Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern

Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, Lorrie Faith Cranor
Carnegie Mellon University
{ fschaub, amarella, pok, bur, chaop, eforney, lorrie }@cmu.edu

***Abstract*—Third-party companies increasingly track users' web browsing behavior, which raises privacy concerns. A number of browser extensions inform users about this tracking, yet the extensions' impact on user attitudes has not been well studied. We conducted a 24-participant, qualitative lab study evaluating how three popular extensions (Ghostery, DoNotTrackMe, and Disconnect) influence users' privacy awareness and privacy concerns. Before using any tool, many participants assumed tracking occurs, yet were unsure of specifics. The extensions provided limited insight; participants remained uncertain who the tracking companies are, what data they collect, and for what purpose. While using a browser extension, participants reported increased privacy concern due to increased awareness of tracking, yet this concern was mitigated by feeling protected by the extension. However, some participants distrusted the extensions or concluded the extension would tracked them. While all three extensions provided some additional awareness, users remained confused about many aspects of data tracking.**

I. Introduction

Users are often unaware that technologies like embedded advertisements, analytics code, social widgets, and cookies enable third parties to track their web browsing for purposes like analytics and targeted adverting [13]. Third parties like Google, Facebook, and advertising networks track a user's activities across websites to generate detailed profiles of a user's interests for online behavioral advertising (OBA) [18]. However, many users are uncomfortable with targeted advertising [15], [20].

To address users' privacy concerns, websites and tracking companies inform users about their data practices through privacy policies and sometimes provide opt-outs. The underlying assumption is that making data practices transparent facilitates informed privacy decision making [6] and, once informed, users will take steps to protect their privacy [11]. However, privacy policies and opt-out tools are difficult to understand [9], cumbersome to use [10], and largely ignored by web users [6], [14]. A number of web browser extensions aim to empower users by displaying the tracking activities on websites they visit and enabling them to block known trackers.

We conducted a between-subjects, qualitative lab study with 24 participants to study whether and how such privacy browser extensions influence users' privacy awareness and concern. To this end, we selected three popular privacy browser extensions (Disconnect, Ghostery, and DoNotTrackMe) and created a placebo tool as a control. Through task-based, semi-structured interviews, we observed participants installing and using one of these extensions in a number of scenarios.

Before using any extension, many participants assumed in the abstract that some data about their web browsing and searches is collected, yet were unsure precisely what is collected, precisely who is collecting it, or why. Privacy concern depended on the user's engagement and familiarity with a website, as well as the site's reputation. The three extensions we tested each gave users some limited clarity about the names of companies collecting their information, but participants were still not sure who these companies were, what data they were collecting, or why they were doing so. Using an extension, participants' privacy concern increased due to their new awareness of the prevalence of tracking, yet this concern was balanced out by feeling protected by the extension. Furthermore, participants felt more concerned when they would be logged into an account because they felt more personal information was involved. Some participants worried that the extensions themselves were collecting their browsing data or doubted the effectiveness of the extensions.

We further analyze how particular interface elements shaped users' awareness and concerns, as well as which were ineffective or ignored. We discuss design recommendations for improving the user experience of privacy extensions.

II. Related Work

We discuss related work on privacy concerns and awareness in the context of online tracking and browsing, as well as specific privacy awareness tools and related usability studies.

A. Privacy Concerns and Awareness

Web users are concerned about third-party tracking [15]. Wills and Zeljkovic studied whether personalized reports derived from users' browsing history can improve their awareness of third-party tracking. They identified concerns about tracking, location access, and inferring demographics [22].

Privacy awareness enables users to form more accurate mental models of privacy risks and thereby better manage their online privacy in accordance with their expectations and privacy preferences [16]. In the context of online tracking, privacy awareness entails an understanding about what data is being collected by which entities for what purposes, what entities that information is shared with, and corresponding risks

USEC '16, 21 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2016.23017

and benefits [17]. Bergmann found that presenting specific elements of a privacy policy in close proximity to the required data positively impacts privacy awareness [4]. Malandrino et al. found that people without a technical background were likely to take steps to protect their privacy when made privacy aware [11]. Tsai et al. found that people are willing to pay a premium in order to purchase items from privacy protective websites when privacy information is made salient in search results [19]. Soft-paternalism through "nudging" aims to guide users towards better privacy choices [1], e.g., by providing real-time awareness about risks. Wang et al. [21] found that nudges can help reduce unintentional disclosures on Facebook.

B. Privacy Awareness Tools

Privacy awareness tools are designed to inform users about privacy policies and settings. They should avoid displaying jargon to users, simplify configuration, and convey information about the tool's capabilities and current state using persistent indicators [5]. Privacy Bird was an early browser privacy add-on that displayed colored icons and played bird sounds to inform users whether a website's privacy policy matched their preference settings [7]. To facilitate comparison of privacy policies across websites, Privacy Finder displayed privacy information in search engine results [19]. Kelley et al. designed and tested privacy nutrition labels, standard-format privacy website privacy notices similar to food nutrition labels [8].

A variety of web browser extensions, including those tested in this study, block web trackers, which Balebako et al. found generally effective in limiting targeted ads [3]. Extensions also inform users about trackers present on websites; our study focuses on this informational aspect. In a usability study of some browser privacy extensions, browser privacy features, and online opt-out tools, Leon et. al found users had difficulty configuring all the tools tested [10]. While we evaluate newer versions of some of these tools, we focus especially on their influence on privacy awareness and concern.

III. Overview of Browser Extensions Studied

Most browser privacy extensions focus on detecting and blocking third-party tracking. Some extensions aim to improve privacy awareness by indicating how many trackers were detected or blocked on the current website, linking to more information about trackers, and providing blocking controls. We studied three popular Chrome extensions that focus on privacy awareness: Ghostery,[1] Disconnect,[2] and DoNotTrackMe[3] (DNTMe). These extensions are similar in the features offered and information provided, but differ in *how* they present information to users. Next, we provide an overview of the extensions' user interface elements that communicate privacy-relevant information. We further assess their tracker-detection performance to objectively compare their effectiveness.

A. User Interface Elements

Each extension has an icon, a main panel, and documentation about privacy implications. Ghostery and DNTMe also display an alert bubble when a website loads.

[1]Ghostery v. 5.3.0, https://www.ghostery.com
[2]Disconnect v. 5.18.14, https://disconnect.me/disconnect
[3]DNTMe v. 3.2.1139, https://www.abine.com/donottrackme

Fig. 1: Icons of Ghostery, DNTMe, Disconnect, and control.

