Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode

Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar†, Sascha Fahl†, Blase Ur
University of Chicago, †Leibniz University Hannover
{yuxiwu,panyagupta,weim,blase}@uchicago.edu, {acar,fahl}@sec.uni-hannover.de

ABSTRACT

All major web browsers include a private browsing mode that does not store browsing history, cookies, or temporary files across browsing sessions. Unfortunately, users have misconceptions about what this mode does. Many factors likely contribute to these misconceptions. In this paper, we focus on browsers' disclosures, or their in-browser explanations of private browsing mode. In a 460-participant online study, each participant saw one of 13 different disclosures (the desktop and mobile disclosures of six popular browsers, plus a control). Based on the disclosure they saw, participants answered questions about what would happen in twenty browsing scenarios capturing previously documented misconceptions. We found that browsers' disclosures fail to correct the majority of the misconceptions we tested. These misconceptions included beliefs that private browsing mode would prevent geolocation, advertisements, viruses, and tracking by both the websites visited and the network provider. Furthermore, participants who saw certain disclosures were more likely to have misconceptions about private browsing's impact on targeted advertising, the persistence of lists of downloaded files, and tracking by ISPs, employers, and governments.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; *Browser security*;

KEYWORDS

Private browsing, Web browser privacy, Usable privacy, User study, Incognito mode, Private browsing mode

ACM Reference Format:
Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar†, Sascha Fahl†, Blase Ur. 2018. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *WWW 2018: The 2018 Web Conference, April 23–27, 2018, Lyon, France.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3178876.3186088

1 INTRODUCTION

Each of the five web browsers widely used today — Chrome, Edge, Firefox, Safari, and Opera — offers a private mode that stops storing browsing history and caching data across sessions. Unwanted information from the user's browsing history will not appear in the history bar, auto-filled forms, or search suggestions. Private modes thus help users hide browsing sessions from people sharing a device with them.

While these private modes aim not to save user data locally, many threats to privacy are outside their scope. For example, private mode does not aim to prevent tracking over the network. While browser cookies do not persist across private browsing sessions, this is a minor barrier to tracking by third-party advertising and analytics companies, who can employ more sophisticated fingerprinting techniques [14, 17]. Furthermore, implementations are imperfect, often leaving some traces of local activity [1, 36, 47].

Despite the limited protections private modes provide, some users overestimate these protections [13, 20]. This overestimation reaches far; Eric Schmidt, former CEO of Google, once stated, "If you're concerned, for whatever reason, you do not wish to be tracked by federal and state authorities, my strong recommendation is to use incognito mode, and that's what people do" [38].

In this paper, we take initial steps toward unpacking these misconceptions by conducting a user study of how browsers' own explanations of private mode impact users' understanding of what these modes do. Browsers differ in how they explain private mode; even the mode's name differs (e.g., "Incognito Mode" in Chrome, "InPrivate" in Edge, and "Private Browsing Mode" in Firefox). We focus on the *disclosure*, or full-page explanation browsers present when users open a new window in *private mode* (the catch-all term we use across browsers). Notably, disclosures often differ between a given browser's desktop and mobile versions.

We conducted a between-subjects online study in which 460 participants each saw one of 13 different disclosures (the desktop and mobile disclosures of six popular browsers, plus a control disclosure) rebranded for a hypothetical new browser. Participants answered questions about what would happen in twenty different browsing scenarios. In some of these scenarios, private mode protects the user's privacy, while the other scenarios encapsulate previously documented misconceptions [13, 20] about private mode.

We found that participants had many misconceptions, including beliefs that private mode would prevent geolocation, protect from malware, eliminate advertisements, and prevent tracking by the websites visited and network providers. The particular disclosure participants saw impacted their misconceptions. Compared to a meaninglessly vague control condition, the current and previous Chrome desktop disclosure led participants to answer more scenarios correctly; no other disclosure we tested had a significant effect. Participants who saw certain disclosures were more likely to have misconceptions about private mode's impact on specific scenarios: targeted advertising, the persistence of lists of downloaded files, and tracking by Internet service providers (ISPs), employers,

WWW 2018, April 23–27, 2018, Lyon, France

ACM ISBN 978-1-4503-5639-8/18/04.
https://doi.org/10.1145/3178876.3186088

and governments. Phrases used in some disclosures (e.g., "tracking protection") appear to contribute to misconceptions.

While prior work has documented misconceptions about private mode, our study is the first to focus on the role browsers' disclosures play. These disclosures, which users see each time they open a new private browsing window, are the main vector for disabusing users of misconceptions that might derive from loaded names like "private browsing mode" and "incognito mode" [24, 39, 48]. While we found that some browsers' disclosures are better than others, all disclosures we tested failed to correct important misconceptions.

2 BACKGROUND AND RELATED WORK

We first summarize features of current browsers' private modes. We then discuss prior work on misconceptions about private mode and work on privacy communication more broadly.

2.1 Features of Private Browsing

All major web browsers include a private mode designed to protect against local privacy threats with physical access to a machine [1]. These modes aim to remove local copies of browsing history, temporary files, and cookies from a machine. That said, the implementation of these features is imperfect [1]. Xu et al. demonstrated that sophisticated attackers can still gain access to information from private sessions [47]. Similarly, Satvat et al. found vulnerabilities that enable sophisticated attackers and malware to steal information from private mode [36]. While such attacks are important to overall browser security, they are not the focus of our work. Instead, we study how users' expectations compare to private mode's intended protections. To determine these intended protections, we examined both browser-specific documentation and prior research on private modes. For potential behaviors that were not formally documented, we conducted informal experiments.

No browser intentionally stores browsing history from private mode after a session is closed [6, 21, 22, 28, 31, 34]. This guarantee does not at all apply to remote services; if a user is logged into an account, the provider of that account can certainly record the user's browsing activity [1]. Browsers aim to delete temporary files (e.g., cached files) when private sessions are closed. All browsers except Edge launch private browsing with fresh cookie storage; Edge uses the store from standard mode. All browsers clear cookies after the private session is closed. Across browsers, autofill information from standard mode is available when using private mode, but no browser offers to save autofill details automatically [6, 30, 34].

