of Firefox.

Understanding

No participants who tested the DAA website understood what opting out means in this context. Four participants incorrectly stated that opting out will stop tracking. Only DAA-5 did not

Tool	Capabilities	Strengths	Weaknesses
Blocking			
AdBlock Plus	Blocks tracking, blocks ads	Facilitates awareness of trackers when users click icon. Users are guided to pick a filtering list.	Configuration interface confusing, includes jargon. Difficult for participants to find specific trackers to unblock. Difficult for participants to understand differences between filtering lists.
Ghostery	Blocks tracking	Facilitates awareness of trackers through on-screen alerts. Alerts helped resolve broken website elements. Easy installation.	Configuration interface includes jargon. Participants unaware that default settings don't block trackers. Multiple steps required to enable blocking.
IE-TPL	Blocks tracking, enables DNT headers	Easy to install TPLs from provider websites.	Configuration interface confusing. Participants unaware that default settings don't block trackers. Participants did not realize they had to choose a TPL in order to be protected. Even when prompted, participants were unable to choose a TPL using the interface. Difficult to unblock specific trackers.
TACO	Blocks tracking, sets permanent opt-out cookies and blocks third-party cookies	Sets opt-out cookies by default and prevents deletion. Facilitates awareness of trackers from icons and alerts. Suggests workarounds for broken website elements. Provides diverse privacy features.	Large number of privacy features overwhelmed participants. Configuration interface confusing, includes jargon. Initial configuration took a long time. Difficult for participants to find specific trackers to unblock. Participants unaware that default settings don't block trackers. Participants didn't notice workaround suggestions.
Opt-out			
DAA	Sets opt-out cookies for 79 advertising companies	Provides links to more information about each tracker. Easy to select specific trackers.	Initial configuration took a long time. Difficult to navigate to actual opt-out page. Not obvious that opting out of all trackers requires switching out of default tab on opt-out page. Participants incorrectly believed that they were opting out of tracking. Participants did not realize that deleting cookies nullifies opt-outs. Opt-outs sometimes fail. Participants unable to confirm opting out was effective.
Evidon	Sets opt-out cookies for 184 advertising companies and provide links to opt out of 118 additional companies	Provides links to more information about each tracker. Easy to select specific trackers. Provides links to non-standard opt-outs. Provides the most comprehensive list of tracker and advertising opt-outs.	Initial configuration took a long time. Participants incorrectly believed that they were opting out of tracking. Difficult to navigate to actual opt-out page. Participants did not realize that deleting cookies nullifies opt-outs. Difficult for users to complete non-standard opt-outs. Opt-outs sometimes fail. Participants confused by "opt-out request sent" messages with no additional information. Participants unable to confirm opting out was effective.
PrivacyMark	Sets opt-out cookies for 160 advertising companies	One-click opt-out.	Participants did not realize that deleting cookies nullifies opt-outs. Participants unable to confirm opting out was effective. Requires dragging icon to bookmarks toolbar, which participants could not find. Tutorial video states incorrectly that tool will stop tracking. Participants thought clicking icon would delete cookies.
Built-in			
IE-Settings	Blocks specified cookie types	Default settings provide some protection.	Configuration interface confusing, includes jargon. Participants couldn't figure out how to block all third-party cookies.
Firefox	Blocks specified cookie types, DNT	Participants could easily block third-party cookies and enable DNT headers.	Participants didn't know what protection DNT provided.

Table 1. Summary of strengths and weaknesses of each tool identified by observing participants during usability testing.

mention tracking, but she thought that opting out "makes it easy to block advertisers from sending you ads."

All participants who used Evidon's opt-out tool similarly misunderstood opt-out to mean that they could not be tracked or would receive fewer ads. However, Evidon's opt-out website explicitly states, "If you opt out, you will still see ads online, and in some cases data may be collected about your browsing activity."[11] After opting out initially, EV-1's expectation was that she would see "probably only 10% of the ads that I used to see." Most participants mistakenly believed they could no longer be tracked. EV-3 thought that Evidon's opt-out configures "who gets your information and whether they can/cannot use it," while EV-4 believed he was "telling ad companies that I do not wish to participate in tracking behaviors." EV-5 thought he could now browse without "worrying about my information being collected."

