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

October 31, 2011

CMU-CyLab-11-017

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

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

October 31, 2011

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 they were using was blocking OBA when they had not properly configured it to do so.

Executive Summary

Online behavioral advertising (OBA) is "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests" [9]. Consumers may control OBA using a number of tools, including those developed as part of industry self-regulatory programs. 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. We tested the usability of nine representative tools from three broad categories for controlling behavioral advertising: three opt-out tools, two built-in browser settings, and four blocking tools. These tools use a variety of mechanisms to allow consumers to control OBA. Some tools use *opt-out cookies* to store a user's preference not to receive OBA. Other tools transmit *Do Not Track* (DNT) headers to websites to signal that a user does not wish to be tracked. Still other tools block communication with websites matching entries on a *Tracking Protection List* (TPL).

Tools evaluated

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.

- **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, select some or all of the 79 participating companies, and click a button to set opt-out cookies.
- **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. Similar to the DAA opt-out site, Evidon's opt-out page allows consumers to select from 184 companies from which to opt out of OBA. In addition, Evidon provides links to 118 other companies from which a consumer may opt out through other means.
- **PrivacyMark** is a bookmark tool that sets opt-out cookies for over 160 companies whenever it is clicked. PrivacyMark is offered by Privacy Choice, a company that sells privacy-related services to companies and provides free privacy tools for consumers.

All major web browsers 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.

- **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.
- **Internet Explorer 9** allows users to select between six privacy levels. These levels restrict or block cookies based on a website's Platform for Privacy Preferences (P3P) compact policy. A user can also choose advanced settings that block all first-party or third-party cookies, and set exceptions on a per-site basis.

We tested four blocking tools, which allow users to choose domains or patterns to block. The browser will not communicate with a blocked 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 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.

- **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 Local Shared Objects (LSOs, sometimes called "Flash cookies"). In addition, TACO offers other features designed to help users protect their online privacy.
- **Adblock Plus 1.3.9** is an open-source tool that relies on filter subscription lists maintained by third parties to determine what to block. Users select which filter subscriptions to install.
- **IE9 Tracking Protection** is a mechanism built into Internet Explorer 9 that blocks websites based on TPLs provided by third parties. Users select which TPLs to install. When users enable TPLs they also enable the sending of DNT headers.

Methods

We sought non-technical participants who were not knowledgeable about privacy tools, but who were interested in trying them. 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.

Each participant came to our lab individually for a 90-minute 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 an informational video about online behavioral advertising produced by the *Wall Street Journal*. Next, we asked participants to perform a series of tasks on our laboratory computer. We provided a simulated email from a friend that included the URL of a support website from the tool provider where the participant could download, use, or learn about the assigned tool. After installing (if applicable) and configuring the tool to match his or her personal preferences, the participant answered questions to measure his or her perceptions and understanding of the tool. To evaluate participants' ability to use the tools' main features, we next asked participants to configure the tools according to a set of specifications we provided. Finally, we set the tool to a fairly protective setting and asked participants to perform five typical tasks using the web browser 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.

Results

None of the nine tools we tested empowered study participants to effectively control tracking and behavioral advertising according to their personal preferences. We summarize our major findings here.

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. Users were unable to set opt-out or blocking preferences meaningfully on a per-company basis.

Inappropriate defaults. The default settings for most of the tools we tested were not appropriate for users who are interested in protecting their privacy. Web browsers do not enable most of their privacy features by default, which is likely appropriate for a general audience. On the other hand, once a user enables a privacy feature, a protective default for that feature seems reasonable. However, IE does not guide users to subscribe to a Tracking Protection List, which is necessary for the TPL feature to provide protection. Furthermore, if a user proactively downloads a browser add-on like Ghostery or TACO, or 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 tracker blocking involves multiple clicks. Similarly, no advertising companies are selected by default on the DAA and Evidon opt-out sites.

Communication problems. Overall, tools were ineffective at communicating their purpose and guiding users to properly configure them. 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. 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, when instead they may continue to be tracked but no longer see targeted ads. 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, undoing their opt-out.

Need for feedback. Many of the tools we tested provide insufficient feedback to users. 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. In contrast, Ghostery and TACO users received notifications on every website visited about which companies were attempting to track them and whether trackers had been blocked. Users appreciated this feedback and gained an understanding of what the tool was doing.

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. 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. 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 expressed their desire to easily delete all tracking cookies without losing essential site functions.

Confusing interfaces. Most tools suffered from major usability flaws. For instance, multiple participants opted out of only one company on the DAA's website, despite intending to opt out of all. Others mistook the page on which advertising companies register for the DAA as the opt-out page. Participants testing TACO never realized that they were not blocking any trackers. 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. More emphasis on tool usability is needed in order to empower users to control behavioral advertising.

Conclusion

We found serious usability flaws in all nine tools evaluated. Our results suggest that 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. There are significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web. Even with additional education and better user interfaces, it is not clear whether users are capable of making meaningful choices about trackers.

1 Introduction

The United States Federal Trade Commission (FTC) and other government regulators have voiced concern 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 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 of an in-depth study investigating the usability of tools to limit OBA. We also provide a high-level discussion of usability problems associated with 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. Users mistakenly believed that opt-out tools were protecting them against tracking when those tools do not provide that functionality. 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 may 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 Tracking Protection Lists (TPLs) and other 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 methods, and discuss our results. We conclude with a summary of our high-level findings and a discussion of implications for online privacy today. We provide an appendix with more detailed results and screenshots of the tools tested.

2 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, 18].

[1] http://www.networkadvertising.org/networks/principles_comments.asp

[2] http://www.aboutads.info/principles/

2.1 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 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 [17].

2.2 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 signal that users do not wish to receive interest-based advertising from companies. 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 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 [4]. Leon et al. found that more than 20 of the 100 most-visited sites have inaccurate or erroneous CPs and discovered "thousands of sites using identical invalid CPs that had been recommended as workarounds for IE cookie blocking" [14].

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.

2.3 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 [6]. Ha et al. conducted focus groups to examine users' awareness and management of cookies, and asked participants to evaluate two cookie-management tools [11]. In a series of interviews and surveys, McDonald and Cranor found that users were confused by the interface of built-in browser cookie-management tools [17].

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" [13]. 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 [5].

3 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.

3.1 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 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 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.

3.2 Browsers' built-in settings

Web browsers generally include privacy options among their built-in 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 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.

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, and set exceptions on a per-site basis. IE9 offers additional privacy features, which we discuss with the *blocking tools*.

3.3 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 on the good faith of the advertising networks.

[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/

When a site is blocked, the browser will not communicate with 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 Tracking Protection Lists (TPLs). Users may install TPL subscriptions curated by third parties.

4 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 at the CyLab Usable Privacy and Security Laboratory on the Carnegie Mellon University campus during August 2011.

4.1 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 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 most moderate to severe usability problems can be identified with five participants [15].

4.2 Testing protocol

Each of the the 45 individual 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. Participants were randomly assigned to the tools considering their browser and OS preferences. 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 an informational *Wall Street Journal* video about online behavioral advertising.[10] We then collected perceptions and attitudes specifically about behavioral advertising. Next, we asked participants to perform three types of tasks using a computer in our laboratory configured with their assigned Internet browser and operating system. We reset the browser settings between each participant 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.

[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

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, or learn about the tool. An example of one of the simulated emails used is shown in Figure 1 in the appendix. The URLs of the support websites are listed in Table 2 in the appendix. After installing (if applicable) and configuring the tool to match his or her personal preferences, the participant answered an After Scenario Questionnaire (ASQ) [16] 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. These companies were arbitrarily selected from the pool of companies common to these tools. 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 Resolve Problems. We set the tool to a fairly protective setting and asked the participant to perform five typical browsing tasks using the web browser 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 further questions and filled out a System Usability Scale (SUS) questionnaire [7].

4.3 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 understanding the roots of the difficulties 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 different 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.

5 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.