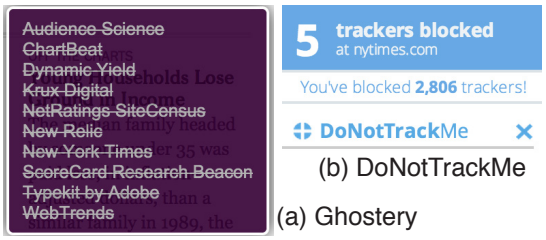


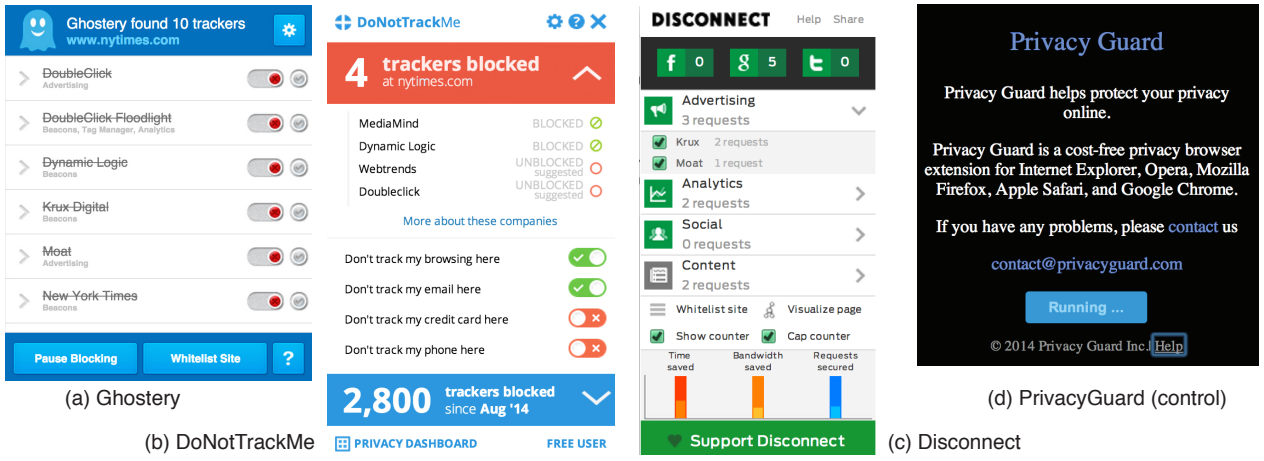
Fig. 2: Alert bubbles of Ghostery and DNTMe.

1) Extension icon & alert bubble: Figure 1 shows the icons that Ghostery, DNTMe, and Disconnect place in the Chrome toolbar. All icons contain a number indicating either detected trackers (Ghostery), blocked trackers (DNTMe), or the total number of tracking requests (Disconnect). DNTMe adjusts the background color when all (green) or only some trackers (orange) are blocked. Ghostery and DNTMe further temporarily show an alert bubble (Figure 2) when a page is loaded. Ghostery lists all detected trackers with blocked ones crossed out. DNTMe gives the number of trackers blocked.

2) Main panel: The main panel of each extension (Figure 3) can be opened by clicking the extension's icon. The top of Ghostery and DNTMe's main panels prominently display how many trackers have been found and blocked, respectively. In the same place, Disconnect displays specific counters only for Twitter, Google, and Facebook trackers. All extensions list third-party companies they have detected/blocked. Ghostery and DNTMe emphasize the tracker name/origin, while Disconnect groups trackers in expandable categories. Ghostery displays categories for trackers in smaller print below the company name. Clicking on a tracker name in Ghostery shows the tracker's URL and a link to a detailed profile of the company. Clicking on the name in Disconnect shows the company's website. DNTMe does not provide tracker-specific information; a "more about these companies" link leads to a general website that educates users about risks of online tracking and advertises DNTMe's premium version.

All three extensions let users block/unblock individual trackers. Ghostery distinguishes between blocking on the current website and all websites. By default, DNTMe allows "suggested" trackers, for which blocking would break website functionality. DNTMe shows switches to prevent browsing, email, credit card, and phone tracking; the latter two options require DNTMe's premium version. At the bottom of the screen, Disconnect estimates the time and bandwidth saved, as well as requests secured by blocking trackers. DNTMe shows the total number of trackers blocked since installation.

3) Installation & documentation: Ghostery and Disconnect each have a video on the Chrome Web Store explaining their functionality and third-party tracking in general. Disconnect's video emphasizes speed improvements and malware filtering. Ghostery's description is lengthy, whereas Disconnect and DNTMe's are succinct. After installation, Ghostery shows a configuration wizard letting users opt in to share information



(a) Ghostery (b) DoNotTrackMe (c) Disconnect (d) PrivacyGuard (control)

Fig. 3: Main panels of (*a*) Ghostery, (*b*) DoNotTrackMe, and (*c*) Disconnect, as well as the (*d*) control (Privacy Guard).

about trackers with Ghostery, explaining the alert bubble, and letting users configure blocking settings. The first time the user opens the main panel, Ghostery shows a tutorial explaining the blocking controls, such as pausing blocking and whitelisting the current site. DNTMe shows a post-installation page that only asks users to register. Disconnect shows neither a configuration wizard nor tutorial.

B. *Tracker Detection Performance*

To better understand the tracker data shown to users, we evaluated what trackers each tool detects on Alexa's top 100 websites.[4] We instrumented each extension to log trackers detected after 10 seconds on a page. Each extension was installed in a dedicated Chrome instance in a separate virtual machine. We collected data for all 100 websites three times per day on five consecutive days (12–2pm EST, June 30 – July 4, 2014). Based on the tracker URL, we correlated trackers across extensions. For example, Ghostery lists Google AdWords, Analytics, and AdSense as separate trackers, while Disconnect only shows a "g" letter summarizing all Google trackers. For DNTMe, in the absence of URLs, we manually mapped tracker names to Ghostery and Disconnect. Disconnect displays the number of HTTP requests, rather than the number of trackers. We matched these HTTP requests to unique trackers to facilitate comparison.

We found that Ghostery detected the most trackers, and more trackers per website on average (Figure 4). Ghostery detected 232 unique trackers (3.81 average per website), Disconnect 107 (3.10), and DNTMe 64 (3.42). Figure 4 shows the large variations across tools in the number of trackers detected on a given site. While Disconnect typically displayed a large number on its icon because it counts HTTP requests, not unique trackers, its detection rate was similar to DNTMe and lower than Ghostery.