Private mode does not, however, protect against remote threats. With one exception, browsers' private modes do not alter the visibility of a user's IP address or otherwise change how traffic appears on the network. Only Opera's VPN feature [33] provides some limited protection. While it hides browsing activities from users' ISPs, Opera's VPN servers have the ability to snoop on their users' browsing behavior. Between this limitation and the opt-in nature of Opera's VPN, this tool's ability to prevent tracking is limited for most users. Also, Firefox[1] and Opera VPN provide protection against common tracking networks. Private mode also does not aim to stop all local activity. Files downloaded in private sessions remain afterwards, while all browsers we tested other than Brave do not save the list of files downloaded in private mode. All browsers can access existing bookmarks in private mode, and new bookmarks saved in private mode are available in future sessions [22, 31, 34].

Browsers differ somewhat in their private modes. Chrome and Edge do not save preferences (e.g., pop-up blocking, download locations) from private sessions, while Firefox and Opera do. Browsers similarly differ in how they handle browser extensions. Edge completely disables extensions, while Firefox and Safari leave them enabled by default. Chrome and Opera disable extensions by default, but let users manually enable them.

2.2 Previously Documented Misconceptions

To create the browsing scenarios for our study, we gathered misconceptions about private mode previously documented in the academic literature and news media. Two prior user studies have focused on misconceptions about private mode. Gao et al. surveyed 200 Mechanical Turk workers, examining qualitatively why participants used private browsing modes and what they believed the modes do [20]. More recently, the search engine DuckDuckGo conducted a demographically representative sample of 5,710 Americans, documenting seven misconceptions about private browsing [13].

Prior work has found that some users incorrectly believe private mode shields them from tracking by visited websites, online advertising companies, the government, and ISPs [13, 20, 24, 27, 39], and some are also under the misconception that websites cannot view IP addresses in private mode, thereby preventing geolocation [13]. Furthermore, some users believe that private mode can control what third parties save [24]. For instance, users may not consider that companies can record browsing histories when users are logged into their accounts, regardless of browsing mode [13, 16]. Users were also not aware that ad networks can track browsing across the Internet [11, 17, 25]. Finally, some users believe that private mode protects them from viruses/malware and blocks all ads [20].

While we aimed to test all misconceptions documented in prior work, some were too vague to test in a controlled manner. For instance, the misconception "websites that I visit do not know my identity" [13, 20] could refer to websites associating pseudonymous activity from different browsing sessions, or it could refer to determining a user's real-world identity. Similarly, the misconception that "private browsing keeps my computer clean" [20], could refer to any range of files being deleted upon exiting a private session.

2.3 Communicating Privacy and Security

While our study is the first to focus on privacy disclosures related to browsers' private mode, there is a large literature on user-centered communication about online privacy and security. Privacy disclosures can take many forms and be delivered through different modalities [37]. Within web browsers, numerous studies have investigated SSL warnings [2, 18, 41, 42], as well as visual icons for indicating connection security [19], ad personalization [26], site trustworthiness [35], and privacy policies [43, 46].

Despite the web's privacy and security risks [25], users often click through browsers' warnings and disclosures [2]. Recent research has designed disclosures that are harder to ignore [10] by using polymorphic warnings [4, 9, 45] or strategic timing [15]. Recent

[1] https://support.mozilla.org/en-US/kb/tracking-protection

work has focused on presenting users with personal examples [23] or automatically generated, data-rich disclosures [3, 7, 12].

3 METHODOLOGY

We conducted an online survey of participants recruited through Amazon's Mechanical Turk service for "a research study on web browsing behavior." Participants were paid $5 to complete the half-hour survey. We required that participants be 18 years or older, live in the United States, and have completed 100+ HITs with a 95%+ approval rating. Below, we present our overall survey structure followed by detailed descriptions of the thirteen conditions and twenty browsing scenarios we tested. Finally, we describe our quantitative and qualitative analysis methods.

3.1 Survey Structure

We began by asking participants to imagine a new web browser called Onyx. We chose to use a hypothetical browser to minimize biases associated with perceptions of current browser vendors or prior experiences with a particular browser [44]. We explained, "Onyx has a mode called private browsing mode. When you open a new private browsing mode window in Onyx, you see the screen below." At this point, we presented a simulated browser window containing the disclosure specified by the participant's condition (detailed in Section 3.2) and specified, "Please make sure to read the information presented below before continuing on to the rest of the survey." We clarified that we used *Standard Mode* to mean "Onyx's default mode, which is modeled after the default browsing mode of current web browsers (e.g., Chrome, Edge, Firefox, Opera, and Safari)." Similarly we defined *Private Browsing Mode* as the "mode described on the previous page" so that participants would base their answers on the disclosure text.

The main survey section presented twenty browsing scenarios (Section 3.3) in randomized order. These represented a mixture of situations in which private mode would have an effect and where it would not. We asked participants to assume an individual named Brian had opened a brand new computer and installed Onyx in its default configuration immediately prior to each scenario. We collected responses to both multiple-choice questions and a free-response question for each scenario. We provided a link to "reopen the disclosure in a new tab" on top of each page, instrumenting this link to record when participants reopened the disclosure. Finally, we asked participants demographic questions about age, gender, and technical background. We also asked about their usage of current browsers and their private modes.

3.2 Survey Conditions

Each participant was randomly assigned to one of thirteen conditions corresponding to a private browsing disclosure. All disclosures had a uniform design to prevent bias and differed only in the text displayed. Table 1 details the text of all thirteen disclosures.

We took twelve of these disclosures verbatim from the respective landing pages of six major browsers. We chose the five most popular browsers–Chrome, Edge, Firefox, Safari, and Opera– and Brave because it is a relatively new browser explicitly designed for privacy. We tested the disclosure used on the Mac OS desktop version for all browsers other than Edge (Windows 10) as of August 2017. In addition, because Chrome's disclosure had been redesigned shortly before the beginning of the study, we included Chrome's previous disclosure. We also tested the mobile versions of these browsers, excluding Edge, whose mobile version was in beta at the time of research. In cases where mobile disclosures differed between Android and iOS, we tested the one that differed most from the desktop version. Finally, to understand what actionable information disclosures provided participants, we created a control condition that made meaninglessly vague assertions about protecting privacy.