The mechanism for opting out confused users. None of the participants who tested the DAA's website, and only two of the participants who tested Evidon's website, understood that opting out sets an opt-out cookie on their computer. All other participants who mentioned cookies mistakenly thought that cookies were being blocked. DAA-1 thought he was temporarily stopping cookies, DAA-2 expected that opting out "prevents third-party cookies from being installed on my computer," and DAA-3 said, "it blocks cookie creation and transfer." Evidon participants also thought opt-out blocks access to cookies. For instance, EV-2 said, "Somehow, it will prevent those companies from looking at the cookies that accumulate in my computer." Although they misunderstood the opt-out process, some participants liked the links to learn about the companies that participate in the opt-out program.

None of the PrivacyMark participants initially understood that the purpose of the tool was to set opt-out cookies. Three of the participants watched the video on PrivacyChoice's website, which states incorrectly that this tool stops online tracking. Common misconceptions were that PrivacyMark either prevented cookies from being sent or deleted cookies. In the eyes of PM-2, PrivacyMark "clears cookies, prevents cookies from being sent, or encodes cookies so that advertisers cannot see them." Participants retained their misconceptions of PrivacyMark's purpose even after performing a number of browsing tasks with the tool installed.

[11] http://www.evidon.com/consumers/profile_manager#tab3

Three of the participants who tested either the DAA or Evidon websites drew parallels between opting out and Do Not Call lists. DAA-4 expressed a negative attitude, saying that the DAA opt-out is "almost like Do Not Call lists, not like that works." DAA-5 said, "Everyone gets ads. You have to intentionally remove yourself, like Do Not Call."

Four of the participants who tested Evidon noted disliking the "opt-out request sent" message that sometimes appeared in place of "opted out." EV-1 was representative in saying, "I do not have a way to verify that I successfully opted out. The request was sent, but I am not sure if I actually opted out." Another participant received an "opt-out failed" message, leading him to question the effectiveness of the process.

Users were unhappy that Evidon's "Select All" option selected only companies whose opt-out could be completed on Evidon's page. EV-1 felt that the idea that "if you select all, you will not opt-out of *all* is misleading."

Overall, users were unsure of how successful their opt-outs were, with EV-2 stating, "You just have to hope that it is working." EV-4 similarly wondered, "I do not know if I actually did anything." He was also confused about the meaning of the trade group affiliations listed on Evidon's opt-out page, saying, "It would be nice to know what these [DAA, NAI] affiliations are." EV-5, who was redirected to the NAI website a handful of times during his 47-minute Evidon opt-out process, said that he believed that the NAI is an "ad agency" used by a number of companies.

PrivacyMark's lack of communication with users was its major usability issue; users wanted an indication that PrivacyMark was working. For instance, PM-2 described the feature she wanted to see in PrivacyMark as "a little notification telling you that it is working, blocking something." PM-5 suggested that she "would like to be able to check from which companies I have opted out. I want to choose specific companies I want to block." PM-4 felt that the lack of communication meant that it was not doing anything.

Finally, most participants who used cookie-based opt-out tools mistakenly believed that deleting their cookies would further protect their privacy. However, unless they use a tool designed to prevent opt-out cookie deletion (e.g. TACO, Beef TACO, "Keep my opt-outs" by Google, "Keep more opt-outs" by PrivacyChoice), users who delete their cookies inadvertently delete their opt-out cookies, undoing their opt-out.

Built-in tools

Browsers differ in the ease of changing settings

Most participants were able to find their browser's privacy settings page, although they were confused by the page's interface and jargon. IE users were unsure how IE's P3P-based settings related to third-party cookies. IE-1 spent more than 10 minutes trying to find the Internet Options window. Although she eventually found the window, she never clicked on the 'Privacy' tab. The other four participants were able to find the settings page, but the settings they chose differed from their expectations in all cases. For instance, IE-4 incorrectly expected that the default settings "will block third-party cookies." IE-5, who chose the 'High' privacy setting, was unsure what that setting actually meant. She said, "I hope what I chose, 'high,' will block cookies from dangerous websites, but from safe ones everything will get through." The explanations next to the privacy levels are based on P3P Compact Policies, which are likely unfamiliar to an average user.