IV. Methodology

We conducted a qualitative lab study to evaluate the effects of the privacy extensions on user's privacy awareness and concerns. Our goals were: (1) to understand users' baseline

[4]http://www.alexa.com/topsites, list retrieved on July 1, 2014.

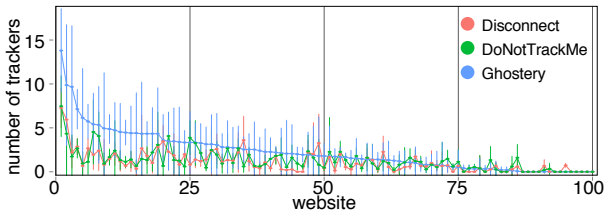


Fig. 4: Average number of trackers detected by each tool on the Alexa 100 (ordered by the average number detected by Ghostery). Error bars indicate standard deviation.

privacy awareness and concerns during browsing *without* using an extension; (2) to learn how each extension influences privacy awareness and concern; and (3) to understand the impact of different user interface elements. Our study was approved by CMU's Institutional Review Board.

A. *Study protocol*

We recruited 24 participants without a Computer Science background via Craigslist and flyers posted across the city. Participants came to our lab and chose either a Windows or a Mac laptop running the Chrome web browser. Before each session, the browser history was reset and all extensions uninstalled. Sessions lasted 39–86 minutes (median: 57 minutes) and were audio recorded and screen captured. Participants received $15.

Each participant was assigned one browser extension round-robin and completed browsing tasks on multiple websites. These tasks were integrated into a semi-structured interview. Participants were encouraged to think aloud during tasks. Participants completed three browsing tasks *without* a privacy extension, then installed the assigned extension and performed similar tasks *with* the extension installed. To install the extension, we guided participants to the Chrome Web Store and asked participants to familiarize themselves with the extension. Because Disconnect and DNTMe block tracking by default, we configured Ghostery to do the same.

The tasks required participants to research a given topic on a specified website. They researched one topic on three websites without the extension, and then researched a second

topic on the same websites with the extension. We selected websites (amazon.com, nytimes.com, veoh.com) to represent a range of popularity (high: Amazon, NYTimes; low: Veoh) and categories (retail, news, video). All participants knew Amazon and NYTimes, but none knew Veoh. Amazon had the fewest trackers (Disconnect: 1–19 requests; DNTMe: 1–7 trackers; Ghostery: 1–2 trackers), Veoh the most (Disconnect: 9–56; DNTMe: 1–14; Ghostery: 7–9), and NYTimes was in between (Disconnect: 4–39; DNTMe: 0–11; Ghostery: 3–16).

To identify two topics with similar perceived privacy concern for participants to research, we conducted an MTurk survey (n=100) in which participants rated their privacy concern for 14 privacy-sensitive terms identified by Marthews & Tucker [12] on a 7-point scale. Based on the results, we chose "depression" and "body odor" as a pair of search terms with similar concern ratings and meaningful search results on all three websites. To account for ordering effects, the order of websites was counterbalanced with a 3x3 Latin square, and the order of search topics was counterbalanced with two 3x3 Latin squares with inverted topic order. Thus, half of the participants researched "depression" first, the other half "body odor."

B. Control condition

Participants were assigned one existing extension (Ghostery, Disconnect, DNTMe) or a placebo extension, called PrivacyGuard. This control condition examined whether changes in privacy concern resulted from information provided by real extensions, or just an expectation of privacy protection. Our PrivacyGuard extension "helps protect your privacy online" and has an icon and a main panel (Figures 1 & 3d), yet no actual functionality or content.

C. Eliciting privacy concern and privacy awareness

In the interview part after each task, participants were asked to rate their privacy concern on a 7-point scale (*not at all concerned* (1) to *extremely concerned* (7)) and to explain the rationale for their rating. The rating served to help participants articulate their level of concern and provide anchoring for changes in their concern across the different tasks they performed. To measure privacy awareness, we asked participants after each task "Do you think that information about you is being collected or shared on this website?" If yes, we asked them (1) who was collecting/sharing what information, (2) for what purposes that information may be collect or shared, and (3) how comfortable they were with those practices.

We then asked participants to imagine they were researching the same topic while logged in with a personal account. They again rated and explained their concerns and described what collection or sharing practices take place (*with account*). Finally, we asked participants to imagine that the extension was no longer installed (*after extension*). Thus, participants rated their concern and answered the same questions in six situations for each of the three websites:

- M1: *before extension*
- M2: *before extension – with account*
- M3: *with extension*
- M4: *with extension – with account*
- M5: *after extension*
- M6: *after extension – with account*

The goal of these variations was to gain insight into relative changes in privacy concern before, with, and after using a privacy extension, as well as the impact of being explicitly identifiable by the first-party website (account). Therefore, we asked participants why their concern rating increased, decreased or remained the same. Following the browsing tasks, we also asked participants about the comprehension and utility of specific UI features.

D. Qualitative Data Analysis

All interviews were transcribed. Two authors developed an initial coding taxonomy from a subset of interviews and iteratively refined this codebook with iterative coding until sufficiently high inter-rater reliability was reached (Krippendorff's α=.84). Our final codebook contains 111 codes in 8 broad categories. It is structured in a multi-level hierarchy accounting for differences in each tool's features, leading to the large number of codes. We coded the remaining interviews independently, resulting in 2,623 annotations overall. We then conducted collaborative affinity diagramming to clarify and understand themes. We report the number of participants who expressed each theme, in order to give a better sense of our data. These numbers should not be interpreted to imply statistical or quantitative comparisons.

V. Results

We present participants' privacy awareness and concerns during the six browsing situations tested. Overall, the extensions gave participants some awareness of tracking, albeit incomplete and flawed. In most cases, the tool made participants feel somewhat protected from tracking. In each situation, participants felt more concern when they would be logged into an account, because personal information was involved.

Before using any extension, many participants held an abstract notion that data about their web browsing is collected, but they were unsure what is collected, who is collecting it, or why. The extensions provided some limited clarity about the names of companies collecting their information, but participants were still not sure who these companies were, what data they were collecting, or why they were doing so. With an extension, participants' privacy concern increased due to their new awareness of the prevalence of tracking, yet this concern was mitigated by feeling protected by the extension. However, some participants distrusted the extensions or felt that the extensions were collecting data about them.