3.3 Survey Scenarios

We created twenty browsing scenarios to capture actual benefits and previously documented misconceptions of private mode [13, 20]. We tested nine where private browsing does not have any effect and six where it does, even if the protection is imperfect. We also included five scenarios where the effect of private browsing is browser- or context-dependent as perceptions of these scenarios color overall expectations of private mode. Scenarios took two main forms: distinguishing and comparative.

Sixteen *distinguishing scenarios* measured differences participants perceived between standard mode and private mode. To do this, we constructed parallel yes-or-no questions about the browser feature in each mode and asked participants to explain why they chose the same or different responses across modes. We asked about standard and private mode separately to disambiguate misconceptions specific to private mode from broader misunderstandings.

The following is an example set of questions for one scenario:

(1) Imagine that, using Onyx in **standard** mode, Brian goes online shopping on FunFashion.com and adds two items to his shopping cart. Brian then closes Onyx. Brian then opens Onyx in **standard** mode. Will his items still be available in his shopping cart?*(Yes, No)*
(2) How confident are you in your answer to the previous question? *(Very confident, Confident, Somewhat confident, Not at all confident)*
(3) Imagine that, using Onyx in **private** mode, Brian goes online shopping on FunFashion.com and adds two items to his shopping cart. Brian then closes Onyx. Brian then opens Onyx in **standard** mode. Will his items still be available in his shopping cart?*(Yes, No)*
(4) How confident are you in your answer to the previous question? *(Very confident, Confident, Somewhat confident, Not at all confident)*
(5) If you chose the same answers for standard and private mode, why? If you chose different answers, why?

In addition to the persistence of shopping cart items, we presented distinguishing scenarios related to the persistence of browsing history, site pop-up preferences, bookmarks, the list of downloaded files, downloaded files themselves, and cached photos across sessions. To gauge perceptions related to tracking by the websites visited, we presented separate distinguishing scenarios about whether Google searches across browsing sessions can be associated with the same user if the user is, or is not, logged into a Google account. We also presented separate distinguishing scenarios regarding tracking from the following three entities: an Internet Service Provider (ISP), an employer (while using the employer's

Table 1: The 13 conditions we tested, along with the browser version from which we took that disclosure's text. All disclosures were rebranded for the hypothetical Onyx browser. Text in italics was displayed in larger font as a header.

Name	Disclosure
Control	*private browsing mode.* Onyx's private browsing mode protects your privacy and keeps you safe as you browse the Internet. It was carefully designed by Onyx's engineers to let you stay incognito as you browse.
Brave (v0.19)	*this is a private tab.* Private tabs are not logged in page history. Private tabs and their cookies vanish when the browser is closed. File downloads, new bookmarks, and passwords can still be saved while using a private tab and will not be removed when the private tab is closed. Please note: Even though sites you visit in private tabs are not saved locally, they do not make you anonymous or invisible to your ISP, your employer, or to the sites you are visiting.
Brave-Mobile (Android, v1.0)	*private browsing.* Onyx won't remember any of your history or cookies, but new bookmarks will be saved.
Chrome (v60)	*you've gone incognito.* Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Onyx won't save the following information: Your browsing history, Cookies and site data, Information entered in forms. Your activity might still be visible to: Websites that you visit, Your employer or school, Your Internet service provider.
Chrome-Mobile (iOS, v60)	*incognito mode.* Your recent activity and search history aren't available when you're in incognito.
Chrome-Old (v59)	*you've gone incognito.* Pages that you view in incognito tabs won't stick around in your browser's history, cookie store or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept. However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your Internet service provider or the websites that you visit.
Edge (v40)	*browsing inprivate.* When you use InPrivate tabs, your browsing data (like cookies, history, or temporary files) isn't saved on your device after you're done. Onyx deletes temporary data from your device after all of your InPrivate tabs are closed.
Firefox (v54)	*private browsing with tracking protection.* When you browse in a Private Window, Onyx does not save: visited pages, cookies, searches, temporary files. Onyx will save your: bookmarks, downloads. Private Browsing doesn't make you anonymous on the Internet. Your employer or Internet service provider can still know what page you visit. *tracking.* Some web sites use trackers that can monitor your activity across the Internet. With Tracking Protection Onyx will block many trackers that can collect information about your browsing behaviour.
Firefox-Mobile (Android, v54)	*private browsing + tracking protection.* Onyx blocks parts of the pages that may track your browsing activity. We won't remember any history, but downloaded files and new bookmarks will still be saved to your device.
Opera (v45)	*private browsing.* As soon as you close all private windows, all the information connected with them will be erased. If you want even more privacy - turn on the VPN.
Opera-Mobile (Android, v42)	*your secrets are safe.* Onyx won't save the browsing history of your private tabs.
Safari (v10)	*private browsing enabled.* Onyx will keep your browsing history private for all tabs in this window. After you close this window, Onyx won't remember the pages you visited, your search history, or your AutoFill information.
Safari-Mobile (iOS, v10)	*private browsing mode.* Onyx won't remember the pages you visited, your search history, or your AutoFill information after you close a tab in Private Browsing Mode.

network), and government agencies. Other scenarios gauged perceptions about whether browser extensions would be active, IP addresses would be visible on the network, estimating geolocation was possible, and browsing history could be recovered by a forensics expert with physical access to the machine.

The remaining four scenarios were more naturally expressed as a comparison between standard and private modes. In these four *comparative scenarios*, we asked participants to compare the relative incidence of some property between modes. For example, participants saw the following questions and multiple-choice responses for a scenario about the loading speed of webpages:

(1) How will the speed at which webpages load compare in standard versus private browsing mode?
   - *They will load much more quickly in **private** mode than in standard mode.*
   - *They will load more quickly in **private**...*
   - *They will load a little more quickly in **private**...*
   - *They will load at the same speed.*
   - *They will load a little more quickly in **standard**...*
   - *They will load more quickly in **standard**...*
   - *They will load much more quickly in **standard**...*

(2) How confident are you in your answer...

(3) Why?

In addition to loading speed, we also presented comparative scenarios about the total number of ads, the proportion of targeted ads based on prior browsing, and virus and other malware protection.