Tool	Capabilities	Strengths	Weaknesses
Blocking			
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 when users click icon or enable alert. 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.
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.
AdBlock Plus	Blocks tracking	Facilitates awareness of trackers when users click icon. Users are forced to pick a filtering list so have protection right away. Blocks ads.	Configuration interface confusing, includes jargon. Difficult for participants to find specific trackers to unblock. Difficult for participants to understand differences between filtering lists.
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, sets DNT headers	Participants could easily block all third-party cookies. Participants could easily turn on DNT.	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. While most tools have additional strengths and weaknesses, we report here only those that were revealed when study participants interacted with the tools.

5.1 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, 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 and/or web searches, while many others mentioned social networking activities and the contents of emails. 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 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, while some mentioned antivirus software. Only a few mentioned built-in browser settings.

5.2 Opt-out tools

5.2.1 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 assigned 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 For Your Browser," which means that many users only opt out of companies that have already begun tracking them. In our test, in which each user began with a new Firefox profile, Yahoo! always appeared alone on this list. 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 opted out of all participating companies. Figures 2 and 3 in the appendix show the DAA home page and DAA opt-out default page. Since participants had difficulty navigating the DAA site, the opt-out process took a relatively long time. Participants also expressed displeasure when the DAA website displayed an error 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 "Manage your online 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, 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, as seen in Figure 6 in the appendix.

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-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, shown in Figure 4 in the appendix, incorrectly assume that the user has previously enabled the bookmarks toolbar. This toolbar is not enabled by default in recent versions of Firefox.

5.2.2 Understanding

No participants who tested the DAA website understood what opting out means in this context. Four of five participants incorrectly stated that opting out will stop tracking. Only DAA-5 did not mention tracking, but she thought 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 only two of the 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." Although they misunderstood the opt-out process, some participants liked that both the DAA and Evidon sites include 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. When asked what PrivacyMark does, Participant PM-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 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."

The Evidon website's possibility of displaying either "opted-out" or "opt-out request sent" also dissatisfied

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

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." Another participant received an "opt-out failed" message, leading him to further question the opt-out process' effectiveness.

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." Figure 5 in the appendix shows the web page that users were shown after selecting "all" and opting out.

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.

Although PrivacyMark empowers users to opt out with one click, its 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, 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 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.

5.3 Built-in tools

5.3.1 Informed users try to block third-party cookies

Although Internet Explorer does block some (but not all) third-party cookies by default, privacy-sensitive participants had difficulty choosing configurations that matched their expectations. Most participants were able to find the privacy settings page, although they were confused by the page's interface and jargon, and also unsure how the 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." 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 both configure and accurately describe their privacy settings. For example, FF-1 blocked both first- and third-party cookies, 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."

5.3.2 Users like 'Do Not Track' option but are skeptical about 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 suggests that participants like the idea that they can stop 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 mentioned that she learned this from the Firefox privacy webpage we had directed her to at the beginning of the study, 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."

5.3.3 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, including blocking third-party cookies, in 1 to 4 minutes. Figures 7 and 8 in the appendix show the privacy settings in Firefox 5 and IE 9, respectively.

5.3.4 Fine tuning settings to fix broken elements

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 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 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."

5.4 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.

5.4.1 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 five participants testing AdBlock Plus installed the tool without assistance, while one participant required assistance finding the options menu. Particiants found the installation process for Ghostery, in particular, to be especially simple.

5.4.2 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, which participants found cumbersome. 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 all trackers. The remaining participant selected a handful of trackers and cookies to block. Figures 9 and 10 in the appendix show Ghostery's main configuration interface.

All five 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 take advantage of the tool's diverse 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 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, "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!" Figure 14 in the appendix shows TACO's main configuration interface.

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 unblocked Google AdSense. However, none of our participants understood what they were blocking, and most were unsure how to differentiate between the filtering lists offered. Figure 16 in the appendix shows AdBlock Plus' main configuration screen.

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 to send a DNT header, 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." Similarly, TPL-4 stated, "I did not configure anything, but I think it will block all tracking." Figure 13 in the appendix shows the TPL configuration interface. Participants encountered several usability problems, some previously discussed by Cranor [3], leading them to select less than optimal privacy settings.

5.4.3 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 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. 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. Participants noted that an alphabetical list would have been much faster for them. Participants also experienced problems with jargon, confusing the "Targeted Ad Networks" and "Web Tracker" categories in TACO's interface.

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. Participants had trouble navigating AdBlock Plus' interface and understanding the jargon that accompanied filtering rules. 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 (the TPL we specified) and then downloading it from the Fanboy website. Participants were also unsure whether they actually downloaded any TPLs. TPL-5 wondered aloud,"Did I add it?" after he received no confirmation. IE TPL participants were also asked to configure the personalized TPL to allow and block content from two specific domains, respectively. None of the the participants were able to configure custom preferences that unblock specific trackers.

5.4.4 Fine tuning settings to fix broken elements

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.com task, it was easy for participants 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. 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. Figure 17 in the appendix shows the complexity of trying to unblock a specific tracker using AdBlockPlus. Some participants hovered their mouse cursor over the ABP icon to learn which items were blocked, yet these notifications did not help them to unblock particular trackers. 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 participants to notice problems. The mouse pointer started blinking and the site never responded after participants 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 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 five Ghostery participants solved the problem by unblocking specific trackers, while the other participant 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 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. 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.

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, as in the nytimes.com task. 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 five TACO participants experienced problems inviting friends. 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. The two other TACO participants never 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.

5.4.5 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, participants 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 said, "It tells you exactly what trackers are on the web page and gives you control to block them." Participants 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 fix broken elements on 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."

Similarly, participants liked TACO because they can click the TACO icon to see who is attempting to track them. TACO-1 said "It tells you what companies are tracking you, and you can click [them] on and off." Figures 11 and 15 show the alerts provided by Ghostery and TACO, respectively. These alerts improved participants' awareness of tracking and understanding of the purpose of these tools.

Four of the five TACO participants said they would use TACO in their daily browsing because it reduces the amount of tracking. Nevertheless, TACO-4 was not confident about using the tool, finding it cumbersome.

Participants 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. Participants 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."

6 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.

6.1 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. Users were unable to set opt-out or blocking preferences meaningfully on a per-company basis. In order to better match user expectations, blocking and opt-out tools should allow users to easily opt-out 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.

6.2 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 interface changes could make users more aware that they need to select a TPL, guiding them to do so.

6.3 Communication problems

The tools we tested were ineffective at communicating their purpose and guiding users to properly configure them. 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, Internet Explorer 9 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.

6.4 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.

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.

6.5 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. 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 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 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 expressed a desire to easily delete all tracking cookies without losing essential site functions, improving privacy without compromising functionality. 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.

6.6 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. 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. 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.

6.7 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 evaluated, demonstrating that the status quo is insufficient for empowering users to protect their privacy. 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.

Our results suggest that 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. Users have great difficulty distinguishing between tracking companies. They also lack sufficient knowledge about tracking technology or privacy tools 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 advertising companies and the technologies for tracking are 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. *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. 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, ch. User-Based Evaluations, 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. Tech. rep., 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*, ACM (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] 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.

[14] 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 *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, WPES '10, ACM (New York, NY, USA, 2010), 93–104.

[15] Lewis, J. R. Legitimate use of small samples in usability studies: Three examples. Tech. rep., IBM, Inc., 1991.

[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] Soltani, A., Canty, S., Mayo, Q., Thomas, L., and Hoofnagle, C. J. Flash cookies and privacy. *SSRN eLibrary* (2009).

[19] 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).