A. Participant Demographics

Our 24 participants, six per condition, were 18 to 63 years old (median: 22) and most were female (62%). Over 60% had at least a bachelor's degree. They held a handful of occupations: student (14), admin (4), educator (2), and other (4). No participant reported being color blind. Fourteen (58%) had previously installed browser extensions. Most common were ad blockers (6) and a Reddit extension (2). One participant each had used Ghostery (P3) or Disconnect (P12) before; they were assigned different extensions in our study.

B. Baseline Privacy Awareness and Concerns (M1 & M2)

We first report participants' privacy awareness and concerns before installing an extension. Since they had yet to use an extension, we combine the participants from all conditions.

1) Privacy awareness: When completing the browsing tasks without a privacy extension (M1), all 24 participants assumed abstractly that information about them could be collected and/or shared. However, most participants had an incorrect model of who was collecting information and what they were collecting. Participants were often uncertain whether information was being collected: "It seems possible. It's really hard to tell. You have no way of knowing. I would assume probably some information, yes, is being collected about me." (P7). Four participants based their judgements on the ads shown on a website, which suggests they were looking for a direct effect of information being collected or shared.

Most participants thought the website they are visiting collects information (21), followed by advertisers and sponsors (11), and third parties in general (10). Interestingly, five participants assumed that the manufacturer of a product they viewed on Amazon or the creator of a Veoh video would also receive information about them. A few participants also assumed government agencies (4), ISPs (3), and browser creators (e.g., Google) (1) collect browsing information. Most participants assumed that information about their online activities (18) and searches (17) would be collected. Fewer were aware that this information enables inferences about their behavior and interests (8). Some participants mentioned information about their computer (7), primarily IP address (5). Others expected collection of personal information they entered (5), such as payment information (4) or their address (3).

Participants primarily stated that the purpose of data collection and sharing was general advertising/marketing (16), targeted advertising (12), analytics (14), and providing targeted recommendations on the site (10).

Overall, many participants had a general understanding that information about their browsing and searches may be collected about them for advertising, analytics, and recommendations. They had a less accurate picture, however, of exactly who was collecting information or how this information was being used to make inferences about them. Nearly all participants had difficulty making assertive statements about data collection, which is not surprising giving the opaqueness of the complex data-collection ecosystem. P13 exemplifies this uncertainty, responding to a question about who collects information by saying, "Not really sure. Definitely Amazon. I know when you look stuff up on Amazon, a second later all the banner ads are very similar to what you've been looking up. So I guess Google does banner ads and stuff, right?"

2) Privacy concerns before extension (M1): Prior to installing an extension, no participants expressed universal concern about their privacy. They either stated reasons for both concern and unconcern at the same time (14) or said they were completely unconcerned (10). Four main reasons for unconcern emerged: First, eight participants perceived data collection to be beneficial because they liked receiving tailored ads and recommendations. Thirteen participants were not concerned because they were not logged in to the websites, while six noted they had not shared anything personal with the websites and therefore assumed their actions could not be linked to them. Third, others were not concerned about the types of information they thought could be collected (13) because they were just browsing (7). For example, P15 stated, "I don't really care if someone on amazon.com sees I'm trying to buy deodorant. That's not really something that I would be embarrassed about." The website's reputation and popularity (10) was the fourth important factor. Participants trusted the website (9) with their data and expected a limited scope of collection (4). As P7 incorrectly explained, "It's not like they give this information to other companies, or at least it doesn't seem like there would be any reason for them to do that." Four participants expressed some concern, yet felt data collection was the unavoidable "cost of doing business on the Internet" (P3) or they "don't know how to avoid it" (P23).

Participants' stated concerns largely mirrored the reasons for unconcern. Participants were concerned because visited websites (11), ISPs (2), and the government (2) may track their online activities. Others specifically disliked targeted ads (5), which P12 explained were indicators of ongoing data collection. Some participants perceived their online activities as personal or sensitive (5), especially when doing more than just browsing (4) and when the website had personal information (2). Distrust of a website was a further reason for concern (8). Participants were less concerned with NYTimes than Amazon because they do not explicitly provide personal information to a news site. They were also less concerned with NYTimes than Veoh because they were unfamiliar with Veoh.

3) Privacy concerns before extension with account (M2): More than half of the participants (12) said they would be more concerned about privacy if logged into an account when browsing, but eight participants provided reasons for both increased concern and concern remaining the same depending on website. Participants noted increased concern because an account is often linked to personal information (12) and facilitates data collection (11). Both aspects result in higher exposure (12) because data collectors can link participants' online activities to them, including potentially sensitive searches (4). Linkage also may result in them receiving embarrassing recommendations (2). Concern also depends on the sensitivity of the activity. P19 explained, "I think my concern level depends on what I'm searching. Like, body odor is pretty general so I'm not very concerned about it...If I have some sort of sickness...I don't want people to know that I'm searching for it."

The main reason for privacy concern remaining the same was trusting the website (8), which entailed assuming that data would not be shared and that a reputable website would be secure. Others assumed that having an account would not change what information is being collected or shared (4). As P7 explained, "They're going to associate your buying habits regardless, based on whether you're using a computer or using your account. I don't think it's a whole lot worse. They're still going to know you're some person using a computer that's going to be searching for those things."

C. Awareness and Concerns with Extensions (M4 – M6)

The privacy extensions influenced privacy awareness and concern, yet were unsuccessful at helping participants better

understand third-party data collection. Participants learned from the extensions about a litany of companies tracking them, yet still did not know why these companies were present on the website, how they got there, or what data they were collecting. In this section, we discuss similarities and differences across the three treatment conditions. Afterwards, we discuss the control condition, which had negligible effect on privacy concern.

1) Privacy awareness: The extensions increased some participants' awareness of third-party tracking. However, none of the tools increased participants' understanding about the rest of the OBA ecosystem, such as why these companies are collecting data or what specific information they are collecting.

Before using Disconnect, four participants already named advertisers or third parties as entities collecting data about their browsing. After using Disconnect, one additional participant named third parties among data collectors. However, one participant who previously named third parties as data collectors became far more focused on Disconnect itself collecting his data. Other participants were confused about the OBA ecosystem in part due to the plugin showing a mix of unfamiliar companies and companies that were familiar from other contexts tracking them. For example, P10 noted that "Google or Clipsyndicate...seemed to be the most prominent [trackers]." Note, however, that Clipsyndicate was a video's creator on Veoh. P14's mental model was also incorrect; he assumed that other "illegal sites" would collect information to "see if they could steal videos or stream data from [Veoh]." DNTMe and Ghostery each also led one additional participant to name third parties as data collectors in addition to the four participants for each plugin who noted third parties before using the tool.