3.4 Quantitative Analysis

We aimed to understand to what degree the disclosures or demographic factors influenced the correctness of participants' responses for all twenty scenarios in aggregate, as well as participants' overall confidence in these responses. For each participant, we computed a *correctness score* by summing the number of scenarios for which their response was correct (comparative scenarios) or response about private mode was correct (distinguishing scenarios). The correct response differed based on the browser or the browsing context for six scenarios relating to the page loading speed, the persistence of domain-specific preferences, whether browser extensions are active, information extractable by a forensics expert, shopping carts, and the total number of ads. We excluded these six and calculated the correctness score from the fourteen remaining scenarios.

We similarly created an overall *confidence score* per participant by summing that participants' self-reported confidence (0 through 3, from "not at all confident" through "very confident") across the same scenarios as the correctness score. We created linear regression models with each of the scores as the dependent variable and the following independent variables: the condition; the number of times the participant reopened the disclosure; and the participants' gender, age, technical expertise, and use of private mode.

Our second type of quantitative analysis aimed to understand, at a finer-grained level, how the disclosure participants saw impacted each individual scenario (and thus the particular private browsing feature or misconception that scenario encodes). For each of the twenty scenarios, we conducted an omnibus test to determine whether responses about what would happen in private mode differed significantly depending on which of the 13 disclosures

the participant saw. We analyzed the yes/no responses for private mode in the sixteen distinguishing scenarios using Pearson's χ^2 test. When a contingency table contained an expected value below 5, we used Fisher's exact test (FET). In the four comparative scenarios, our response variable was ordinal. Therefore, we used the nonparametric Kruskall-Wallis (KW) H test for our omnibus test across groups. We use $\alpha = .05$ throughout. We correct for multiple testing using the Benjamini-Hochberg method.

We chose 12 planned comparisons (equal to the degrees of freedom in our experiment) to investigate three targeted research questions. First, we investigated whether the widely-deployed disclosures led to significantly more correct conceptions of private mode compared to the control disclosure we created.

RQ 1: How do each of the six desktop disclosures compare to the control? To answer this, we performed the following six planned comparisons: Brave vs. Control; Chrome vs. Control; Edge vs. Control; Firefox vs. Control; Opera vs. Control; Safari vs. Control.

We further noticed that the disclosure in the desktop versions tended to differ substantially from the same browsers' mobile disclosures, which were often much shorter.

RQ 2: How do mobile versions of disclosures compare to the disclosure in the same browser's desktop version? To answer this, we performed the following five planned comparisons: Brave vs. Brave-Mobile; Chrome vs. Chrome-Mobile; Firefox vs. Firefox-Mobile; Opera vs. Opera-Mobile; Safari vs. Safari-Mobile.

Finally, because Chrome's disclosure changed noticeably shortly before we performed our study, we investigated how this redesign impacted misconceptions.

RQ 3: How does the recently redesigned Chrome disclosure compare to the previous Chrome disclosure? To answer this, we performed the following planned comparison: Chrome vs. Chrome-Old.

We only performed planned comparisons when the omnibus test was significant. For planned comparisons in the sixteen distinguishing scenarios, we again used Pearson's χ^2 test (or Fisher's exact test, as appropriate). For planned comparisons of ordinal responses in comparative scenarios, we used the Mann-Whitney U (MW) test.

3.5 Qualitative Analysis

To gauge *why* participants had particular misconceptions, we performed qualitative coding for the seventeen scenarios at least 20% of participants answered incorrectly. For each of these scenarios, a member of the research team read the free-text explanations accompanying incorrect responses. The researcher subsequently performed open coding, iteratively updating the codebook as necessary. We followed a similar process to identify themes in the reasons participants gave for using private browsing. First, a member of the research team performed open coding to identify eighteen and twenty codes for desktop and mobile users, respectively. The researcher then used axial coding for consolidation and clarification, resulting in fifteen themes for desktop and sixteen for mobile. Codes were not mutually exclusive; participants could give multiple reasons for using private browsing.

A second member of the research term independently coded all of the data following the codebook. Cohen's κ ranged from 0.651 to 0.860 per scenario, with a median of 0.716. To focus on recurring themes, we only report codes that occurred for at least 10% of incorrect responses.

4 RESULTS

We first provide an overview of our 460 participants (Section 4.1) and, for those who used private mode in their daily browsing, the reasons they gave for doing so (Section 4.2). Echoing prior work, we found that participants use private mode to hide browsing activity, prevent the saving of log-in information, and avoid cookies. Augmenting this prior work, we found that some participants used private mode to avoid ad targeting and web personalization.

The remaining sections focus on how the disclosures impacted participants' expectations for the twenty browsing scenarios. In Section 4.3, we present the results of participants' correctness scores and confidence scores aggregated across scenarios. Compared to our control disclosure, participants who saw the Chrome or Chrome-Old disclosure gave significantly more correct responses. Surprisingly, no other disclosures we tested differed significantly from the meaningless control disclosure, and our results suggest that some disclosures may have led to additional misconceptions.

To more fully understand the reason for incorrect responses, we delved into the twenty scenarios one at a time. For three scenarios, participants' responses were overwhelmingly correct (Section 4.4). Unfortunately, participants overestimated the protections afforded by private mode for eight scenarios, whereas they underestimated the protections in three scenarios (Section 4.5). These misconceptions included expectations that private browsing mode would prevent geolocation, ads, and viruses, as well as tracking by both the websites visited and the network provider. For five of the twenty scenarios, participants' responses differed significantly across disclosures. These five scenarios related to targeted advertising, the persistence of lists of downloaded files, and tracking by ISPs, employers, and governments.

4.1 Participants and Their Browser Usage

Of our 460 participants, 54.6% identified as male, 44.6% as female, and 0.8% as another gender. 70.9% of participants were between 25 and 54 years old, 8.0% were younger, and 20.8% older. Only 11.5% of participants were classified as having technical expertise due to having held degrees or jobs in computer science, IT, or related fields. Nearly all participants used Chrome for desktop browsing on a regular basis (96.7%), although many additionally used Firefox (64.3%), and to a lesser extent, Edge/Internet Explorer (21.1%) and Safari (14.3%). Chrome was also the most popular for mobile browsing (73.7%), although Safari (33.0%) was used more than Firefox (12.6%) and Edge/Internet Explorer (2.2%).