A Introducing participants to tested tools

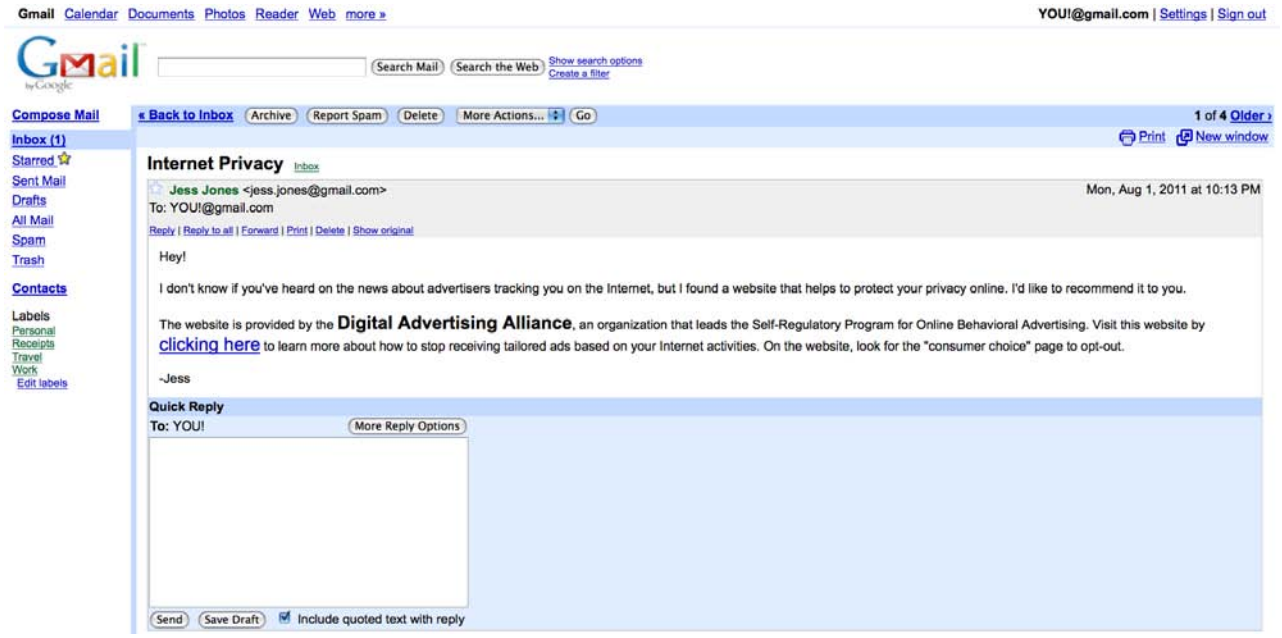

Figure 1: This screenshot shows the email that was used to introduce participants to the DAA website. Similar emails were used to introduce other participants to their assigned tools. When participants clicked on *clicking here* links, they were taken to a support webpage from the tool provider.

Tool	Tool's support webpage
Blocking	
TACO	http://abine.com/preview/taco.php
Ghostery	http://www.ghostery.com/
IE-TPL	http://windows.microsoft.com/en-US/windows7/How-to-use-Tracking-Protection-and-ActiveX-Filtering
AdBlock Plus	http://adblockplus.org/en/
Opt-out	
DAA	http://www.aboutads.info/
Evidon	http://www.evidon.com/
PrivacyMark	http://www.privacychoice.org/privacymark
Built-in	
IE-Settings	http://windows.microsoft.com/en-US/windows7/Change-Internet-Explorer-9-Privacy-settings
Firefox	http://support.mozilla.com/en-US/kb/Options%20window%20-%20Privacy%20panel

Table 2: This table shows the URL of the support webpage for each of the tested tools. Participants were directed to these URLs to learn about their assigned tool.

B Screenshots of opt-out tools

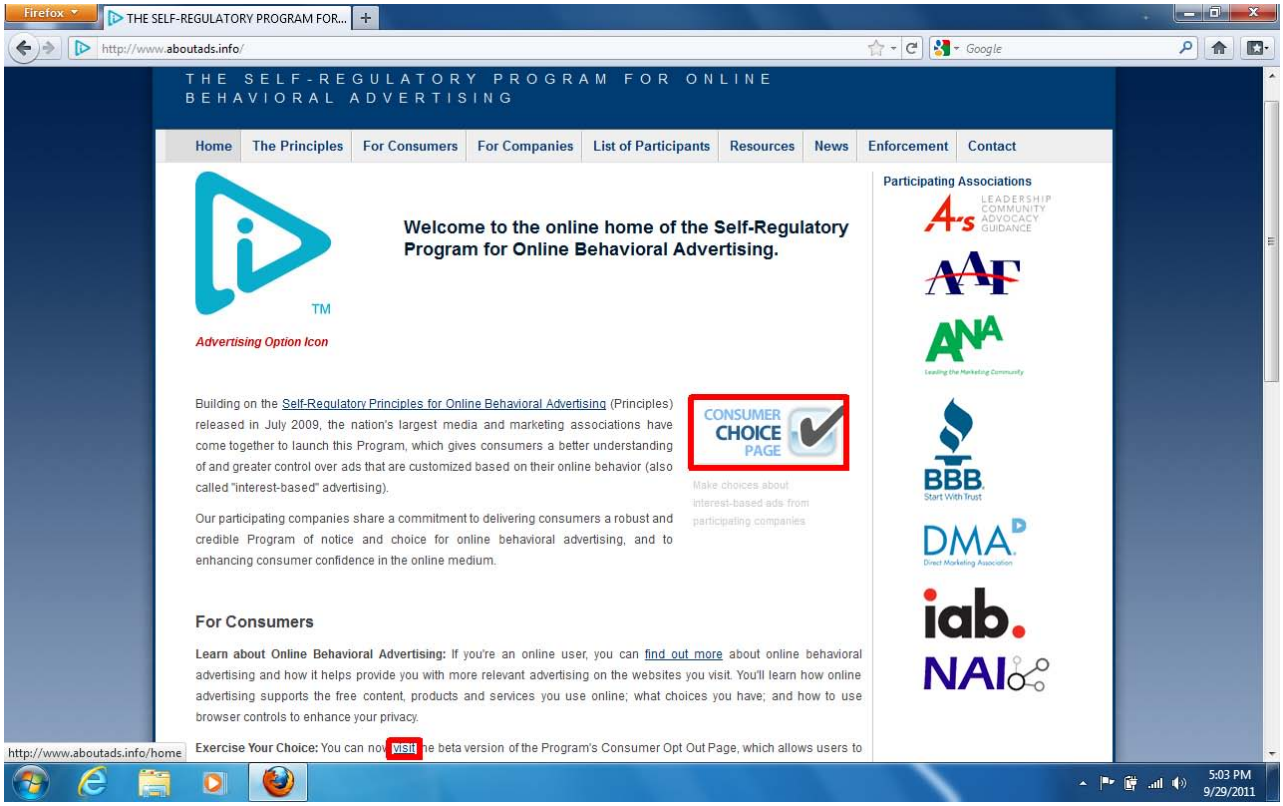

Figure 2: The DAA home page, with red rectangles indicating links to the opt-out page. Most users didn't realize the checkmark icon or "visit" links would lead them to the opt-out page. Instead, two of the five participants testing the DAA's opt-out instead clicked a "click here" link lower on the page, even though the full text of the sentence containing the link was "If you would like to register to use the icon, please *click here*." Those two users were very confused when they landed on a page where advertising companies can register to join the DAA, with one user wondering why opting out costs $5,000.