For Disconnect and DNTMe, some participants were concerned that not all third parties would be blocked, or that malware would be collecting information. P11 (DNTMe) was concerned about "the people who got around the tracker [tool] I guess. Some of the advertisers, malware, spyware...you kind of run into a little more risk with like a video website than you would in other places." None of the Ghostery participants voiced similar concern. However, in each group at least 1 participant (2 for Disconnect) assumed the extension itself would collect information about them. This concern seems to derive from the browser permissions the plugins require and which are therefore shown to users upon installation. When installing a privacy plugin, the user is told that the plugin will have access to all of their browsing. While this statement is technically true, it seemed to stir up skepticism for some participants absent any explanation why.

Prior to using a plugin, many participants felt that "browsing" data in the abstract could be collected. The extensions did not substantially impact awareness of what information may be collected beyond this pre-existing notion. Disconnect participants primarily named browsing (4) and interests (2) as the types of information that could be collected. DNTMe participants primarily named searches (5), browsing (3), personal information (3), and interests (2). Ghostery participants primarily named searches (4), browsing (2), and IP address (2). Unexpectedly, DNTME participants did not state browsing more frequently, despite DNTMe's prominent "Don't track my browsing here" option (cf. Figure 3b).

Furthermore, most participants were left unaware of why companies were tracking them. Although Disconnect and Ghostery explicitly refer to advertising and analytics in their main panels (cf. Figure 3), few participants mentioned these terms (2 Ghostery, 3 Disconnect). P14 (Disconnect) and P21 (Ghostery) incorrectly assumed that data would be collected to protect from malware or detect illegal activity (P14). P11 (DNTMe) misguidedly assumed data collection simply aims "to make sure they're not going on illegal websites or doing illegal things."

2) Privacy concerns with extension (M3): While all three extensions increased privacy awareness, they had different effects on privacy concern. Participants using DNTMe or Disconnect while browsing generally expressed increased privacy concern. In contrast, privacy concern remained the same as before installing the plugin for most Ghostery participants. This contrast stems from DNTMe and Disconnect participants either increasing or not changing their concern rating regardless of the website they were visiting, whereas some Ghostery participants' concerns decreased on particular websites while using the plugin.

Participants' reasons for changed or unchanged privacy concern were diverse. The most common reason given for privacy concern remaining the same was not perceiving any harm in tracking (4 DNTMe, 3 Ghostery, 2 Disconnect), due to just browsing (3), expecting to be tracked (1), or not being logged into an account (1). For Ghostery, some participants did not change their concern because either the plugin confirmed prior beliefs (1), participants worried about other entities (e.g., ISP) still collecting data (1), or feeling in control as a result of the plugin (1). In contrast, two Disconnect participants questioned the extension's effectiveness and two DNTMe participants felt uneasy about trackers despite the extension blocking them.

Most participants whose privacy concern increased as a result of the plugin cited increased awareness of the extent of third-party tracking as the reason (4 Ghostery, 3 Disconnect, 3 DNTMe). For instance, P10 (Disconnect) stated, "The volume of blocked items that came up [on Veoh] was a little shocking, especially compared to the other sites." Similarly, P5 (Ghostery) stated, "I'm more concerned just from the standpoint that now I have more information and I have a little bit more control...Before it was uninformed concern and there wasn't much I can do about it. And now it's informed concern and I can do something about it."

Disconnect and DNTMe participants stated additional reasons for increased privacy concern. P18 (Disconnect) and P7 (DNTMe) did not understand why the trackers detected would want to collect information about them, displaying a lack of understanding of the OBA ecosystem. P22 (Disconnect) and P11 (DNTMe) were worried that the first-party website would still collect information, which is in fact the case as these tools do not impact first-party tracking.

Other participants, however, increased their privacy-concern ratings primarily because of the extension itself, rather than their awareness of third parties. For example, P6 said, "I don't think I'm concerned about the New York Times. I'm concerned about Disconnect having this information all in one place about all of the websites." Of course, third

parties correlate information about visits to many websites over time, which P6 did not seem to consider. Some participants also generally distrusted their extension's effectiveness. For instance, P7, P15, and P23 expressed general distrust toward DNTMe due to DNTMe pushing its premium features. P7 explained, "You open this, it has some sort of counter that says all the trackers blocked. Why is that even necessary there? The only reason it even has it is because it's trying to advertise itself. So I don't feel like the point of the company is to help you."

Participants who lowered their privacy-concern rating generally felt the extension was effective at blocking (4 Ghostery, 2 Disconnect, 1 DNTMe). In notable contrast to other tools, more than half of the participants using Ghostery lowered their concern rating for this reason. P13 explained, "This is a lot more [trackers] than I was thinking there would be. The more it blocks, the more it makes me feel better."

3) Privacy concerns with extension with account (M4): Overall, when assuming being logged into an account while using a privacy extension, participants' privacy-concern ratings increased for all three extensions. DNTMe and Disconnect participants felt being logged in facilitated data collection, and they furthermore questioned their extension's effectiveness and trustworthiness. In essence, the extension increased privacy concerns rather than mitigating them. In contrast, half of the Ghostery participants decreased their concern rating compared to M2 (logged into an account, yet without any privacy extension) because they trusted Ghostery to protect them.

Four DNTMe participants increased their concern rating because accounts are associated with personal information. P19 was additionally concerned "because all these websites...listed here, I have no idea what they are...I'm concerned, I'm not sure what they are collecting or why are they trying to access here." In contrast, P11 and P15 decreased their ratings because they trusted the plugin to protect them. Notably, while being logged into an account ostensibly facilitates more accurate tracking by a first party, being logged into an account does not necessarily facilitate third parties' data collection.

Other DNTMe participants did not change their concern rating because they were not worried about the information that may be collected (2), previously believed data collection occurs (1), or assumed the information collected would not be shared (1). Two participants were aware of information collection, yet nonetheless were unsure how to evaluate risk. P11 explained, "Once you're logged in, even with the [extension], there's so many different places to input information...you might not even realize [it] goes anywhere else."