In contrast, participants testing Firefox were able both to configure and describe accurately their privacy settings. For example, FF-1 blocked both first- and third-party cookies, but added exceptions for websites she uses, such as Amazon.com. She explained that Firefox "seems to be effective at limiting cookies... I like more stringent privacy setttings, but I have some exceptions, mainly entertainment." FF-4 accepted first-party and blocked third-party cookies, saying that her configuration "clears away all the cookies that you do not want...I wanted less cookies, less tracking, less invasion." The three other Firefox participants kept the default cookie settings, which allow both first- and third-party cookies. However, these participants demonstrated awareness of their settings. For instance, FF-3 explained that she "didn't want it to not track completely since I'm sometimes interested in ads."

We observed a stark difference in the performance of participants testing IE and Firefox. When asked to do so, none of the IE participants were able to allow first-party and block third-party cookies. The option to block third-party cookies is contained in the 'Advanced' menu, which only IE-2 opened. Rather than blocking third-party cookies as they had been instructed, IE-2, IE-3, and IE-5 chose the 'Low' setting on Internet Explorer's privacy slider, falsely believing they had accomplished their goal. In contrast, all five Firefox users were able to configure the specified settings, including blocking third-party cookies, in 1 to 4 minutes.

Users like 'Do Not Track' but are skeptical of its effectiveness

When asked to configure Firefox's privacy settings as they would on their own computer, four of the five Firefox participants enabled DNT. This behavior suggests that participants like the idea of stopping tracking with a single click. Nevertheless, users were skeptical about DNT's effectiveness. For example, FF-5 said, "[DNT] would probably just put a wrench in their program, but they could probably figure something else out." Both FF-1 and FF-3 correctly realized that DNT relies on advertisers' good faith. FF-1 had learned this fact from the Firefox privacy webpage, explaining, "Firefox says that DNT is voluntary. I would like to think websites will actually respect my preferences, but I am not sure."

Participants did not understand the details of the DNT mechanism, though they expressed their desire for it to stop tracking. For example, FF-3 felt that DNT meant, "Don't allow behavioral advertising to happen. Don't share...my browser history or my information," whereas FF-4 thought it meant that "websites will not be allowed to collect cookies on me. They will not be able to remember what I have done."

Fine tuning settings to fix broken elements

Both IE and Firefox users were able to remove Facebook from a blacklist in order to log in. All five IE users and all

five Firefox users correctly recognized that they were unable to login to Facebook because Facebook had been blacklisted. Although all participants removed Facebook from the blacklist, IE-1 never refreshed Facebook's page after changing her settings and thus she was not able to login after 10 minutes of trying. It took the other four users between 1 and 5 minutes from when they noticed there was a problem to successfully logging in. Removing Facebook from the list of blacklisted domains was sufficient for IE users to complete the task of inviting a friend to Farmville, but Firefox users needed to perform an extra step that proved difficult for most. Only two Firefox participants were able to invite their friends to Farmville by enabling third-party cookies. Although FF-4 solved the problem, she was confused by why her solution worked, stating, "I think I am getting confused between third-party cookies and others." FF-1 displayed similar confusion during her unsuccessful attempt to load Farmville's 'Invite Friends' feature, commenting, "I do not know why cookies are required to invite friends."

Blocking tools

While participants were able to install all four of the blocking tools, they had trouble configuring them to match their preferences. In many cases, participants erroneously believed they had chosen configurations that would block most or all third-party tracking. When the tools blocked content participants needed to complete browsing tasks, they were often unable to take appropriate corrective action, instead either failing to complete the task or disabling the tool entirely.

Installing blocking tools is easy

Overall, participants experienced few difficulties installing blocking tools. All participants who tested Ghostery, TACO, and IE-TPL were able to install the tool without any assistance, although TACO took participants longer to install. Four of the participants testing AdBlock Plus installed the tool without assistance, while one participant required assistance finding the options menu. Participants found the installation process for Ghostery to be especially simple.

Participants tried and failed to configure strong protections

Although participants were able to install the blocking tools with relative ease, they experienced difficulty configuring these tools appropriately. Participants were confused by jargon in the interface, and in some cases thought erroneously that they had chosen the most protective configuration when the tool was actually doing little.