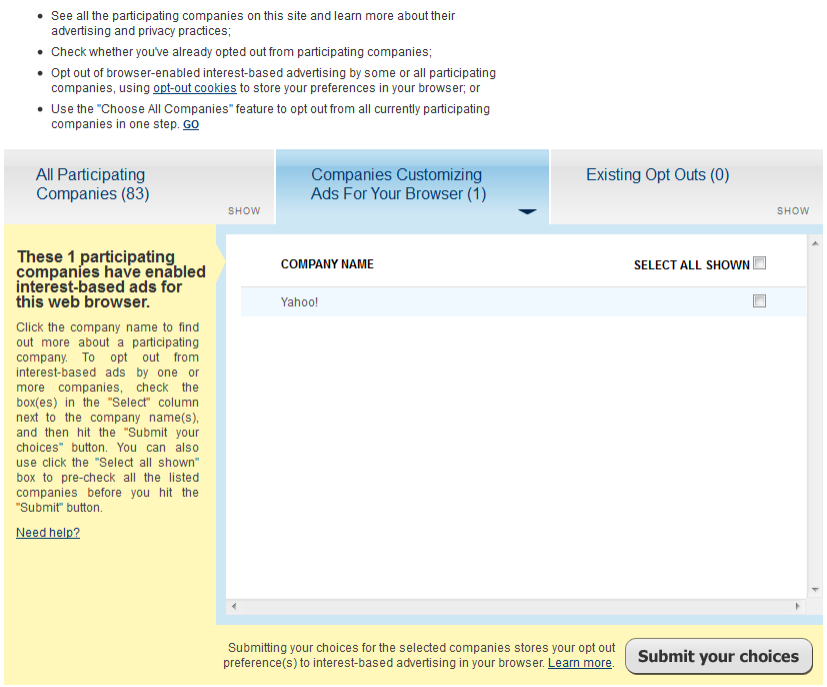

Figure 3: The DAA opt-out page, whose layout confused users. The page has three tabs: "All Participating Companies," "Companies Customizing Ads For Your Browser," and "Existing Opt Outs." The default tab is "Companies Customizing Ads For Your Browser," which appears even when a user clears her cookies. To actually opt out of all available companies, a user must first click the "All Participating Companies" tab before choosing "Select All Shown."

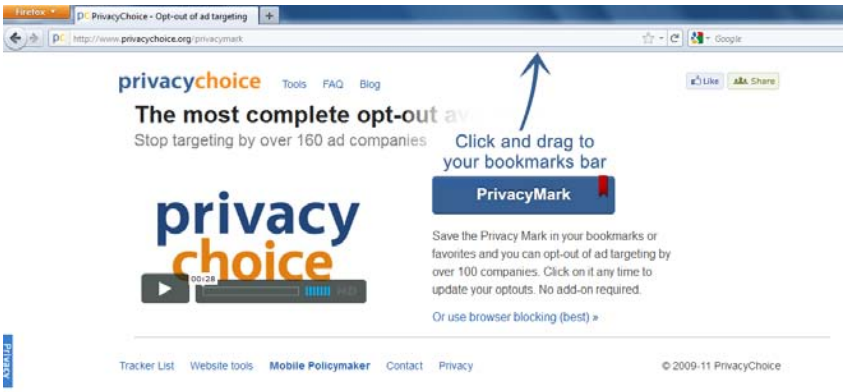

Figure 4: PrivacyMark's installation website. Users had difficulty using PrivacyMark to opt out since it asks the user to drag the PrivacyMark icon to the browser's Bookmarks Toolbar. This toolbar is not enabled by default in newer versions of Firefox, which led to confusion for users.

Name	Category	Affiliations	Opt-out
140 Proof	Other	IAB	go to site
24/7 Real Media	Ad server, Network	AAAA, DAA, IAB, iASH Europe, NAI, TRUSTe	go to site
33Across	Network, Optimizer	DAA, IAB, NAI	opted out
4info	Network	IAB	go to site
Accuen Media	Agency, Network		opt-out request sent
Acerno	Network	NAI	opted out
Acxiom (Relevance-X)	Offline data aggregator, Online data aggregator, Retargeter	DAA, IAB	opt-out request sent
Ad Desk	Ad server, Network	IAB, NAI	opt-out request sent
Ad River	Ad server		go to site
Adap.tv	Ad server, Exchange	IAB	opt-out request sent
Adara Media	Analytics provider, Data solution	DAA, NAI, TRUSTe	opted out
Adblade	Network		go to site
AdBrite	Exchange	DAA, IAB, NAI, TRUSTe	opted out
AdBuyer	Demand side platform		opt-out request sent
AdCentric (Cossette)	Ad server		opt-out request sent
Adchemy	Demand side platform	DAA, NAI	opted out
Adconion Media Group	Network, Optimizer	DAA, IAB, NAI	go to site

Figure 5: Evidon's opt-out page. Although participants were more successful opting out of companies on Evidon's page than on the DAA's page, they were confused and annoyed by the site's terminology. After choosing "Select All" and opting out, users receive one of three different messages for each company: "opted out," "opt-out request sent," or "go to site." Participants were particularly unhappy with the ambiguity of "opt-out request sent" and the extra effort required to "go to site" to opt out.

Figure 6: Two determined participants chose to "go to site" for the companies from which they were unable to opt out automatically. The second of these participants opted out for 47 minutes. Since a handful of opt-out pages were offered only in languages other than English, he used Google Translate to learn how to opt out and confirm that his opt-out had been recorded. This figure shows part of the translation he generated while opting out of Freak Out, one of the Japanese networks.

C Screenshots of tools built into browsers

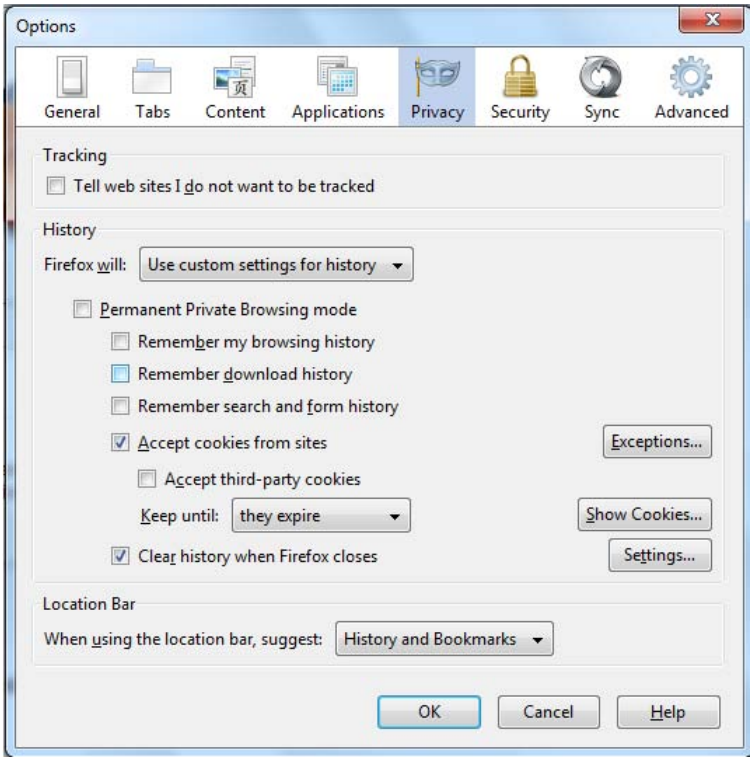

Figure 7: Firefox 5's built-in privacy features. Using the privacy options built into the Mozilla Firefox 5 browser, participants were generally successful in blocking third-party cookies, which are often cookies from advertisers, while still accepting first-party cookies. Although Firefox doesn't show any of the checkboxes seen in this figure until the users chooses "Firefox Will: Use custom settings for history," all participants were able to find these options following the instructions on Mozilla's website that they read before configuring Firefox.

