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

ABSTRACT

We present results of a 45-participant laboratory study investigating the usability of tools to limit online behavioral advertising (OBA). We tested nine tools, including tools that block access to advertising websites, tools that set cookies indicating a user's preference to opt out of OBA, and privacy tools that are built directly into web browsers. We interviewed participants about OBA, observed their behavior as they installed and used a privacy tool, and recorded their perceptions and attitudes about that tool. 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 tend to be unfamiliar with most advertising companies, and therefore are unable to make meaningful choices. Users liked the fact that the browsers we tested had built-in Do-Not-Track features, but were wary of whether advertising companies would respect this preference. Users struggled to install and configure blocking lists 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.

Author Keywords

Usability, Privacy, Cookies, Online Behavioral Advertising

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 government regulators have been voicing concern about online behavioral advertising (OBA) for over a decade [6]. 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" [7]. Industry organizations have developed self-regulatory principles and frameworks that call for companies to offer consumers the ability to control targeted advertising. [1] [2]

Consumers may control OBA using a number of tools. However, successful use of these tools requires that the user is able to install a tool, configure it to match his or her preferences, and use the tool effectively. While these tools have the potential to satisfy the concerns of consumers and regulators, there has been little rigorous evaluation of the usability and effectiveness of these tools.

In this paper, we present results from what we believe to be the first study investigating the usability of tools to limit OBA. We present a high-level abstraction of usability problems in these tools.

We tested nine tools, including tools that block access to advertising websites, tools that set cookies indicating a user's preference to opt out of OBA, and privacy tools that are built directly into web browsers. We conducted a 45-participant, between-subjects laboratory study in which we interviewed participants about OBA, observed their behavior as they installed and used a privacy tool, and recorded their perceptions and attitudes about that tool.

We found serious usability flaws in all nine tools we examined. The online opt-out tools were challenging for users to understand and configure. Moreover, the current opt-out approach, which is based on users opting-out from specific companies, is ineffective because users tend to be unfamiliar with most advertising companies, and therefore are unable to make meaningful choices. Further, since opting-out depends on cookies, privacy-minded users who delete their cookies will unwittingly cancel their opt-out. Users liked the fact that the browsers we tested had built-in Do-Not-Track features, but were wary of whether advertising companies would respect this preference. Users were confused by technical jargon and complicated settings in some tools. Users also struggled to install and configure blocking lists 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 introduce the privacy tools that we tested, present our testing methodology, and discuss our results. We con-

CHI 2012, May 5–10, 2012, Austin, TX, USA.

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

clude with a summary of our high-level findings and a discussion of implications for online privacy today.

BACKGROUND AND RELATED WORK

Online advertisers track users as they navigate the Internet, constructing a profile for the purpose of delivering targeted advertisements. Third-party HTTP cookies are the main mechanism used for online tracking. 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, 17].

User concerns about behavioral advertising

According to a 2009 study [18], if given a choice, 68% of Americans "definitely would not" and 19% "probably would not" allow advertisers to track them online even if their online 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 [15].

Industry self-regulation

The Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA) are industry organizations that have published self-regulatory principles that mandate that users be able to opt-out of ad targeting. Both organizations maintain websites where users can set advertising network opt-out cookies that replace cookies containing unique identifiers and signal that users do not want to be tracked. However, Komanduri et al. found many instances of non-compliance with the NAI and DAA requirements [10]. 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" [8].

Another example of attempted industry self-regulation is the Platform for Privacy Preferences (P3P), a standard for computer-readable privacy policies 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. IE9 uses CPs to evaluate websites' data practices and can reject cookies based on user preference [3]. Leon et al. found that more than 20 of the 100 most-visited sites have inaccurate or erroneous CPs [12]. and discovered "thousands of sites using identical invalid CPs that had been recommended as workarounds for IE cookie blocking."

Two recent concepts 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, which are filter rules that allow users to block all content and scripts from specified websites.

Usability of privacy tools

Prior studies have examined the usability of privacy tools. Cranor et al. designed and conducted user evaluations of a privacy agent that examined websites' P3P policies and notified the user when they were inconsistent with his or her stated preferences [5]. Ha et al. conducted focus groups to examine users' awareness and management of cookies, and asked participants to evaluate two cookie management tools [9]. In a series of interviews, McDonald and Cranor found that users were confused by the interface of built-in browser cookie management tools [15].