Ghostery permits users to block tracking cookies and web bugs, but these options are off by default. Users must navigate multiple steps filled with jargon to turn on blocking. Only one participant blocked all available trackers, the highest level of protection. Three participants did not block any trackers, but two of these participants nonetheless believed they had configured the tool to block all trackers. The remaining participant selected a handful of trackers and cookies to block.

All participants who tested TACO selected the default blocking and opt-out features, which set (and prevent the deletion of) opt-out cookies, yet do not block any trackers. This configuration does not exploit the tool's significant privacy-enhancing features. Two TACO participants attempted to use the tool's identity protection features, even though neither configured any options to opt out of or block web tracking. TACO-2 spent 15 minutes installing the tool and setting preferences, attempting yet failing to configure TACO's "safe e-mail" and "safe phone number" features. Although she stated that she hoped to block cookies, she was unable to; although she remembered seeing an option to block cookies, she later forgot where this option was amid TACO's many features. TACO-4 stated that she was very concerned with privacy and was determined to use all of TACO's features. After spending 24 minutes trying to configure the tool and watching its video tutorials, she questioned TACO's trustworthiness. She remarked, "I think this is a false sense of security. Give us your information and we will anonymize it. Yeah, sure!"

Four of the AdBlock Plus participants chose the default filtering subscription list without changes, while ABP-4 chose the default list but unblocked Google AdSense. However, none of our participants understood what they were blocking, and most were unsure how to differentiate between filtering lists.

All participants testing IE Tracking Protection also kept the default setting, which provides minimal protection because it only sends a DNT header without subscribing users to a TPL. However, participants believed they were configuring the tool protectively. For instance, TPL-2 explained the rationale for his configuration as, "I just tried to get like the maximum privacy." Many of the usability problems encountered by participants testing Tracking Protection Lists had been previously identified by Cranor [3].

Changing configurations is difficult

When asked to configure blocking tools according to a specified configuration, participants' initial problem was often finding the tool again in order to change its settings. Although the add-ons toolbar was enabled, participants ABP-2, ABP-3, GH-2, and TACO-4 all required assistance finding their respective tools. Many of these participants mistakenly looked for these tools in the "All Programs" area of the Windows Start Menu. Others clicked on "Add-Ons" to open the add-ons manager, but never realized that they needed to click on "Extensions" to see which add-ons were already installed.

Only two TACO participants were able to configure TACO according to the specification we provided, spending 6 minutes and 16 minutes to do so. The three other TACO participants were unable to block web trackers. TACO-2, who spent 8 minutes before giving up, never realized that she could click on the "Not Blocked" text listed under web trackers to block them. TACO-4, who worked for 12 minutes before giving up, didn't realize that clicking on a category of trackers produced a drop-down menu of the companies whose trackers were blocked. All participants who realized they could click on this drop-down menu complained that companies were presented in a seemingly random, rather than alphabetical, order.

Similarly, only two AdBlock Plus participants configured the tool as we specified. Two others didn't select the specified

filter subscription, and one gave up. Participants had trouble navigating AdBlock Plus' interface and understanding the jargon that accompanied filtering rules. However, four of the Ghostery participants correctly configured the tool. The remaining participant required assistance finding the tool's options page and also neglected to enable one specified feature.

When asked to add a specific IE TPL, all five participants were able to do so. However, three participants were unsure how to use the IE interface to add TPLs, instead using a search engine to find the TPL on the web. Participants were also unsure whether they actually downloaded any TPLs. In addition, none of the the IE TPL participants were able to configure custom preferences that unblock specific trackers.

Fine tuning settings to fix broken elements

AdBlock Plus, Ghostery, and TACO participants encountered problems at websites because of the tool. IE TPL participants did not encounter any problems because the TPL that was installed did not block critical content at the visited sites.

In the nytimes.com task, participants noticed that there was a problem when they could not watch the required video. All five AdBlock Plus participants and four of the Ghostery participants realized that the tools were preventing the video from showing up. Every participant who noticed the problem eventually solved it. One AdBlock Plus participant unblocked a single tracking domain, while the other four participants disabled AdBlock Plus on nytimes.com. For instance, ABP-3 realized in less than a minute that something had been blocked, and he spent eight minutes trying unsuccessfully to unblock particular trackers. In the end, he disabled AdBlock Plus on nytimes.com. The Ghostery participants who solved the problem unblocked a single tracking domain.