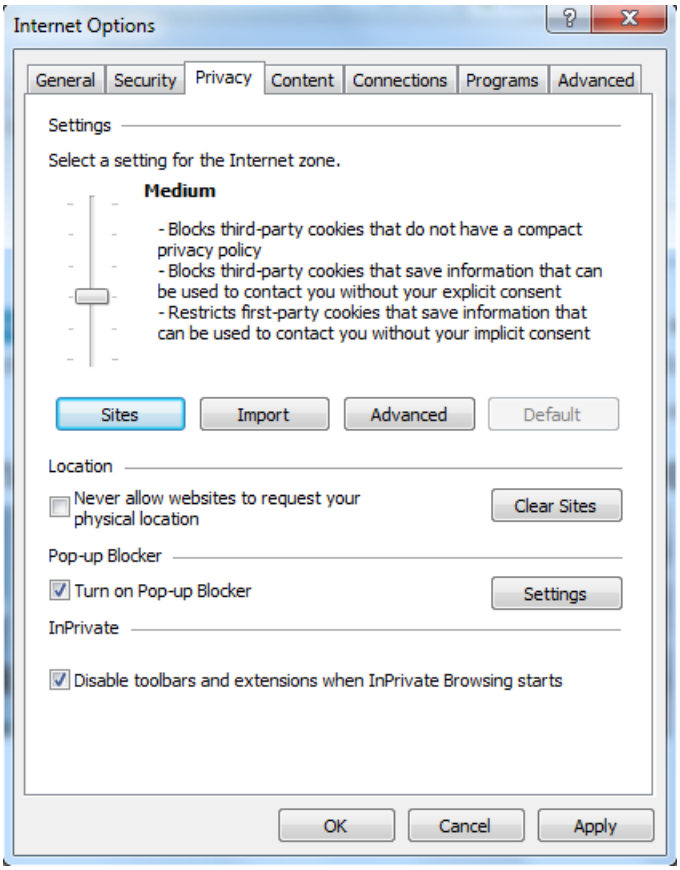

Figure 8: Internet Explorer 9's built-in privacy features. In contrast to Firefox, participants testing Internet Explorer 9 were unable to block third-party cookies while enabling first-party cookies. The option to perform this blocking is part of the "advanced" menu, which no users chose to view. Users were confused by the slider for choosing privacy settings, neither understanding its references to compact privacy policies nor the options it presented.

D Screenshots of blocking tools

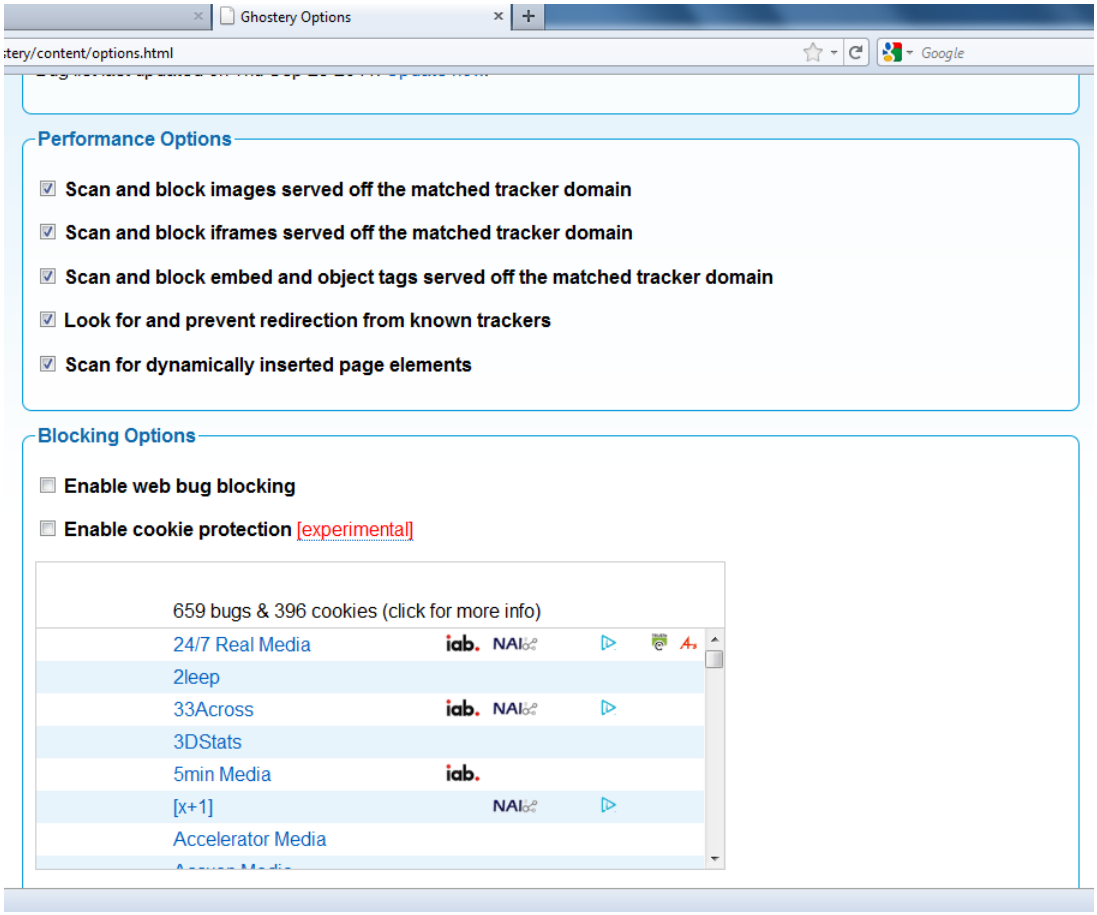

Figure 9: Ghostery's configuration interface. Users found the configuration of Ghostery relatively confusing. Although it's intended as privacy software, Ghostery doesn't block any trackers by default. On this configuration screen, users must select both "Enable web bug blocking" and "Enable cookie protection" for full protection. Some participants were apprehensive about using cookie protection since it is labeled "experimental" in red, a color that often indicates a problem.

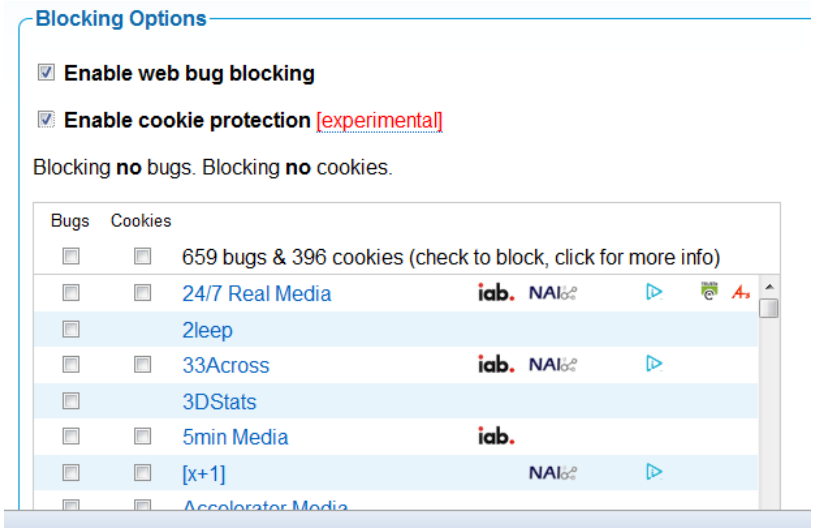

Figure 10: Ghostery's configuration interface, once cookie protection has been enabled. Once a user chooses to "enable web bug blocking" or "enable cookie protection," she must further select from a list of companies that appears for this blocking to take effect. While it comes first on the list, the button to select all options is unlabeled. Furthermore, participants didn't understand the difference between blocking web bugs and enabling cookie protection.

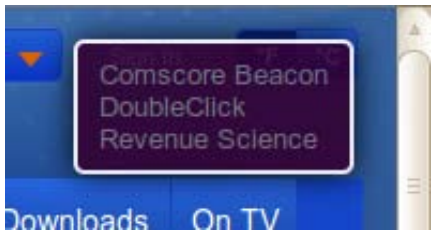

Figure 11: The alert Ghostery presents on each site a user visits. As users visit websites, Ghostery presents an ephemeral pop-up alert indicating which companies have trackers on that page. Participants noticed and correctly understood that those companies were attempting to track their browsing on the page.