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 and offered suggestions for avoiding them. For example, they caution against designs that "require excessive configuration to manage privacy" [11]. Brunk offers recommendations for developers of privacy software including giving "the user feedback that preventative features are operational" [2]. Cranor advises 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 [4].

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 to control behavioral advertising. Where we were aware of multiple similar tools, we selected those that appeared most comprehensive or easiest to use based on the authors' assessments. Tests of Internet Explorer settings were conducted using IE 9 on Windows 7. All other tools were tested using Mozilla Firefox 5.0.1 on either 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. A separate opt-out cookie must be set for each advertising network. To simplify this process, opt-out tools provide a mechanism for users to opt out of dozens or hundreds of advertising networks all in one place.

DAA Consumer Choice is a web-based opt-out tool hosted by the Digital Advertising Alliance, an industry group. 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 advertis-

[3]http://www.aboutads.info/choices/

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

Browsers' Built-in Settings

Web browsers generally also include privacy options among their settings. These settings, while less comprehensive than add-ons or tools designed specifically for protecting privacy, are currently available to users of all major browsers. 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.

Mozilla Firefox 5 includes a privacy panel with options to delete browsing history automatically, choose what kinds of cookies to accept, and "Tell web sites I do not want to be tracked" by sending a DNT header to websites a user visits. A user may choose to accept no cookies, accept cookies except from third-parties, or accept all cookies.

IE9 has privacy settings centered on cookies. IE9 provides a privacy slider that allows users to select between six privacy levels. 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, and set exceptions on a per-site basis. IE9 offers additional privacy features, which we discuss with the *blocking tools*.

Blocking Tools

We tested four blocking tools, which allow users to choose domains or patterns to block. With blocking tools, users are relying not on advertisers' good faith, but rather on the scope of a list of blocking rules. When a site is blocked, the browser will not make any requests to that site, completely preventing that site from tracking the user.

Ghostery 2.5.3 is a browser plugin available for all major web browsers. When a user visits a website, Ghostery[7] finds and disables cookies, scripts, and pixels that are used for tracking. It notifies users about which companies have been blocked and allows users the option of selectively unblocking these companies. Ghostery is now owned by Evidon.

TACO 4.0 blocks trackers and also provides a mechanism for setting opt-out cookies for a number of ad networks, as well as the ability to delete LSOs. In addition, TACO[8] offers features designed to help users protect their online privacy by creating disposable email addresses, protecting the data entered into forms on the Internet, and creating alternate Internet identities for the user. TACO is owned by Abine, a privacy services company.

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,[9] 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. Users may install TPL subscriptions from third parties.

METHODOLOGY

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. All participants were recruited from the [blinded urban region of the US] 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 most moderate to severe usability problems can be identified with five participants [13].

Testing protocol

Each of the the 45 sessions was moderated by one of two researchers who had jointly moderated 11 pilot sessions. The average session length was 90 minutes, and participants received $30 Amazon gift cards. We used audio recording and screen capture to document each session. We began each session with a semi-structured interview to gather the participant's perceptions, knowledge, and attitude about online advertising. We then showed the participant a *Wall Street Journal* video about online behavioral advertising.[10] Next, we asked participants to perform three tasks using their assigned Internet browser and operating system. We reset the browser settings between each participant. 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 suggesting they try the assigned tool. The email included the URL of a support website from the tool provider where the participant could download, use,

[4] http://www.evidon.com/consumers/profile_manager#tab3
[5] http://www.privacychoice.org/privacymark
[6] http://gs.statcounter.com/
[7] http://www.ghostery.com/
[8] http://abine.com/preview/taco.php
[9] http://adblockplus.org/en/
[10] http://online.wsj.com/video/92E525EB-9E4A-4399-817D-8C4E6EF68F93.html

or learn about the tool. After installing (if applicable) and configuring the tool to match his or her own preferences, the participant answered an After Scenario Questionnaire (ASQ) [14] and responded to open-ended questions to measure his or her perceptions and understanding of the tool.

Configuration of Specified Settings. To evaluate participants' ability to use the tools' main features, we asked the participants to configure the tools according to a set of 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. They also chose specific settings for the notification messages provided by the tool. 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. The participants then answered another ASQ survey followed by verbal questions.

Fine Tuning Settings to Overcome Interference. We set the tool to a fairly protective setting and asked the participant to perform three typical tasks using the web browser with the tool installed and active. 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. 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 the game Farmville. Participants testing Ghostery and TACO saw only whitespace where the game should have been. The participant then answered further questions and filled out a System Usability Scale (SUS) questionnaire [16].