Similarly, Disconnect participants who did not change their concern rating previously expected data collection (1), were unconcerned about it (1), did not acknowledge the privacy tool in their reasoning (2), or did not know how to evaluate associated risks (2). Reasons for increased privacy concern also mirrored those of DNTMe; participants were concerned that accounts facilitate data collection (3). P6 was further concerned that Disconnect itself would collect information, while P14 questioned DNTMe's effectiveness, saying, "I'm pretty sure this plugin, it's not catching all of them...since the data world is huge."

4) Privacy concerns after extension (M5 & M6): We were also interested in participants' privacy concerns when considering browsing without an extension after they had used one and ostensibly had increased awareness about tracking as a result of previously using the extension. Privacy concern increased substantially compared to M3 for Ghostery and Disconnect, but it increased only marginally for DNTMe. For all three extensions, however, privacy concern increased substantially compared to participants' concern before installing the extension (M1 & M2). This result suggests that the extensions were effective both at increasing overall privacy awareness and at making participants feel somewhat protected from tracking.

No participants' concern ratings decreased. Primary reasons for increased concern were awareness about tracking (4 Disconnect, 4 Ghostery, 3 DNTMe) and a perceived lack of protection without the extension (4 Disconnect, 4 Ghostery). Participants whose concern did not change noted that despite awareness of tracking, they did not consider their browsing sensitive unless they were logged into an account (3 Disconnect, 3 DNTMe, 2 Ghostery). Some did not mind tracking (3 Disconnect), or trusted that the website would not collect sensitive data (2 (Ghostery). For P6 (Disconnect) and P7 (DNTMe), taking away the extension removed the risk of the extension collecting data about them, which balanced an increased risk of third party tracking. P6 explained, "If the plugin is not installed, they're not stopping anything, but they're [the extension itself] not housing anything either."

Assuming the same situation but with an account (M6) led to a slight increase compared to M4 and M5 for all extensions. The primary reasons for increased concern were a perceived lack of protection (4 Disconnect, 3 DNTMe) combined with an account facilitating data collection (2 Disconnect, 2 DNTMe, 2 Ghostery). Participants whose concern remained the same stated that creating an account requires providing information (3 Disconnect, 3 DNTMe, 3 Ghostery), which led them to expect information being collected (3 DNTMe, 2 Disconnect, 1 Ghostery). P15 (DNTMe) and P22 (Disconnect) did not change their concern for NYTimes because they rarely used the website and incorrectly assumed no information about them would be collected because "it's just a news website...It's not trying to gain information from me, I don't think" (P15).

5) Control condition: In the control condition, we observed almost no change in concern ratings between M1, M3, and M5. However, when participants imagined being logged into an account, the PrivacyGuard extension reduced concerns, similar to Ghostery. All six participants in the control group felt that PrivacyGuard did not explain its functionality. In the absence of this information, participants primarily speculated that it prevented information collection (4). For five of the six participants, however, the vague explanations about functionality led them not to change their privacy-concern rating while using PrivacyGuard (M3) because they assumed it did not impact privacy (3) or they felt their activities were not sensitive (3). Two participants increased their concern rating because they were skeptical of PrivacyGuard; two others lowered their concern rating because they did not see evidence of targeting.

When participants imagined being logged in (M4), participants' concern remained mostly the same, in contrast to other tools. PrivacyGuard participants said they trusted the website (3), perceived their activities as not sensitive (2), did

not expect information to be collected due to a lack of visible changes to the website when using PrivacyGuard (2), or were skeptical of PrivacyGuard (2). In contrast, participants in the three treatment conditions generally increased their privacy concern, suggesting that these increases were attributable to increased awareness of tracking from information provided by Ghostery, Disconnect or DNTMe.

When participants assumed the extension was no longer installed (M5 & M6), we found a limited placebo effect for 2 participants who felt a lack of protection without PrivacyGuard. Although there was some placebo effect related to feelings of protection, many of the changes in privacy concern for Ghostery, DNTMe, and Disconnect seem attributable to the real extensions' actual functionality.

D. Effectiveness of User Interface Elements

We further analyzed the screen and audio recordings to study how participants interacted with the extensions in order to understand how specific UI elements impact privacy awareness and concern. We also asked them about their perceptions and utility of specific UI elements at the end of the interview. While the information provided during installation and shown on the extensions' icons gave participants some awareness of blocking, many participants were left confused about the overall tracking ecosystem and what precisely the tools were communicating.

1) Installation and documentation: The installation process and associated documentation for each tool, including videos and tutorials, helped participants gain a better understanding of the functionality and purpose of the extensions. However, confusing descriptions and use of jargon (e.g., "invisible websites") also led to skepticism.

Across conditions, almost all participants inspected the information provided in the Chrome Web Store before installing the extension. Some (4 Disconnect, 1 Ghostery) also watched the video provided. A small number of them visited the extension's help pages (2 DNTMe, 1 Disconnect, 1 Ghostery). For Disconnect, the information provided increased awareness about tracking (4) and convinced participants that pages will load faster (3). However, two participants were not sure if requests are actually blocked, while one was confused about the term "invisible websites" used by Disconnect to refer to trackers. For DNTMe, four participants felt this information provided awareness about tracking, yet two felt uncertain whether DNTMe blocks trackers. All six participants noticed DNTMe's premium features. However, the information requested during setup (email, credit card) made some skeptical of DNTMe (2). Similar to DNTMe, three of the six Ghostery participants gained awareness of tracking and that Ghostery stops information from being sent.

In addition to information provided by the extension, many participants read user reviews before installation (6 DNTMe, 4 Disconnect, 4 Ghostery), which led to increased confidence in Ghostery (3), but mixed perceptions for Disconnect and DNTMe. For Disconnect, the reviews convinced one participant that it collects users' information, one became more skeptical, whereas another participant gained confidence. For DNTMe, two participants gained some confidence, while one became skeptical due to mentioned spam emails and annoying pop-ups. Another aspect that fostered skepticism for Disconnect were the required browser permissions (2). As P18 said, "Okay, so it accesses all my data on all my websites, it reads. How is this any better than regular?"

2) Extension icon & alert bubble: Each tool has an icon in the browser toolbar. Participants that noticed the icon's changing numbers used the icon as guidance to calibrate privacy concerns and as a trigger to probe further. However, the icons' small size prevented some participants from noticing it, which was particularly common with DNTMe.

Four of the six Disconnect participants paid attention to the icon and understood that it showed blocked requests, although two thought it indicated blocked companies or websites. Four of the six noticed the number changing across websites, which shaped their perception of these websites. P10 explained how "being more aware of exactly what was happening each time I was on the site made it easier to quantify how I was feeling." P1 did not notice the icon at all. P22 noticed it, yet did not interact with it "because once I install an extension I kind of forget about it and just assume it's working."