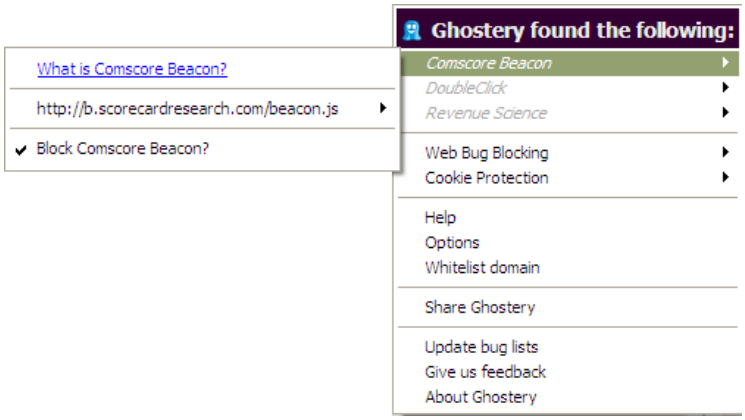

Figure 12: The Ghostery options that appear when a user clicks on its icon in the toolbar. A user is able to block or unblock particular trackers.

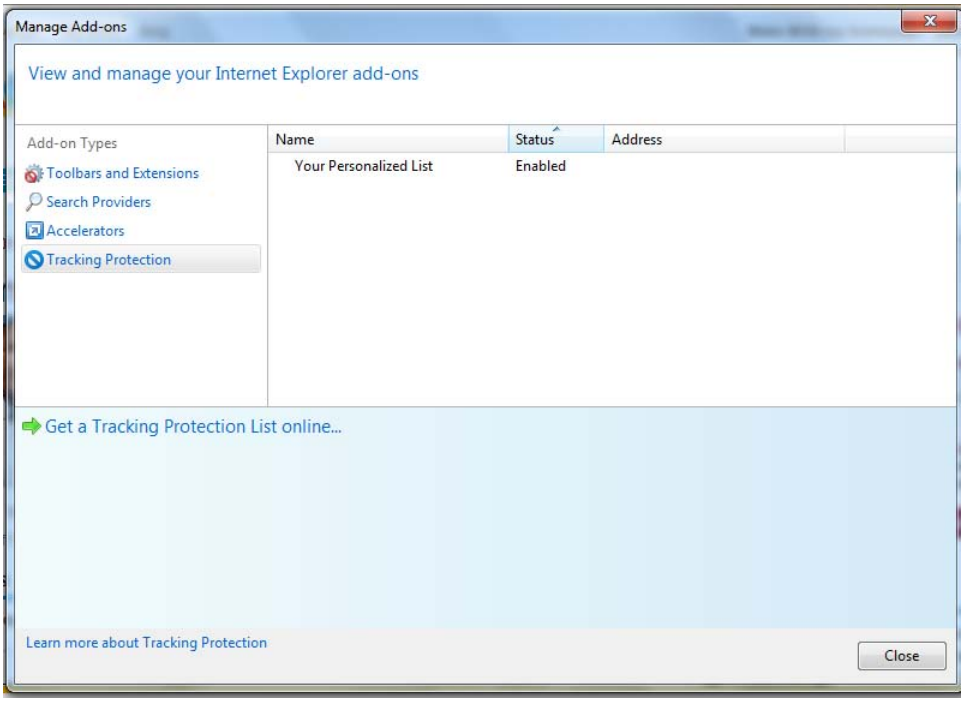

Figure 13: Internet Explorer's Tracking Protection List configuration screen, after enabling "Your Personalized List." Users must click "Get a Tracking Protection List Online" to block tracking; participants in our study did not realize this.

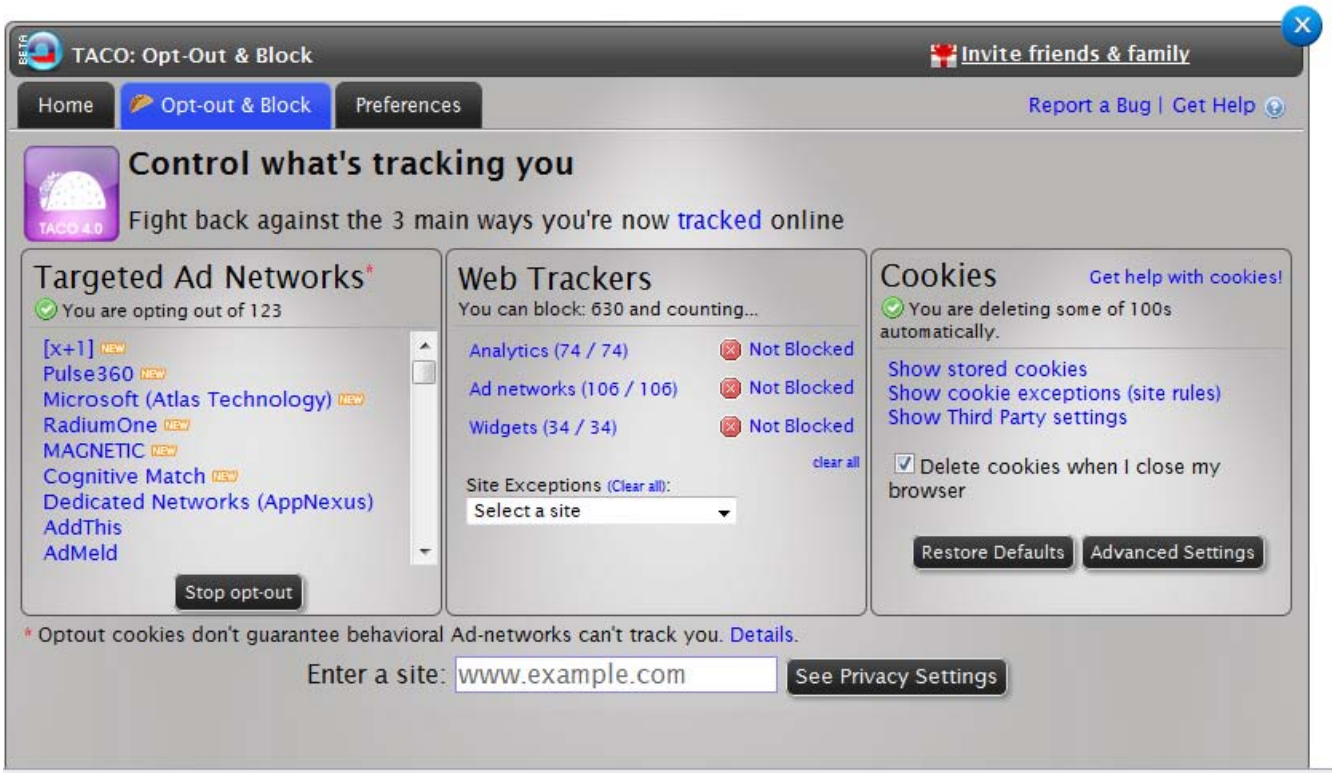

Figure 14: The interface for configuring TACO's blocking and opt-out features. Simply accessing this screen, which users found confusing, requires four steps. Once here, the user is presented with three categories of tracking: "Targeted Ad Networks," "Web Trackers," and "Cookies." The distinction between these categories was opaque to users. To enable blocking, a user must click on the three "Not Blocked" pieces of text that don't appear to be clickable. Even after choosing all three available categories, the user is informed, "You are blocking some of 630." No participants were ever told they were blocking all 630.

Figure 15: The alert TACO presents on each site a user visits. The distinction between "ad networks" and "web trackers" was confusing to users, as was the cumulative nature of "tracking attempts" stopped.