Limitations

Due to small sample size and 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 qualitative results. 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 different tools over time. However, we note that a user who is dissatisfied with a tool within the first hour may opt not to continue using it.

RESULTS

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

Participants

Our participants were fairly well-educated, with 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 in a variety of occupations. None had a background in computer science or web development. The level of initial knowledge about behavioral advertising was fairly uniform across conditions.

In our initial interview, the majority of participants expressed an awareness that the ads they see are sometimes tailored to their interests, though they conflated contextual and behavioral advertising. Only a few were aware that ads they see were related to their visits to other web sites. In addition, only a few participants mentioned cookies might be involved (though they did not know how) and none of the participants demonstrated an understanding of how tracking mechanisms work. After they viewed the behavioral advertising 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 and some mentioned antivirus software. Only a few mentioned built-in browser settings.

Opt-Out

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 they wished to opt out. Two of the five participants to test the DAA's website (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." Other participants also experienced difficulty finding the link to the opt-out page.

Once they arrived on the DAA's opt-out page, participants had trouble choosing companies due to the page layout. The DAA's opt-out is organized with the tabs "All Participating Companies," "Companies Customizing Ads For Your Browser," and "Existing Opt-Outs." The default view is "Companies Customizing Ads...," which contains Yahoo even just after clearing the browser's cookies. 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 go to the "All Participating Companies" tab to choose all companies. The other three DAA participants all chose to opt out of all participating companies by choosing "Select All."

All five participants who tested Evidon successfully located the opt-out mechanism, although EV-2 did mention that "the opt out option is hidden." 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.

We observed that users who wish to opt-out of all companies linked from Evidon's page can 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-2 explained, "I need to opt-out of everything; otherwise it will be useless." 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, which entails dragging an icon to a browser's bookmarks toolbar, was confusing for users because of its unfamiliarity. PM-4 remarked, "Usually software goes through a different installation process." PM-1 was initially confused about where the bookmarks toolbar was located.

Understanding

No participants who tested the DAA website understood what opting-out means. Four of five participants incorrectly stated that opting out will stop tracking. Only DAA-5 did not mention tracking, but she though that opting out "makes it easy to block advertisers from sending you ads." She expected to see 50% fewer ads while browsing, stating that if opt-out doesn't result in fewer ads, "I would think that opt-out is pointless."

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." After completing the browsing tasks, she concluded that she "saw slightly less ads." 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 five participants who tested the DAA's website, and two of five 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."

None of the PrivacyMark participants initially understood that the purpose of the tool was to set opt-out cookies, even though three of them watched the video on PrivacyChoice's website. Common misconceptions were that PrivacyMark either prevented cookies from being sent or deleted cookies. When asked what PrivacyMark does, Participant PMk-1 stated, "[PrivacyMark] deletes information, whatever you search for, and that will not be connected to the advertisers." 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.

Three of the ten participants who tested either the DAA and 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."

The Evidon website's possibility of displaying either "opted-out" or "opt-out request sent" also caused trouble for users. Four of the five participants who tested Evidon's opt-out mechanism disliked receiving the "opt-out request sent" message. EV-1 was typical of these users, 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."

Users were also unhappy that Evidon's 'Select All' option only selected the subset of advertising 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." EV-2 echoed, "I liked that you could select all. Unfortunately, you cannot do it."

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

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

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, explaining, "In theory, it sounds like a good idea. In practice, it didn't seem to be effective."

Finally, most participants who used cookie-based opt-out tools said that deleting their cookies would further protect their privacy, after downloading opt-out cookies.

Built-in Tools

Informed Users Try to Block Third-Party Cookies

Most participants testing Internet Explorer were able to find the privacy settings page, although they were confused by the page's interface and jargon, and unclear how the P3P-based settings related to third-party cookies. IE1, 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. Although the other four participants were able to find the settings page, 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." IE provides explanations next to the privacy levels, but uses terminology related to P3P compact policies, unlikely to be familiar to an average user.

In contrast, participants testing Firefox were able to configure and then accurately describe their privacy settings. For example, FF-1 blocked all cookies (both first- and third-party) but added exceptions to allow websites she uses, including Amazon.com and Pandora.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."

Users Don't Understand What 'Do Not Track' Means

When asked to configure Firefox's privacy settings as they would on their own computer, four of five Firefox participants enabled DNT. However, no users understood how it works. FF-3 misunderstood DNT to mean, "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."