While 80.4% of participants use private browsing at least some of the time for desktop browsers, participants more frequently used standard mode. Across browsers, participants reported using private mode for 15% (median) of their browsing. In stark contrast, only 19.1% of participants used private browsing on mobile devices.

4.2 Reasons for Using Private Browsing Mode

For participants who reported using private mode in their own browsing, we asked a free-response question about why they did so. The top six reasons participants provided were to: 1) hide browsing

Table 2: Linear regression with the number of scenarios the participant answered correctly as the dependent variable. Higher numbers correspond to more correct answers.

Factor	β	SE	t	p
(Intercept)	9.53	0.40	24.0	**<.001**
Condition: Brave	0.79	0.49	1.61	.108
Condition: Brave-Mobile	0.49	0.49	0.08	.940
Condition: Chrome	1.07	0.49	2.16	**.032**
Condition: Chrome-Mobile	0.62	0.50	1.25	.211
Condition: Chrome-Old	1.09	0.50	2.20	**.028**
Condition: Edge	0.05	0.50	0.10	.923
Condition: Firefox	0.88	0.59	1.80	.073
Condition: Firefox-Mobile	-0.30	0.50	-0.60	.550
Condition: Opera	0.57	0.50	1.15	.252
Condition: Opera-Mobile	-0.34	0.49	-0.70	.484
Condition: Safari	0.78	0.51	1.53	.127
Condition: Safari-Mobile	0.95	0.49	1.93	.055
Gender: Male	0.50	0.20	2.51	**.013**
Technical: Yes	0.49	0.31	1.60	.111
Age Range	-0.65	0.52	-1.24	.216
Browsing in Private Mode (%)	-0.00	0.01	-0.26	.792
Reopened Disclosure (#)	0.19	0.16	1.19	.236

history, especially visits to adult websites; 2) prevent targeted ads and search suggestions; 3) achieve "safer" browsing; 4) prevent browsers from saving login-related information; 5) avoid cookies; 6) accommodate intentional or unintentional use by others. Our observations of points 1, 4, and 5 echo Gao et al.'s findings [20]. In addition, we observed a new reason — preventing targeted ads and search suggestions — that 15.1% of participants mentioned for desktop browsing and 15.6% mentioned for mobile.

Although all six reasons largely align with the intended characteristics of private browsing, careful reading of the third point's free text revealed a plurality of definitions of "safer" browsing. For example, P221 simply noted, "I feel a little more secure," while P448 reported, "If I'm going to a site that may be questionable, I use the private mode to protect myself." Some participants also mentioned tracking in a vague sense, such as "I like not being able to be stalked by people when I'm surfing the web" (P148). We further analyze related misconceptions in Section 4.5.

Finally, some reasons for using private mode were tied to a sense of device ownership. Overall, 27 participants considered a desktop or mobile device's shared nature in choosing to use private mode, for example, "[s]o that others in my household don't see the sites I visited" (P123). Another 47 participants considered unforeseen "users," such as thieves, finders of a lost device, or friendly borrowers.

4.3 Aggregate Correctness and Confidence

Our first goal was to understand at a high level the degree to which the disclosure the participant saw impacted their understanding of private mode. To do so, we created two indices per participant:

- **Correctness score**: How many scenarios the participants answered correctly, summed across the comparative scenarios and responses for private mode in distinguishing scenarios. This index excludes six scenarios where the correct answer depended on the browser used or browsing context, as detailed in Section 3.4. Higher values indicate a larger number of scenarios answered correctly.
- **Confidence score**: The sum of the confidence ratings (each on a 0–3 scale) participants gave for the same fourteen scenarios. Higher values indicate greater confidence.

We then created linear regression models for these two indices. For both models, we used the following six independent variables, representing the study-specific and demographic features we hypothesized might be correlated with correctness or confidence:

- Condition; categorical with control as the baseline
- Participant's gender; categorical with female as the baseline
- Whether the participant had technical expertise; categorical with "no" as the baseline
- Participant's age range; ordinal with 18-24 as the baseline
- The percent of time, averaged across browsers used, that the participant browses in private mode; continuous (0–100)
- The number of times the participant reopened the disclosure during the study; continuous (0–5, the maximum observed)

Of the thirteen disclosures we tested, twelve are currently deployed in browsers. Surprisingly, we found that most of these disclosures did not significantly impact participants' understanding of what private browsing mode does and does not do compared to our meaninglessly vague control condition. For only two of these twelve disclosures did the correctness score differ significantly from the control disclosure. As shown in Table 2, participants who saw the disclosures Google Chrome either currently uses (Chrome condition) or previously used (Chrome-Old) for desktop browsers answered more scenarios correctly than those who saw the control disclosure ($p = .032$ and $p = .028$, respectively). Of the fourteen scenarios whose answers did not depend on the browser or browsing context, participants in the control condition answered 10.4 correctly on average. In contrast, Chrome and Chrome-Old participants answered 11.1 and 11.3 questions correctly on average. Two other disclosures (Firefox and Safari-Mobile) seemed to positively impact correctness scores. While the p-values for these disclosures were not below our $\alpha = .05$ threshold, they were marginally significant ($.05 < p < .10$) and therefore may warrant further investigation.

Unfortunately, three of the mobile disclosures appeared less successful than the meaninglessly vague control at informing participants about private browsing mode. Compared to the control (10.4 average correctness score), participants who saw Brave-Mobile (10.1), Firefox-Mobile (9.9), or Opera-Mobile (9.9) had lower correctness scores on average, though these differences were not statistically significant. Among demographic factors, we found that only gender was significantly correlated with the correctness score. Participants who identified as male had higher correctness scores than those who identified as female ($p = .013$)

As shown in Table 3, which disclosure participants saw mostly did not impact their self-reported confidence in their answers. Relative to the control, only participants who saw Chrome-Old ($p = .031$) or Firefox ($p = .043$) were significantly more confident in their answers. Participants who identified as male were more confident in their answers than those who identified as female ($p < .001$), while younger participants were more confident in their answers than older participants ($p < .001$). Surprisingly, participants who spent more time browsing in private mode in their own browsing were less confident in their answers ($p = .010$), which

Table 3: Linear regression with the sum of participants' confidence ratings across scenarios as the dependent variable. Higher numbers correspond to high confidence.