In the Dell scenario, problems were more opaque. The mouse pointer started blinking and the site never responded after participants clicked the checkout button, leading many to believe that the Internet was temporarily slow. However, two TACO participants did not experience this problem due to changes made to the Dell website during the course of the study.

Three of the Ghostery participants realized that there was a problem, albeit after waiting for over two minutes. The other two participants waited for over four minutes until they were primed by the moderator to consider whether Ghostery might be causing the problem. At this point, GH-4 speculated that it was "maybe because I am about to enter personal information," whereas GH-5 attributed the delay to Dell's website. Four of the Ghostery participants solved the problem by unblocking specific trackers, while the other participant uninstalled Ghostery.

None of the three affected TACO participants realized by themselves that something was wrong. After the moderator waited four minutes and then asked the participant whether TACO might be causing the problem, TACO-1 concluded that TACO was the cause. However, TACO-2 still attributed the delay to the webpage, thinking that because she had successfully navigated past the first page of Dell's website, TACO was not causing problems. She said, "I'm like into the page now, so I'm thinking if anything it's just the webpage itself is slow or something... I don't know why it would have anything to do with TACO." TACO-3 also attributed the delay to network issues, explaining, "It just seems to be taking a few minutes." When asked whether TACO might be causing the problem, she decided that TACO might be protecting her from entering personal information. The only TACO participant who solved the problem, TACO-1, unblocked one web tracker and solved the problem in about two minutes.

The Facebook/Farmville task was easier for many participants than the Dell task, both because they had learned about unblocking trackers in previous tasks and because the failure was more evident. In the Facebook/Farmville task, all Ghostery participants experienced problems inviting friends yet were able to solve the problem in about one minute. Four of these participants unblocked specific trackers, while the other participant simply uninstalled Ghostery.

Four of the TACO participants experienced problems inviting friends. By contrast, TACO-1 did not experience problems since she noticed TACO's message that other participants have recommended different settings for this site, and she chose to accept those changes. None of the other TACO participants noticed this message even though all received it. TACO-3 again thought that TACO might be blocking her actions because she was about to enter personal information, although she was not certain that TACO was causing the problem. Neither of the other two TACO participants ever considered TACO as the culprit. TACO-3 gave up after seven minutes without ever noticing the alert about recommended changes. After it was pointed out by the moderator, TACO-4 noticed the TACO alert at the top of the page, but she decided to reject the changes and gave up. TACO-5, however, found an alternate route through the page that circumvented the blocked objects, never realizing that TACO had caused any problems.

Opinions and understanding of tools' capabilities

Following the testing session, we administered a System Usability Scale (SUS) survey in order to evaluate participants' opinions of the usability of the tool tested. All the tools scored between 40 and 50 out of 100 points. According to previous research [18], SUS scores below 50 points should be assigned a failing grade.

In order to evaluate participants' understanding of the capabilities of the tool they tested, we asked true-false questions after the "Configuration of Specified Settings" task and at the end of the testing session. Though none of the tools were particularly good at communicating its purpose, participants found the feedback provided by Ghostery and TACO useful. All five IE TPL participants misunderstood what IE TPLs do and were unable to differentiate between them. Participants did not trust the third-parties that produce TPLs. For example, TPL-4 erroneously believed that Fanboy, a popular TPL curator, "is probably a top advertising company." Participants testing opt-out tools incorrectly believed that those tools would stop online tracking.

DISCUSSION AND DESIGN IMPLICATIONS

None of the tools we tested empowered study participants to control OBA effectively according to their personal preferences. We identify the usability problems that appear endemic to this space and split them into thematic strands.