Furthermore, 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." Although no users understood how DNT works, both FF-1 and FF-3 correctly realized that DNT relies on advertisers' good faith. FF-1 mentioned that she learned this from the tutorial website we had provided, explaining, "Firefox says that DNT is voluntary. I would like to think websites will actually respect my preferences, but I am not sure."

Browsers Differ in the Ease of Changing Settings

We observed a stark difference in the performance of participants testing Internet Explorer and Firefox. When asked to do so, none of the five Internet Explorer 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 in 1 to 4 minutes. The only configuration errors were made by FF-3, who didn't realize that she had misspelled Facebook as 'Facbook' and had chosen to 'allow' rather than 'block' that domain.

Fine Tuning Settings to Overcome Interference

Both Internet Explorer and Firefox users were able to remove Facebook from a blacklist in order to log in. All five Internet Explorer users and all five Firefox users correctly recognized that they were unable to log in 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 never able to log in 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 blacklisted domains was sufficient for Internet Explorer users to complete the task, but Firefox users needed to perform an extra step that proved difficult for most. Only two of the five 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, users 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 users longer to install. Four of the five participants testing AdBlock Plus installed the tool without assistance, while one participant required assistance finding the options menu.

Users Tried and Failed to Configure Strong Protections

Although users were able to install the blocking tools with relative ease, they experienced difficulty configuring these tools appropriately. In some cases, users thought erroneously that they had chosen the most protective configuration.

Ghostery permits users to block tracking cookies and web bugs, but these options are off by default. Only one of five participants 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 trackers. The remaining participant blocked a handful of trackers and cookies.

All five participants who tested TACO selected the default blocking and opt-out features, which set opt-out cookies but do not block any trackers. This configuration does not exploit the tool's significant privacy-enhancing features. Two TACO users attempted to take advantage of identity protection features, even though neither configured any of the options to opt out of or block web tracking. TACO-2 spent 15 minutes installing the tool and selecting her 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; after reviewing TACO's options and noticing a feature for blocking cookies, she later forgot where this option was. 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, "Who says Abine is a company to trust? They will collect information about me... I think this is a false sense of security. Give us your information and we will anonymize it. Yeah sure!"

Four of the five AdBlock Plus participants chose the default filtering subscription list without any further changes, while ABP-4 chose the default list but also unblocked Google AdSense. However, none of our participants understood what they were blocking.

All five participants testing Internet Explorer Tracking Protection also kept the default settings. However, this default setting does not subscribe the user to any TPLs, leaving users with minimal protection. Although all this configuration does is send a DNT header, users 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." Similarly, TPL-4 stated, "I did not configure anything, but I think it will block all tracking."

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 misunderstood the idea of browser add-ons, mistakenly looking 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, expressed, "It is very confusing...How can I block all?" She didn't realize that clicking on a particular category of trackers produced a drop-down menu of the companies whose trackers were blocked.

Similarly, only two AdBlock Plus participants were able to configure the tool as we specified. Two other participants didn't select the specified filter subscription. The remaining participant gave up. However, four of the five 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 Tracking Protection Lists, instead going to search engines to look for the Fanboy TPL and then downloading it from the Fanboy website. Users were also unsure whether they actually downloaded any TPLs. TPL-5 wondered aloud,"Did I add it?" after he received no confirmation. None of the the participants were able to configure custom preferences.

Fine Tuning Settings to Overcome Interference

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

In the NYTimes task, it was easy for users to notice that there was a problem since they could not watch the required video. All five AdBlock Plus participants and four out of five Ghostery participants realized that the tools were preventing the video from showing up. Every participant who noticed the problem eventually solved it. ABP-3 realized in less than a minute that something had been blocked, and he spent 8 minutes trying unsuccessfully to unblock particular trackers. In the end, he disabled AdBlock Plus on the NYTimes site. All four Ghostery participants who solved the

problem unblocked a single tracking domain, while GH-2 gave up after 4 minutes of attempting to unblock trackers.

In the Dell scenario, it was more difficult for users to notice problems. The mouse pointer started blinking and the site never responded after users clicked the checkout button, leading many participants to believe that the Internet was temporarily slow. Five Ghostery and three TACO participants experienced problems; the two other TACO participants did not experience problems due to changes in the Dell website during the course of the experiment.

Three of the Ghostery participants realized that there was a problem on their own, albeit after waiting for over two minutes. However, the two other participants waited for over 4 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 five Ghostery participants solved the problem by unblocking specific trackers, while the other user uninstalled Ghostery.