Factor	β	SE	t	p
(Intercept)	26.0	1.19	22.0	**<.001**
Condition: Brave	1.72	1.46	1.18	.240
Condition: Brave-Mobile	-0.22	1.47	-0.15	.881
Condition: Chrome	1.24	1.47	0.84	.402
Condition: Chrome-Mobile	-0.31	1.48	-0.21	.836
Condition: Chrome-Old	3.20	1.48	1.2.16	**.031**
Condition: Edge	-0.48	1.50	0.32	.748
Condition: Firefox	2.98	1.47	2.03	**.043**
Condition: Firefox-Mobile	1.47	1.48	0.99	.322
Condition: Opera	0.08	1.48	0.05	.958
Condition: Opera-Mobile	0.50	1.46	0.34	.734
Condition: Safari	0.12	1.52	0.08	.938
Condition: Safari-Mobile	0.91	1.48	0.62	.538
Gender: Male	3.46	0.60	5.76	**<.001**
Technical: Yes	1.65	0.92	1.79	.074
Age Range	-5.41	1.56	-3.46	**<.001**
Browsing in Private Mode (%)	-0.05	0.02	-2.60	**.010**
Reopened Disclosure (#)	-0.16	0.48	-0.32	.746

Table 4: Non-misconceptions. The first pair of *Std.* and *Priv.* columns give the correct answer in standard and private mode, respectively. The second pair of columns give the percentage of participants who answered incorrectly.

	Answer		% Incorrect	
Scenario	Std.	Priv.	Std.	Priv.
Downloaded files remain	Yes	Yes	0.7	2.8
History saved in history menu	Yes	No	1.1	5.2
Photos cached across sessions	Yes	No	9.6	10.2

we hypothesize may have been due to experiencing events that challenged their assumptions about private mode.

4.4 Non-Misconceptions

We denoted scenarios where over 20% of participants (across disclosures) answered the question about private mode incorrectly as exhibiting misconceptions. As shown in Table 4, there were three scenarios for which nearly all participants answered the question about private mode correctly (i.e., were non-misconceptions). Overall, 97.2% of participants correctly realized that files downloaded in private mode would remain on the computer after the browsing session was closed, as in standard mode. All but 1.1% of participants knew that their browsing history was saved in the history menu in standard mode, and all but 5.2% of participants knew that it would not be saved in the history menu in private mode. Similarly, whereas all but 9.6% of participants knew that, in standard mode, photos viewed in the browser would be cached for quicker loading in future sessions, all but 10.2% of participants knew that this caching would not occur in private mode.

4.5 Misconceptions

Despite focusing participants' attention on the disclosure, we still observed misconceptions that cover the spectrum of previously documented misconceptions. We differentiate between misconceptions that overestimate and underestimate private mode.

4.5.1 Overestimating Private Mode's Protections. Participants had a number of misconceptions in which they overestimated what private mode would do. A surprising 56.3% of participants believed that even while a user was logged into a Google account, their search queries would not be saved while in private mode. The large majority of participants (144) believed this to be the case because private mode does not save search histories, conflating the browser's local history with Google's. Further, 77 participants believed that private mode would remove logged info retroactively.

Some participants (46.5%) believed bookmarks saved in private mode would not persist in later sessions. For example, 54 participants believed that private mode deletes all local, temporary data, including bookmarks. Due to a typo in the survey instrument, the data we report includes a fraction of users (around 25%, according to qualitative responses) who understood the typo to imply that we were asking about a different browser. Nonetheless, we still label this scenario a misconception because of participants who believed bookmarks would be deleted when closing private mode.

In addition, 40.2% of participants thought websites would not be able to estimate a user's location. Most (125 participants) believed location hiding was simply a feature of private browsing, but a further 21 participants specified geolocation would be impossible because IP addresses, used to estimate location, were hidden.

Nearly all participants correctly realized that their browsing could be tracked by their ISP, employer (when on their network), and the government while in standard mode. However, 22.0%, 37.0%, and 22.6% of participants mistakenly believed that ISPs, employers, and the government would be unable to track them when they used private mode.[2] Most commonly, participants simply believed that no search history would be saved, so outside entities would not have access. Other reasons included mistaken expectations that IP addresses would be hidden, cookies could no longer be used, and that private mode automatically included VPN functionality. Interestingly, 10 participants believed the government would need a warrant to access browsing activity from private mode.

Overall, 27.1% of participants believed private mode offered more protection against viruses and malware than standard, primarily attributing this to private mode not saving information, especially cookies and ads, locally. For example, P146 declared, "it's a no brainer really, when in private mode nothing is stored," while P67 added, "when you are in private mode there is no direct link to you or your computer so malware etc. would not be saved onto your computer or in your cookies." Other participants simply believed, without specifics, that private mode was more secure, "because private mode sounds and usually is more secure when visiting websites, I would think it would be much safer to visit them" (P197).

Additionally, 25.2% believed sites a user visited in private mode would be unable to see the user's IP address. Most (89 participants) believed that this was a feature of private browsing, similar to

[2] Although Opera's VPN functionality would provide some of these protections, it is not enabled by default.

Table 5: Scenarios where participants held misconceptions, shown with the correct answers and percentage of participants who gave incorrect answers. For comparative scenarios, (in)equality symbols denote the correct answer, and we give the sum of all participants answering otherwise.

Scenario	Answer		% Incorrect	
	Std.	Priv.	Std.	Priv.
Overestimating private mode's privacy protections				
Search queries associated (logged in)	Yes	Yes	1.5	56.3
Bookmarks saved across sessions	Yes	Yes	25.4	46.5
Geolocation can be estimated	Yes	Yes	5.2	40.2
Employer can track browsing	Yes	Yes	1.1	37.0
Better protected from viruses/malware	Std. = Priv.		27.1	
IP address can be collected	Yes	Yes	0.7	25.2
Government can track browsing	Yes	Yes	4.1	22.6
ISP can track browsing	Yes	Yes	3.0	22.0
Underestimating private mode's privacy protections				
Downloaded file in browser's list	Yes	No*	1.3	51.7
Proportion of targeted ads	Std. > Priv.		30.9	
Search queries associated (not logged in)	Yes	No	20.2	30.0

Except in Brave's private mode, which does retain download history

geolocation. P151 noted, "private modes...block your outgoing information, this includes IP." Some (10) confused private mode with VPNs: "Private mode usually masks the IP address by using the VPN style option that would generate a different IP address" (P72).