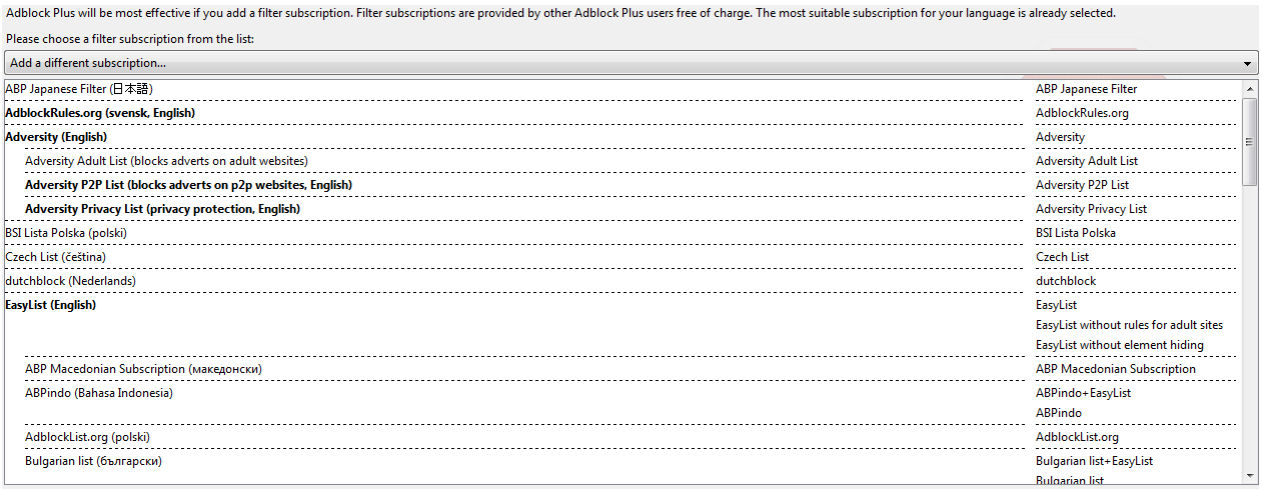

Figure 16: The main configuration screen for AdBlock Plus. The instructions at the top ask the user to subscribe to a filtering list. In contrast to Internet Explorer TPLs, all participants subscribed to a filter list when testing AdBlock Plus since the interface prompts the user to do so. However, subjects didn't know which filtering subscription to select or how to comparatively evaluate these subscriptions.

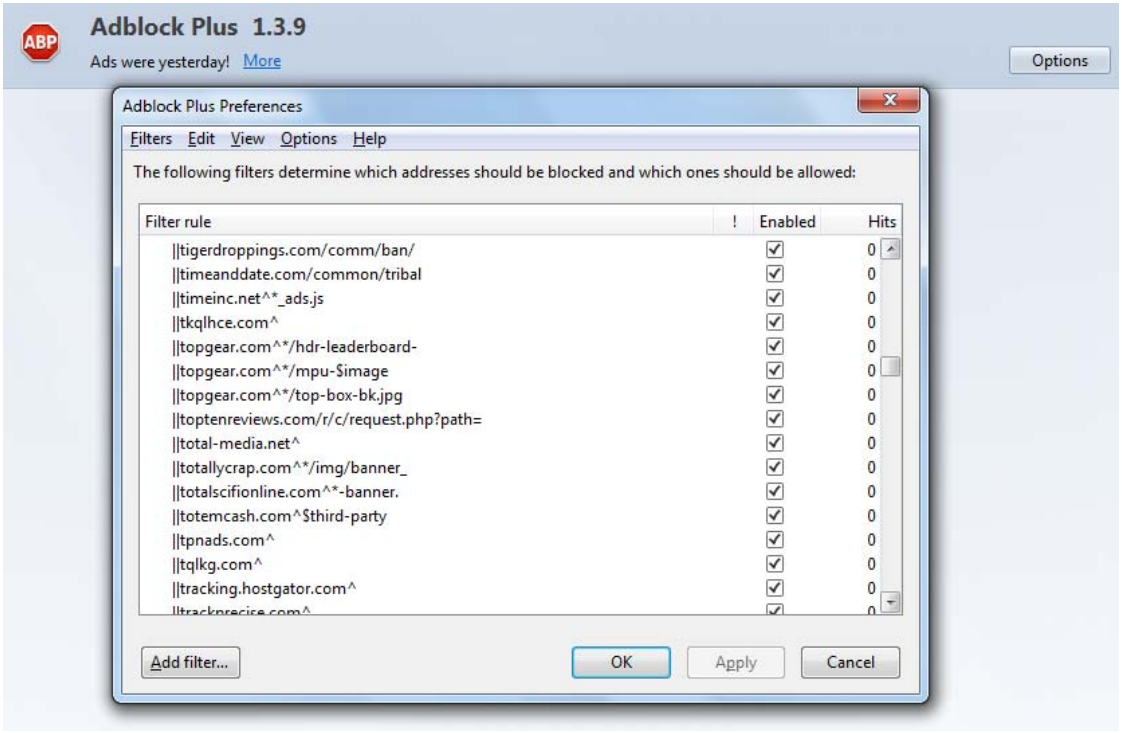

Figure 17: The options screen for AdBlock Plus, showing filter rules. Resolving problems was difficult for AdBlock Plus users since they didn't know which filters from a particular list had affected a particular website. If a user is trying to unblock filters that are causing problems on a website, she will be presented with an "options" screen containing all filter rules. Only experts can interpret these rules.

E Participants' opinions about tools

We summarize here what each participants told us about the tool he or she tested during the exit interview. In some cases participants' perceptions are not accurate or their comments reflect what they read about a tool more than what they personally experienced.

Tool	Features liked	Features disliked	Desired features	Benefits perceived
		Ghostery		
GH-1	Configuration on a per-tracker basis	None	Tutorial about trackers and tool usage	Controls information disclosure
GH-2	Ability to block advertising	Slow to configure	None	Not seeing ads
GH-3	Observing what trackers are on the web page, ability to block trackers on a web page	None	More contextual awareness	Controls information disclosure
GH-4	Seeing fewer ads, awareness of who is collecting data	None	Ability to remember choices	Fewer pop-up ads, awareness of trackers
GH-5	Awareness of source of ads, easy to configure, configuration on a per-tracker basis	Tool blocked a flash video	None	Control ads, controls information disclosure
		TACO		
TACO-1	Awareness of who is collecting data	None	None	Allows users to specify who can track them, provides better awareness
TACO-2	Not seeing ads, fill out forms, removing cookies	None	None	Prevents all ads, removes cookies
TACO-3	Awareness of who is collecting data, awareness of blocked ads	None	None	Prevents tracking
TACO-4	Awareness of trackers	Difficult to use, creates false sense of security	Option to block all ads	Fewer ads
TACO-5	Awareness of trackers, ability to block trackers	None	Ability to block only certain trackers	Allows users to specify who can track them
		AdBlock Plus		
ABP-1	Not seeing ads	Difficult to use	Better interface, easier access to preferences	Fewer distractions
ABP-2	Easy to configure	None	More information about what is blocked	Protects privacy, fewer distractions
ABP-3	Easy to use	Unintuitive	Better notice that installation is successful	Fewer ads, prevents tracking
ABP-4	Easy to use	Contents of filter lists unknown	None	Less annoying ads, prevents tracking
ABP-5	Easy to install	Difficult to configure	Ability to allow desired ads, ability to preview blocked ads	Fewer ads, improved security
		IE TPL		
TPL-1	Ability to customize what is blocked	None	Better instructions, a help button	Provides more appropriate content in searches
TPL-2	Ability to customize what is blocked	Difficult to install and use	Better instructions	More privacy, blocks third-party cookies
TPL-3	Ability to customize what is blocked	Couldn't figure out how to personalize tracking list	Ability to know what is blocked, ability to unblock some trackers	Stops targetted ads
TPL-4	None	No feedback that tool is working	Feedback that tool is working	More privacy, controls information disclosure
TPL-5	Fewer ads	None	Notice that user is being tracked, mechanism for knowing which trackers to trust	Fewer ads

Table 3: Participants' opinions about blocking tools, paraphrased from exit interviews.