In contrast, none of the three affected TACO participants realized by themselves that something was wrong. After the moderator waited four minutes and then asked the user 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. I hit the review and checkout button. It's just not loading." When prompted 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.

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 users unblocked specific trackers, while the other participant simply uninstalled Ghostery. Four of the five TACO participants experienced problems inviting friends. TACO-1 did not experience problems since she noticed TACO's message that other users have recommended different settings for this site, and she chose to accept those changes. None of the other TACO users 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. The two other TACO participants never considered TACO as the culprit. TACO-3 gave up after 7 minutes without ever noticing the alert about recommended changes. After being primed 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.

Understanding and Willingness to Use

Participants found the feedback provided by Ghostery and TACO useful, helping them gain a better understanding of what the tools were doing. For example, users liked that Ghostery listed the trackers blocked on each web page visited. GH-4 explained, "[Ghostery] shows me who is collecting my data." However, GH-2 mistakenly believed that Ghostery "helps companies [recommended by Ghostery] to track my browsing history."

Most Ghostery participants indicated that they were willing to use the tool. GH-3 expressed, "It tells you exactly what trackers are on the web page and gives you control to block them." Users did indicate a desire for a better explanation about what web trackers are and how to use the tool, as well as an ability for the tool to adjust its settings automatically to overcome interference with websites. For example, GH-3 said, "It would be nice if it could realize what the context is. For example, if you are on Facebook, apps should work."

Four of the five TACO participants said they would use TACO in their daily browsing because it reduces the amount of tracking. Nevertheless, TACO-17 was not confident about using the tool, primarily because it was cumbersome.

Users were commonly confused about IE TPLs. All five participants misunderstood what TPLs do and were unable to differentiate between them. Participants did not seem to 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."

In contrast, all five AdBlock Plus participants said they would use the tool in their daily browsing. Users liked the tool's easy installation and that it blocked ads, although they found configuration difficult. ABP-4 explained, "Filter subscription: I do not really know what that is... Most of these are kind of jargon to me... To be honest, I do not really know what these things are apart from the Google one."

Summary of Results

Table 1 summarizes our findings for each tool over five key aspects, each represented by a column in the table. *Installation and configuration* corresponds to success rates and timing for installing and configuring the tool. *Typical privacy settings* corresponds to how participants initially configured the tool; *High* corresponds with the main features generally being enabled, and *Low* corresponds with the tool generally being rendered ineffective. *Understanding* reflects the accuracy of participants' responses to a set of true-false questions administered after using the tool. Scores for this aspect are relative to the other tools, as even those tools scored as *High* did not facilitate much understanding among our participants. *Awareness* corresponds to the tool announcing privacy risks to its users as a function of participants noticing

alerts. Tools that do not provide alerts are scored *N/A*. *Usability Perception* corresponds to results from the SUS survey. All tools scored between 40 and 50 out of 100. Therefore, we rated each *Medium*.

Tool	Install and configure	Typical privacy settings	Understanding	Awareness	Perceived usability
Blocking					
TACO	Medium	Medium	High	High	Medium
Ghostery	Easy	Medium	High	High	Medium
IE-TPL	Medium	Low	Medium	N/A	Medium
AdBlock Plus	Medium	High	Medium	Medium	Medium
Opt-out					
DAA	Medium	Medium	Medium	N/A	Medium
PrivacyMark	Easy	High	Low	N/A	Medium
Evidon	Medium	Medium	Low	N/A	Medium
Built-in					
IE-Settings	Difficult	Medium	Medium	N/A	Medium
Firefox	Easy	Medium	Medium	N/A	Medium

Table 1. This table summarizes the findings for each tool across five key usability aspects based on our evaluation.

DISCUSSION

None of the nine tools we tested empowered study participants to effectively control tracking and behavioral advertising according to their personal preferences. We identify the usability problems that appear endemic to this space, and we split these usability errors into thematic strands.

Need for Feedback

Many of the tools we tested provide insufficient feedback to users. Users were left unaware whether or not most tools were working, and oblivious to what was happening behind the scenes on different websites.

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 exactly 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.

In contrast, Ghostery and TACO users received notifications on every website visited 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 less useful or annoying over time, and whether users stop noticing them.

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 the majority of these companies. We observed that users generally chose the same settings for all companies on the list. A few users made exceptions for a handful of companies with names they recognized, but mostly users attempted to block trackers from all companies. Asking users to set opt-out or blocking preferences on a per-company basis is not effective.