All six Ghostery participants paid attention to the icon, although two did so only minimally. While five of the six understood that the number indicates privacy threats or blocked third parties, P5 mistakenly thought it indicated the number of searches. Three participants thought the icon shaped their perception of a website. For example, P9 said, "It makes me think that the website that has a higher number of third parties that is potentially more harmful and less safe to use."

Only three DNTMe participants paid attention to the icon, while the other three did not notice the number changing. Asked why, P15 stated, "It's little and it's in the corner." Asked about its meaning, all six participants understood that it indicated the number of blocked trackers. However, only P3 noticed the icon's color changing and reacted by opening the main panel, explaining, "Now the little number by the plugin is yellow, which seems more alarming than green, and it says that one of these tracker sites is unblocked but suggested to be blocked, so that seems bad." Five of the six participants correctly realized colors indicated current privacy risk.

Similar to the icon, Ghostery's and DNTMe's pop-up alert bubbles triggered half of the participants in each condition to open the extension's main panel to learn more. Two participants had noticed Ghostery's alert bubble, but thought that it was gone too quickly. P7 became annoyed with DNTMe's alert bubble, saying, "Whenever it blocks some things it comes up with this little window that says, 'You've blocked seven trackers.' Why is that necessary? It seem unnecessary clutter. It's trying to prove to you how awesome the program is so you'll buy some premium version of the program."

3) Main panel: Clicking on each tool's icon brings users to a main panel. Overall, tools' main panels helped participants gain privacy awareness. However, the jargon employed and manner of presentation often confused participants, causing skepticism and distrust.

Most participants opened the main panel unprompted while browsing (5 Disconnect, 5 Ghostery, 4 DNTMe). Most of these users felt the list of trackers increased privacy awareness and increased their privacy concern (5 Ghostery, 4 DNTMe,

2 Disconnect). However, most participants stated they were unfamiliar with some or all of the companies listed, which led to increased concern (5 DNTMe, 4 Disconnect, 3 Ghostery). For instance, P10 (Disconnect) said, "It made me more aware of where specifically the requests were coming from...I saw a bunch of advertising things that I didn't recognize that made me more uncomfortable." Some participants did not understand what trackers were doing on the visited sites (2 Disconnect, 2 DNTMe), providing another example of these extensions' ineffectiveness at communicating comprehensible information about the data-collection ecosystem. Furthermore, P7 (DNTMe) did not know how to utilize this information, saying, "The thing about esoteric information like this is that it's just there to be reassuring." P3 (DNTMe) tried to interpolate a tracker's purpose from the listed company name.

Hardly any participant accessed the additional information the extensions provide. Only P18 looked at Disconnect's "visualize page" feature and clicked on a tracker name to open its website. For DNTMe, three participants noticed the "more about these companies" option, yet assumed that it would not provide useful information and thus did not click on it. Four participants did not look at the privacy dashboard, believing a "dashboard" would necessarily be complicated (P19).

Understanding of Disconnect's four categories of trackers varied. All six participants understood "advertising," although only three mentioned targeted ads. Only one interpreted "analytics" correctly. P18 was confused by the listed analytics companies, saying, "I think I came across Oracle as one, so software, and, just interface websites, that's analytical." The other four participants had no idea. Three of the six participants understood the "social" category. One participant incorrectly assumed it related to self-help groups for the topic researched (depression). Only two participants understood "content" correctly. Wrong interpretations included "the browser I'm using" (P1), "competing websites" (P18), and recommendations for similar content (P6). The bars at the bottom of Disconnect's main panel were not meaningful to participants, and the term "requests secured" caused particular confusion. P18 explained, "That one I was a little concerned about because it didn't show that all the requests were secured. So request security would mean that these requests haven't been approved."

For DNTMe, all six participants correctly interpreted the large number on top indicating how many trackers were blocked. However, one participant was confused by diverging numbers shown in the main panel and on the icon (blocked versus trackers detected). DNTMe unblocks certain trackers by default when they may break the website and marks those as "suggested" (cf. Figure 3c). Only two participants understood this. Three participants thought it was a suggestion for the user to block them manually, while one assumed the premium version was required to block them. DNTMe's settings sliders were somewhat misleading. Two participants assumed that the first-party website would be prevented from tracking. All participants understood the abstract meaning of the "total number of trackers blocked," yet some were not sure whether the number indicated unique trackers (1) or if it referred only to the current website (1). DNTMe's advertisement of its premium features also led participants to be concerned about DNTMe itself collecting their data.

Ghostery's main panel did not provide many features beyond listing trackers on the current site. P5 was confused by the block/unblock controls next to a tracker's name (cf. Figure 3a), saying, "Red means that they're active, right? No, red means that they can't be stopped, correct?...So there's ten different trackers and they have a slash through them, which means they're all currently blocked. Is that correct?" Similar to Disconnect, all Ghostery participants understood the "advertising" tracker category, yet only half mentioned targeted ads. In contrast to Disconnect, five of the six participants also had a good understanding of "analytics." A likely explanation for the difference is that Ghostery lists more familiar trackers (e.g., Google Analytics) in this list, whereas Disconnect abstracts Google Analytics into the "g" icon. However, in line with prior work [10], five of the six participants had no idea what "beacons" (5) or "widgets" (5) were. P2 tried to make sense of the term "beacons" without success, saying, "The only theory I have is that it works the same as my XBox: It flashes you a beacon when someone is playing the same game as you...But I don't know how it would work here. If someone else is searching for body odor too, it doesn't make sense."

VI. Discussion

We discuss both the limitations of our study and our results' implications for the design of privacy extensions.

A. Limitations

As our goal was to gain nuanced insights, we opted for a qualitative study with 24 participants, rather than a larger scale quantitative study that may have allowed statistical analysis of differences between conditions. While we considered only a limited number of websites and search topics, the websites and search topics served primarily to guide the tasks and encourage interaction with the browser extensions. The lab setting may have further impacted participants responses, however, we found no indications in our interviews that participants misrepresented their concerns. The majority of participants also self-reported that their concerns would be the same when using their own computer, while some stated that they would feel less or more concerned. Because participants only interacted with extensions in a single session, our results do not account for potential habituation effects. Due to the repeated measures design, participants may have been primed about privacy in later questions; we counterbalanced the study to reduce such priming effects. Self-evaluation of privacy concerns can be unreliable due to the anchoring heuristic [2]. Therefore, we focused on participants' relative changes in concern without and with the extension rather than the absolute reported ratings.