Tool	Features liked	Features disliked	Desired features	Benefits perceived
		DAA Consumer Choice		
DAA-1	Easy to configure/use	None	None	Controls information disclosure
DAA-2	Speed of configuration	Not knowing why companies participate, not knowing if opt-out will be honored	Would prefer blocking tool	Prevents some companies from targeting ads
DAA-3	Easy to configure/use	None	None	Allows users to specify who can track them
DAA-4	Easy to configure/use	Not knowing if opt-out will be honored	More companies to choose from, easier website navigation	Allows users to specify who can track them
DAA-5	Listing of companies offering opt-out	None	Indication of what opting out means	Less obtrusive ads
		Evidon Global Opt-Out		
EV-1	Listing of companies offering opt-out	"Select all" feature does not work	Notification of successful opt-out	Fewer ads, fewer third-party cookies
EV-2	The "select all" feature	"Select all" feature does not work, not knowing if opt-out will be honored	Make opt-out feature more prominent	Better awareness of which companies perform tracking
EV-3	Configuration on a per-tracker basis	None	Knowing the websites on which tracking is performed	Allows users to specify who can track them
EV-4	Configuration on a per-tracker basis	Not knowing if opt-out will be honored	More information about what the affiliations such as NAI and DAA are, assurance that the opt-outs are honored	Allows users to specify who can track them
EV-5	Easy to configure/use	Time-consuming to configure	Better organized list of trackers	More privacy
		Privacy Mark		
PM-1	Easy to configure/use	None	Assurance that the opt-outs are honored	Blocking search-based and contextual ads
PM-2	Not seeing ads	Unable to configure	Assurance that the opt-outs are honored, ability to configure preferences	Controls information disclosure
PM-3	None	Not knowing if opt-out will be honored	Assurance that the opt-outs are honored, ability to configure preferences	Controls information disclosure, fewer ads
PM-4	None	Lack of information about trackers, creates false sense of security	Assurance that the opt-outs are honored	None
PM-5	Configuration on a per-tracker basis	Time-consuming to configure	Assurance that the opt-outs are honored, ability to configure preferences	Controls information disclosure

Table 4: Participants' opinions about opt-out tools, paraphrased from exit interviews.

Tool	Features liked	Features disliked	Desired features	Benefits perceived
		IE Privacy Settings		
IE-1	None	Difficult to undo blocking	None	None
IE-2	Block tracking cookies	Difficult to configure	Notification of who is tracking and what collected information is used for	Allows users to specify who can track them
IE-3	Ability to configure third-party cookies	Lack of information about cookies	Assurance that the tool is working	Identity theft prevention
IE-4	Blocking pop-ups	None	None	Blocks third-party cookies, hides physical location
IE-5	Easy to configure	None	None	Blocks cookies
		Firefox Privacy Settings		
FF-1	Ability to stop specific websites from tracking, ability to see who is tracking	None	None	Fewer ads
FF-2	Ability to stop specific websites from tracking	None	Indicate which cookies are being used for tracking	Feeling of security, allows users to specify who can track them
FF-3	Not seeing ads	None	None	Controls information disclosure
FF-4	Block third-party cookies, clear browsing history, browse in private mode	None	None	More privacy
FF-5	Blocks websites	Difficult to remember what is blocked, perceived as ineffective	Simplify configuration	None

Table 5: Participants' opinions about built-in browser tools, paraphrased from exit interviews.

F Participants' understanding of tool capabilities

During the testing session, we asked participants multiple-choice questions that tested their understanding of the tools' capabilities. We asked some questions twice, once before and once after the browsing scenarios; we asked others only before or only after the browsing scenarios. Participants could respond with the answers true, false, or unsure. The tables in this section show the questions that the participants answered and the percentage of correct answers per tool. Overall, participants showed a lack of understanding about the tools' capabilities.

Question	Ghostery	TACO	ABP	IE-TPL	PrivacyMark	DAA	Evidon	Firefox	IE
I will not see advertising on webpages I visit	False (40%)	False (60%)	True (40%)	False (60%)	False (N/A)	False (80%)	False (100%)	False (80%)	False (80%)
I will be more secure from computer viruses	False (60%)	False (80%)	False (80%)	False (80%)	False (N/A)	False (20%)	False (40%)	False (20%)	False (0%)
While using this tool, if I delete the cookies that my browser has stored, I will protect my privacy even more	True (20%)	True (100%)	True (80%)	True (60%)	False (N/A)	False (0%)	False (20%)	True (60%)	True (80%)

Table 6: This table shows the questions that we asked only before the browsing scenarios, after completing the changing configuration task. The table contains the correct answer to each question for each tool, and the percentage of participants who answered correctly. PrivacyMark participants did not perform the changing configuration task and were not required to answer these questions. Firefox and IE settings participants exhibited a particular low understanding for the second question. DAA and Evidon participants exhibited a very low understanding for the third question. In particular, DAA and Evidon participants did not understand that deleting cookies would render the testing tool ineffective

Question	Ghostery	TACO	ABP	IE-TPL	PrivacyMark	DAA	Evidon	Firefox	IE
I can block particular advertising companies from delivering any ads to me	True (80%,80%)	True (60%,80%)	True (80%,100%)	True (60%,60%)	False (*,80%)	False (40%,60%)	False (60%,40%)	False (60%,60%)	False (20%,60%)
I will see fewer ads that are tailored to my interests	True (100%,80%)	True (60%,80%)	True (80%,80%)	True (60%,60%)	True (*,100%)	True (80%,80%)	True (100%,100%)	True (80%,100%)	True (60%,80%)
I can see which online advertising companies are delivering ads to me	True (100%,100%)	True (80%,100%)	True (40%,100%)	False (20%,40%)	False (*,60%)	False (40%,40%)	False (80%,20%)	False (60%,40%)	False (60%,60%)
I can block particular advertising companies from delivering ads that are tailored specifically to me	True (80%,100%)	True (100%,80%)	True (80%,100%)	True (40%,60%)	True (*,20%)	True (100%,100%)	True (80%,80%)	True (100%,20%)	True (40%,40%)
While using this tool, my computer won't download any cookies while browsing the Internet	False (40%,60%)	False (60%,80%)	False (60%,60%)	False (40%,80%)	False (*,60%)	False (40%,60%)	False (60%,60%)	False (40%,100%)	False (40%,60%)

Table 7: This table shows the questions that we asked both before and after the browsing scenarios. The table contains the correct answer to each question for each tool, and the percentage of participants who answered correctly before and after the browsing scenarios, respectively. PrivacyMark participants only answered these questions after the browsing scenarios. Blocking tools exhibited a clear improvement in understanding after having used the tool. DAA and Evidon participants did not show much improvement. Firefox and IE settings participants improved understanding for some questions but reduced it for some others, showing problems understanding the tools' capabilities.

Question	Ghostery	TACO	ABP	IE-TPL	PrivacyMark	DAA	Evidon	Firefox	IE
I can block all advertising companies from delivering ads that are tailored specifically to me	False (40%)	False (20%)	True (80%)	False (60%)	False (60%)	False (80%)	False (40%)	False (40%)	False (40%)
When I visit a website, I will never see any advertising based on other websites I've visited	False (40%)	False (60%)	True (60%)	False (60%)	False (80%)	False (60%)	False (20%)	False (40%)	False (40%)
I can decide when to allow websites that I visit to create a profile of me based on my activities on their own websites.	False (0%)	False (40%)	False (20%)	False (0%)	False (60%)	False (40%)	False (40%)	True (100%)	True (60%)
If I am visiting Amazon.com, I will not see advertisements based on other products I've viewed on Amazon.com	False (80%)	False (60%)	False (0%)	False (60%)	False (40%)	False (60%)	False (80%)	False (20%)	False (40%)
If an advertising company delivers ads to both Walmart.com and CNN.com, I could use this tool to prevent that advertising company from creating a profile of me based on the products I view on Walmart.com and the stories I read on CNN.com	True (100%)	True (80%)	True (60%)	True (80%)	False (40%)	False (20%)	False (0%)	True (60%)	True (60%)
It will be more difficult technologically for advertising networks to track which sites I visit	True (60%)	True (100%)	True (60%)	True (80%)	False (0%)	False (0%)	False (20%)	True (40%)	True (40%)

Table 8: This table shows the questions that were asked only after the browsing scenarios. The table contains the correct answer to each question for each tool, and the percentage of participants who answered correctly. Evidon, DAA and PrivacyMark participants' low understanding for the last two questions in this table suggests that participants incorrectly believe that these tools prevent tracking.