Users Want Protections That Don't Break Things

Participants had difficulty determining when the tool they were using caused parts of websites to stop working. In cases where some content didn't appear or features stopped working, it appeared to participants that the problem was due to their Internet connection. They were especially confused when problems did not occur on the first page of a particular site, but only on subsequent pages.

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 in settings based on feedback from other users. However, most participants didn't notice TACO's notification about these recommendations. An improved notification might be helpful. Another option would be to adjust the settings automatically without waiting for user confirmation. However, there is a risk that tracking companies might game the crowd sourcing 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, when companies use the same cookie for tracking and for critical site functions, users who unblock critical cookies also end up allowing tracking.

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, their action indicates that they likely intend 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 a different set of 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 requires users to subscribe to a TPL before the feature provides additional protections. While automatically subscribing users to a TPL would require Microsoft to select a default TPL, user inter-

face changes could make users more aware that they need to select a TPL, and guide them to do so.

Jargon

Users are capable of understanding and reasoning about their privacy if information is presented in an appropriate manner. However, the tools we investigated 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, Internet Explorer 9 provides a simplistic privacy slider whose six levels (e.g. "medium") do not describe their functionality. Participants were unable to understand the technical explanations next to the slider.

The jargon used to communicate about tracking is also a source of confusion for users. Ghostery and TACO used the following terms whose distinction was meaningless to participants: Web Tracker, Web Bug, Pixel, Tracking Cookie, Tag, Beacon, LSO, Script, Widget, and Targeted Ad Network. Users are agnostic to both the method of tracking and the exact identity of the potentially hundreds of different companies that are tracking them.

Interface Usability Issues

A number of the tools suffered from major usability flaws, suggesting that usability has not been a priority in their design. 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 companies register for the DAA as the opt-out page. Participants testing TACO never realized that they were not blocking any trackers. Furthermore, it seems that TACO bundles too much functionality; 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; to subscribe, the majority of users performed a Google search rather than using the IE interface.

Conclusion

In our 45-participant lab study, we evaluated the usability of tools that limit OBA. We found serious usability flaws in all nine tools evaluted, demonstrating that the status quo is insufficient for empowering users to protect their privacy. In particular, the current approach for advertising industry self-regulation through opt-out mechanisms is fundamentally flawed. Users' expectations and abilities are not supported by existing approaches that limit OBA by selecting particular companies or specifying tracking mechanisms to block. Although we recognize the efforts of the advertising industry, browser providers, and third-parties for contributing an assortment of tools to this ecosystem, we encourage a greater emphasis on usability moving forward.

REFERENCES

1. Ayenson, M., Wambach, D. J., Soltani, A., Good, N., and Hoofnagle, C. J. Flash cookies and privacy II. *SSRN eLibrary* (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. *Web Privacy with P3P*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2002.
4. 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.
5. Cranor, L. F., Guduru, P., and Arjula, M. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction 13* (2006).
6. Federal Trade Commission. Online Profiling: a Report to Congress: Part 2 Recommendations, July 2000.
7. Federal Trade Commission. Self-regulatory principles for online behavioral advertising, 2009.
8. Federal Trade Commission. Protecting consumer privacy in an era of rapid change. Tech. rep., 2010.
9. Ha, V., Inkpen, K., Al Shaar, F., and Hdeib, L. An examination of user perception and misconception of internet cookies. In *CHI extended abstracts*, ACM (2006).
10. 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.
11. 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.
12. 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. CyLab Technical Report CMU-Cylab-10-014, 2010.
13. Lewis, J. R. Legitimate use of small samples in usability studies: Three examples. Tech. rep., IBM, Inc., 1991.
14. Lewis, J. R. *Handbook of Human Factors and Ergonomics*. John Wiley & Sons, Inc., 2006, ch. 49 Usability Testing, 1275–1316.
15. McDonald, A. M., and Cranor, L. F. Beliefs and behaviors: Internet users' understanding of behavioral advertising. In *TPRC* (2010).
16. S., D. J. *The Human-Computer Interaction Handbook*. Lawrence Erlbaum Associates, 2003, ch. User-Based Evaluations, 1093–1117.
17. Soltani, A., Canty, S., Mayo, Q., Thomas, L., and Hoofnagle, C. J. Flash cookies and privacy. *SSRN eLibrary* (2009).
18. Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., and Hennessy, M. Americans reject tailored advertising and three activities that enable it. *SSRN eLibrary* (2009).