Users can't distinguish between trackers

The opt-out websites, as well as the Ghostery and TACO browser add-ons, provide users with lists of companies that they can block or from which they can opt out. However, users don't recognize most of these companies. We observed that users generally chose the same settings for all companies. Only a few users made exceptions for a handful of companies with names they recognized. Users were unable to set opt-out or blocking preferences meaningfully on a per-company basis. In order to align better with user expectations, blocking and opt-out tools should allow users to opt-out easily of all tracking. They should provide more fine-grained choices as an advanced setting and allow users to configure exceptions if they so desire, but not assume that most users are going to exercise such fine-grained control. Filter subscriptions and TPLs allow users to delegate these decisions to trusted experts; however, tools need better interfaces for selecting and installing these lists. In addition, tool providers should develop and test other ways of grouping trackers into meaningful categories that allow users to block or set opt-outs on a per-category basis rather than a per-company basis.

Inappropriate defaults

None of the tools that are not bundled with browsers have default settings that are appropriate for their target audience. If a user proactively downloads a browser add-on like Ghostery or TACO, or proactively visits an opt-out website, this action indicates that he or she likely intends to block tracking. However, Ghostery and TACO do not block any trackers by default, and enabling tracking involves multiple clicks. Similarly, no advertising companies are selected by default on the DAA and Evidon opt-out sites.

The general population of Firefox and IE users may have different expectations. Thus, it might be appropriate for browsers' built-in privacy settings to have less protective defaults. However, once a user enables a browser privacy feature such as TPLs, a protective default for that feature seems reasonable. IE Tracking Protection users must subscribe to a TPL before the feature provides additional protections, yet the interface did not lead participants to do so. While automatically subscribing users to a TPL would require Microsoft to select a default TPL, user interface changes could make users more aware that they need to select a TPL, guiding them to do so.

Communication problems

The tools we tested were ineffective at communicating their purpose and guiding users to configure them properly. The tools tended to present information at a level that is either too simplistic to inform a user's decision or too technical to be understood. For instance, IE9 provides a simplistic privacy slider whose six levels (e.g. "medium") do not describe their functionality. In contrast, participants were unable to understand the jargon-filled technical explanations next to the slider. Ghostery and TACO used the following terms whose distinction was 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 did not understand what the tools would opt them out of, mistakenly believing that they were protected against tracking. Furthermore, opt-out tool users thought deleting cookies would protect their privacy even more, not realizing that deleting their cookies would also delete their opt-out cookies and undo their opt-out.

Need for feedback

Many of the tools we tested provide insufficient feedback to users. Participants were left unaware whether or not most tools were working and oblivious to what they were doing. None of the opt-out tools tested notify users while they are browsing that their preferences are being respected. Furthermore, participants were unsure of what it meant to be opted-out and how they could tell whether opt-out was working. Participants who tested the browser cookie settings also had no mechanism for understanding what was happening behind the scenes unless websites didn't work. DNT mechanisms also provided no feedback; however, there is currently no way for tools to confirm that DNT preferences are being honored.

While AdBlock Plus did not provide explicit feedback, users noticed the absence of all ads on pages they visited and inferred that the tool was effective. Ghostery and TACO users received notifications on every website about what companies were attempting to track them and whether trackers had been blocked. Users appreciated this feedback and gained an understanding of what the tool was doing. However, future work is needed to determine whether these notifications become annoying or users stop noticing them over time.

Users want protections that don't break websites

Participants had difficulty determining when the tool they were using caused parts of websites to stop working. In cases where some content was not displayed or features stopped working, it appeared to participants that the problem was due to their Internet connection.

Some participants suggested that the tools should be able to detect these problems automatically and change their settings accordingly. TACO is able to detect browsing problems and suggest changes based on feedback from other users. However, most participants didn't see TACO's notification about these recommendations. An improved notification might be helpful. An alternative would be to adjust settings automatically. However, there is a risk that companies might game the crowdsourcing system to have their trackers unblocked. TPLs have the potential to address this problem by allowing users to subscribe to a list that has been curated to block most trackers, except those necessary for sites to function. However, participants in our study were unaware of the need to select a TPL and unsure how to decide which TPL to select. In addition, users wanted an easier way to delete all tracking cookies without losing essential site functions. This suggests that built-in browser tools should provide an easy way not

only to block third-party cookies but also to delete third-party cookies without deleting first-party cookies.