B. Design Implications

1) The icon is essential: Participants who noticed that the extension's icon changed, based their privacy concern directly on the icon's number or opened the main panel to investigate further. However many participants did not notice the icon's number changing, perhaps due to the icon's small size. Despite the focus on showing the number of trackers/requests, none of the studied extensions facilitated understanding of a lower or higher number's privacy implications compared to zero trackers. Furthermore, our tracker analysis shows that the most popular websites have very similar and fluctuating numbers of

trackers, which suggests a risk of habituation for users. Thus, instead of focusing on the number of trackers, an indication of the privacy risks associated with specific trackers or tracker categories may be worthwhile to explore. Selective use of icon color can further draw the user's attention to critical situations, such as certain trackers not being blocked, unrecognized external code, or when blocking breaks the website's functionality.

2) Use alert bubble sparingly: Despite their visual presence, most participants did not notice Ghostery's and DNTMe's alert bubbles. Those that did, found them either useful or particularly annoying. Showing these notifications for each website has the same habituation issues as the icon. Basically, users noticing them now, will likely stop processing them over time. Instead of showing alert bubbles on every visited website, they could be used sparingly to only highlight exceptional situations that deviate from expectation.

3) Integrated explanations: While some of our participants opened an extension's main panel, very few accessed any additional information linked there. They expected it to be too complicated or unnecessary. This suggests that any information deemed relevant should be presented in the main panel. The key here is to ensure that included information is actually relevant and actionable to users. This extends to the terminology used in privacy extensions. The extensions used confusing jargon in their main panels and setup material, including terms like social, analytics, widget, or beacon that did not make sense to users in the context of a privacy extension.

4) Setup experience: Our results show that clear setup materials, including videos and tutorials, shape users' mental models of the extension's functionality and help them trust the extension. Insufficient guidance results in misconceptions and uncertainty about functionality and effectiveness, even suspecting that the extension is maliciously collecting data. For instance, the purpose of required browser permissions should be clearly explained, as well as any information requested from users. DNTMe's request for email address and credit card data during setup resulted in increased privacy concern for multiple participants – likely reducing their willingness to purchase advertised premium features.

5) Emphasize why and what: The evaluated privacy extensions were effective at enhancing awareness about who is collecting or sharing information, mainly by listing tracker names. However, participants did not know who most of these companies were and struggled with the extensions' categorization of trackers. Hence, participants lack a frame of reference to determine associated privacy risks and implications. There is need to further investigate approaches for informing users about why these trackers are present, what they are collecting or sharing, and how they use obtained information. While some extensions, like Ghostery, provide links to further information, the information is not accessed and hence not effective.

In conclusion, our 24-participant interview study provided insights into how browser privacy extensions influence privacy awareness and concern. While we find a positive overall effect, current privacy extensions suffer from usability problems that hinder their effectiveness. We presented insights for improving the user experience and design of privacy browser extensions. We believe that our results are relevant for developers of such extensions, as well as browser manufacturers, website operators, and even mobile app developers, who can leverage our results to improve how they communicate privacy risks and implications to users in order to increase their trustworthiness and credibility with customers.

ACKNOWLEDGEMENTS

This research was partially funded by the National Science Foundation under grant agreements CNS-1330596 and CNS-1012763.

REFERENCES

[1] A. Acquisti, "Nudging privacy: The behavioral economics of personal information," *IEEE Seurity & Privacy*, vol. 7, no. 6, pp. 82–85, 2009.

[2] A. Acquisti and J. Grossklags, "What can behavioral economics teach us about privacy?" in *Digital Privacy*. Auerbach Publications, 2008.

[3] R. Balebako, P. G. Leon, R. Shay, B. Ur, Y. Wang, and L. F. Cranor, "Measuring the effectiveness of privacy tools for limiting behavioral advertising," in *Proc. W2SP*, 2012.

[4] M. Bergmann, "Testing privacy awareness," in *The Future of Identity in the Information Society*. Springer, 2009, pp. 237–253.

[5] L. F. Cranor, "Privacy policies and privacy preferences," in *Security and Usability*. O'Reilly, 2005, pp. 447–472.

[6] ——, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice." *J. Telecomm. & High Techn. Law*, vol. 10, no. 2, pp. 273–308, 2012.

[7] L. F. Cranor, P. Guduru, and M. Arjula, "User interfaces for privacy agents," *ACM TOCHI*, vol. 13, no. 2, pp. 135–178, 2006.

[8] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A nutrition label for privacy," in *Proc. SOUPS*, 2009.

[9] P. G. Leon, J. Cranshaw, L. F. Cranor, J. Graves, M. Hastak, B. Ur, and G. Xu, "What do online behavioral advertising privacy disclosures communicate to users?" in *Proc. WPES*, 2012.

[10] P. G. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. F. Cranor, "Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising," in *Proc. CHI*, 2012.

[11] D. Malandrino, V. Scarano, and R. Spinelli, "How increased awareness can impact attitudes and behaviors toward online privacy protection," in *Proc. PASSAT*, 2013.

[12] A. Marthews and C. Tucker, "Government Surveillance and Internet Search Behavior," SSRN, working paper, 2014, http://papers.ssrn.com/abstract=2412564.

[13] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: Policy and technology," in *Proc. IEEE SP*, 2012.

[14] A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, no. 3, pp. 540–565, 2008.

[15] ——, "Beliefs and behaviors: Internet users' understanding of behavioral advertising," in *Proc. TPRC*, 2010.

[16] L. Palen and P. Dourish, "Unpacking "privacy" for a networked world," in *Proc. CHI*, 2003.

[17] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *The Future of Identity in the Information Society*. Springer, 2009.

[18] A. Rao, F. Schaub, and N. Sadeh, "What do they know about me? contents and concerns of online behavioral profiles," in *Proc. PASSAT*, 2014.

[19] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research*, vol. 22, no. 2, pp. 254–268, 2011.

[20] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang, "Smart, useful, scary, creepy: Perceptions of online behavioral advertising," in *Proc. SOUPS*, 2012.

[21] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh, "A field trial of privacy nudges for facebook," in *Proc. CHI*, 2014.

[22] C. E. Wills and M. Zeljkovic, "A personalized approach to web privacy: Awareness, attitudes and actions," *Information Mgmt. & Computer Security*, vol. 19, no. 1, pp. 53–73, 2010.