The disclosure significantly impacted participants' responses about tracking by ISPs, employers, and governments (FET, $p = .005$, $p < .001$, $p = .014$, respectively). Supporting RQ2, Firefox-Mobile performed significantly worse than Firefox in all three scenarios (FET, $p = .009$, $p = .020$, $p = .002$). Whereas only 5.9%, 17.1%, and 8.6% of Firefox participants mistakenly believed private mode would prevent tracking, 37.1%, 45.7%, and 42.9% of Firefox-Mobile participants had such a misconception, respectively. In Section 5, we discuss how Firefox's "tracking protection" feature appears to impact this misconception. For tracking by ISPs and employers, we similarly found a higher rate of misconceptions for Brave-Mobile compared to Brave (FET, $p = .003$ and $p = .002$). While 5.4% and 13.5% of Brave participants expected private mode to prevent tracking by ISPs and employers, 33.3% and 50.0% of Brave-Mobile participants expected the same. We also observed some evidence in support for RQ1. Whereas 13.5% of Brave participants expected private mode would prevent tracking by employers, 40.5% of control participants had this misconception (FET, $p = .018$).

4.5.2 Underestimating Private Mode's Protections. In three scenarios, however, participants underestimated private mode's protections. As shown in Table 5, over half of participants believed the names of files downloaded in private mode would appear in the list of downloaded files, when the opposite is true for all browsers except for Brave. The common explanations for this misconception were closely related: private mode does not prevent files from being downloaded (93 participants) and, if downloads are saved, the file would still be available (86 participants). This misconception seems to stem in part from participants' confusion between the browser's list of recently downloaded files and the files themselves. Nonetheless, we observed significant differences across conditions

Table 6: Distinguishing scenarios where private mode's impact depends on the browser or context.

Scenario	% Yes	
	Std.	Priv.
Items in shopping cart saved across sessions	97.8	78.8
Browser extensions active across sessions	98.3	69.1
Forensic expert can reconstruct browsing history	98.7	52.8
Site-specific preferences (e.g., for pop-ups) saved	98.3	31.3

Table 7: Distribution of responses for comparative scenarios where the impact depends on the browser or context.

Scenario	% Responses		
	Std. > Priv.	Std. = Priv.	Std. < Priv.
Amount of ads	32.2	64.9	2.9
Page loading speed	24.8	53.6	21.6

($\chi^2(12) = 38.1$, $p = .001$). In the control condition, 32.4% of participants mistakenly believed downloaded files would still be listed in the browser. A higher proportion of participants in Brave (62.2%, $\chi^2(1) = 5.4$, $p = .020$) and Firefox (77.1%, $\chi^2(1) = 12.7$, $p < .001$) held this misconception. Notably, both the Brave and Firefox disclosures mention downloaded files.

As private mode deletes cookies across sessions, one should expect to see fewer targeted ads in private mode over time. Many participants were unaware of this; 27.2% believed the proportion of advertisements that would be targeted based on a user's search history would be the same across modes. Most of these participants (70) believed ads were irrelevant to the "privacy" of private mode. They did not fully appreciate that private mode would make third-party tracking more difficult, though not impossible [17]. Expectations about targeting differed by condition (KW, $H(12) = 30.5$, $p = .009$). Surprisingly, a higher proportion of participants who saw the control disclosure were correct than those who saw Brave (MW, $U = 399$, $p < .001$), Chrome (MW, $U = 465$, $p = 0.010$), or Edge (MW, $U = 387$, $p = 0.004$). Furthermore, Brave-Mobile participants were more correct than Brave (MW, $U = 464.5$, $p = 0.019$).

In contrast to search queries when logged into a Google account, which can be associated trivially, associating search queries across sessions in private mode is more difficult, albeit not impossible [17]. While debatable, we chose to consider the 30.0% of participants who believed such searches could be associated across sessions as misconceptions based on their explanations. For example, 47 participants simply expected that Google would be able to know. In P326's words, "Google.com is the worst for snooping on every single individual in the world. Nothing escapes their tentacles."

4.6 Scenarios With Context-Dependent Impact

In the final six scenarios, the impact of private mode depends on either the browser used or the browsing context. While there is not a clear correct answer for these scenarios, we nonetheless included them to document participants' perceptions and expectations.

Browsers differ in handling browser extensions, which can associate sessions and respawn identifiers if active in private mode [48]. Extensions are always enabled in Firefox [29] and Safari [5], yet

always disabled in Edge. In both Chrome and Opera, extensions are disabled by default in private mode, but can be enabled. Similarly, site-specific preferences (e.g., pop-ups) are not saved in private mode by Chrome [21] and Edge, but are saved by Firefox and Opera.

While nearly all participants expected browser extensions to be active and site-specific preferences to persist in standard mode, expectations for private mode were mixed (Table 6). This is notable because these behaviors are subtle vectors for privacy leaks. In private mode, 69.1% of participants expected extensions to be active and 31.3% expected preferences to be saved. Although browsers differ in actual behavior, responses did not differ by disclosure.

While private modes eliminate much of the browsing data stored locally, implementations are imperfect [1, 36, 47]. Nevertheless, 47.2% of participants thought a forensics expert could not determine a user's private browsing history even with physical access.

Whereas Brave blocks ads [8] and Firefox blocks only ads that track users [32], other browsers do not block ads in private mode. Despite these actual differences, responses did not differ by condition; 32.2% of participants expected more ads in standard mode than private mode, while 64.9% expected no difference (Table 7). 100 participants believed standard mode's saving of history would facilitate ads, while 37 participants believed standard mode would have more ads because they thought there would be no cookies in private mode: "This has to do with cookies…If they can't see anything then they have no idea what ads to show" (P82).

Because private browsing mode creates a new cookie store per session, less data may be transferred in web requests, leading to faster page loads. In contrast, because less information is cached, page loads might also be slower. Among participants, 21.6% expected pages to load faster in private mode as fewer "extras" would weigh browsing down. In contrast, 24.8% expected pages to load faster in standard mode, mostly explaining that private mode would lack cached data. However, a few expected private mode to be slowed by security features. P241 wrote, "Private mode has to put the websites into more secure protocols prior to displaying them."