Confusing interfaces

The tools we tested 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. Participants testing TACO never realized that they were not blocking any trackers and multiple participants never realized they could block tracking or third-party cookies since they were confused by features related to anonymous email. Participants did not understand AdBlock Plus' filtering rules. None of the participants who tested IE Tracking Protection realized that they needed to subscribe to TPLs until prompted in a later task. When we asked them to subscribe to a particular TPL, most participants did not use the IE TPL interface but instead performed a Google search for the name of the specified TPL and subscribed via its website.

Conclusion

We found serious usability flaws in all nine tools evaluated, demonstrating that the status quo is insufficient for empowering users to protect their privacy. While we recognize that the advertising industry, browser vendors, and third parties have contributed an assortment of tools to this ecosystem, we encourage a greater emphasis on usability moving forward.

Our results suggest that the current approach to OBA self-regulation through opt-out tools is fundamentally flawed. It is very difficult for users to distinguish between advertising companies. They also lack sufficient knowledge about tracking technology to use existing privacy tools effectively.

There are significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web. The list of tracking companies and technologies is changing constantly, making it difficult for tool providers, let alone users, to keep up. It is difficult and time consuming to determine the purpose and privacy practices associated with every tracker on a website. It is also difficult to determine which trackers can be blocked without breaking desired website features. Even with additional education and better user interfaces, it is not clear whether users are capable of making meaningful choices about trackers.

Acknowledgements

This research was funded in part by a grant from The Privacy Projects and by NSF grants DGE0903659, CNS1012763, and CNS0831428.

REFERENCES

1. Ayenson, M., Wambach, D. J., Soltani, A., Good, N., and Hoofnagle, C. J. Flash cookies and privacy II. *http://ssrn.com/abstract=1898390* (2011).
2. Brunk, B. A user-centric privacy space framework. In *Security and Usability*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly, 2005, ch. 20, 401–420.
3. Cranor, L. F. A first look at Internet Explorer 9 privacy features. *http://www.techpolicy.com/Blog/March-2011/A-first-look-at-Internet-Explorer-9-privacy-featur.aspx*.
4. Cranor, L. F. *Web Privacy with P3P*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2002.
5. Cranor, L. F. Privacy policies and privacy preferences. In *Security and Usability*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly, 2005, ch. 22, 447–472.
6. Cranor, L. F., Guduru, P., and Arjula, M. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction 13* (2006).
7. Dumas, J. S. *The Human-Computer Interaction Handbook*. Lawrence Erlbaum Associates, 2003, 1093–1117.
8. Federal Trade Commission. Online Profiling: a Report to Congress: Part 2 Recommendations, July 2000.
9. Federal Trade Commission. Self-regulatory principles for online behavioral advertising, 2009.
10. Federal Trade Commission. Protecting consumer privacy in an era of rapid change, 2010.
11. Ha, V., Inkpen, K., Al Shaar, F., and Hdeib, L. An examination of user perception and misconception of internet cookies. In *CHI Extended Abstracts* (2006).
12. Komanduri, S., Shay, R., Norcie, G., and Cranor, L. F. AdChoices? compliance with online behavioral advertising notice and choice requirements. CyLab Technical Report CMU-CyLab-11-005, 2011.
13. Krishnamurthy, B., and Wills, C. Privacy diffusion on the web: a longitudinal perspective. In *Proc. WWW* (2009), 541–550.
14. Lederer, S., Hong, J., Dey, A., and Landay, J. Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing 8*, 6 (2004), 440–454.
15. Leon, P. G., Cranor, L. F., McDonald, A. M., and McGuire, R. Token attempt: the misrepresentation of website privacy policies through the misuse of P3P compact policy tokens. In *Proc. WPES* (2010), 93–104.
16. Lewis, J. R. *Handbook of Human Factors and Ergonomics*. John Wiley & Sons, Inc., 2006, ch. 49 Usability Testing, 1275–1316.
17. McDonald, A. M., and Cranor, L. F. Beliefs and behaviors: Internet users' understanding of behavioral advertising. In *TPRC* (2010).
18. Sauro, J. *A Practical Guide to the System Usability Scale (SUS): Background, Benchmarks & Best Practices.* Denver, CO: Measuring Usability LLC., 2011.
19. Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., and Hennessy, M. Americans reject tailored advertising and three activities that enable it. *http://ssrn.com/abstract=1478214* (2009).