Finally, for cookie-based shopping carts, items placed in the cart in private mode would not remain in the cart if the site were opened in standard mode. For carts associated with a user who has logged into an account, private mode likely would not make a difference. Based on our qualitative analysis, this difference in mental models appears to explain why 21.2% of participants expected items added to a cart in private mode would persist in standard mode.

5 DISCUSSION

While prior work has documented general misconceptions about browsers' private modes [13, 20], our study is the first to examine how browsers' disclosures impact these misconceptions. We conducted a user study in which 460 participants saw one of 13 disclosures and answered questions about 20 different browsing scenarios. In most browsers, disclosures about private mode take up the full page each time a new private window is opened. The content of these disclosures differs substantially across browsers, as well as between a given browser's desktop and mobile versions. Users might also learn about private browsing from friends, online articles, or blog posts. Nonetheless, effective disclosures are vendors' most reliable channel to communicate features to users.

Of the thirteen disclosures we tested, only the current and old versions of Chrome's desktop disclosure led to significantly more correct answers than our meaninglessly vague control condition. Chrome's successes may be a result of their disclosures anticipating misconceptions that users have about private mode, and explaining the contrary: for example, that it does not hide browsing activity from employers or ISPs. Other disclosures only explain capabilities, such as deleting local history, or are longer in text length. The difference between Chrome's disclosures and others, however, amounted to only one additional scenario answered correctly. For all disclosures, participants maintained important misconceptions about private mode even though the study focused on disclosures, in many ways a best-case scenario for privacy notices.

The term "private" is heavily overloaded [40], and our results suggest the name "private mode" implies unintended meanings. When disclosures claim users can "browse privately" (Chrome), users may refer back to their broader conceptualization of privacy. For example, P300 explained that "[collecting] the IP address would defeat the purpose of privacy if the site could see that even in private mode," while P133 deduced that because tracking "would be a violation of privacy," ISPs could not collect browsing history. As such, browsers' disclosures have the herculean task of correcting misconceptions users derive from the name "private mode."

The disclosures fail at this task. We found that participants were able to answer correctly about three scenarios where private mode's effects would be apparent locally. In contrast, many over-estimations of private mode's protections reflect more opaque behaviors. In a scenario about searches being tracking while logged into a Google account, P232 wrote about how she actually tried to test her theory that private mode would prevent Google from remembering her search. When the search did not subsequently autocomplete, she validated her theory. However, Google likely still recorded that search. Even without being logged into an account, users can be tracked through browser fingerprinting, and experiments to detect how private mode actually impacts tracking over the network and by websites visited [17] are far beyond the capabilities of end-users. This is the role of privacy disclosures.

Some elements of disclosures were especially problematic. Firefox-Mobile highlights its "tracking protection" feature (for third-party tracking) without further explaining what "tracking protection" is. Notably, many Firefox-Mobile participants mistakenly believed they would be protected from network-level tracking. More generally, disclosures should avoid vague phrases implying private mode will have a broad or comprehensive impact. Poor-performing disclosures all contained such phrases. Opera-Mobile states "your secrets are safe," while Brave notes "tabs and their cookies vanish."

Disclosures appear to be getting worse, not better. Firefox Focus recently introduced a disclosure that ill-advisedly encourages users to "browse like no one's watching." The poor performance of disclosures in our study suggests future work consider personal examples [23], different modalities [37], and even changing the name of the mode to better convey private mode's actual protections.

6 ACKNOWLEDGMENTS

We gratefully acknowledge support from a Mozilla Research Award and assistance from Adam Freymiller.

REFERENCES

[1] Gaurav Aggarwal, Elie Bursztein, Collin Jackson, and Dan Boneh. 2010. An analysis of private browsing modes in modern browsers. In *Proc. USENIX Security Symposium*.

[2] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A large-scale field study of browser security warning effectiveness. In *Proc. USENIX Security Symposium*.

[3] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proc. CHI*.

[4] Bonnie Brinton Anderson, Anthony Vance, Jeffrey L Jenkins, C Brock Kirwan, and Daniel Bjornn. 2017. It all blurs together: How the effects of habituation generalize across system notifications and security warnings. In *Information Systems and Neuroscience*.

[5] Apple. 2017. Safari for Mac: Use private browsing windows in Safari. (March 30, 2017). https://support.apple.com/kb/ph21413?locale=en_GB.

[6] Apple Safari. Accessed July 7, 2017. Private browsing mode (landing page). (Accessed July 7, 2017).

[7] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little brothers watching you": Raising awareness of data leaks on smartphones. In *Proc. SOUPS*.

[8] Brave. Accessed 2017. Brave browser. (Accessed 2017). https://brave.com/.

[9] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. 2014. Harder to ignore: Revisiting pop-up fatigue and approaches to prevent it. In *Proc. SOUPS*.

[10] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proc. SOUPS*.

[11] Aaron Brown. 2015. Watching porn on your internet browser's private mode isn't very private at all. *Express*. (November 20, 2015). http://www.express.co.uk/life-style/science-technology/620887/Porn-Online-Private-Incognito-Browser-Mode.

[12] Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur. 2016. A large-scale evaluation of U.S. financial institutions' standardized privacy notices. *ACM Trans. Web* 10, 3 (2016), 17:1–17:33.

[13] DuckDuckGo. January 2017. A study on private browsing: Consumer usage, knowledge, and thoughts. (January 2017). https://duckduckgo.com/download/Private_Browsing.pdf.

[14] EFF. Accessed 2017. Panopticlick: Is it possible to defend against browser fingerprinting? https://panopticlick.eff.org/self-defense. (Accessed 2017).

[15] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. 2009. Timing is everything?: The effects of timing and placement of online privacy indicators. In *Proc. CHI*.

[16] Alicia Eler. 2012. 5 ways to keep Your Google browsing private. *ReadWrite*. (April 3, 2012). https://readwrite.com/2012/04/03/5_ways_to_keep_your_google_browsing_private/.

[17] Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proc. ACM CCS*.

[18] Adrienne Porter Felt, Alex Ainslie, Robert W Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL warnings: Comprehension and adherence. In *Proc. CHI*.

[19] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking connection security indicators. In *Proc. SOUPS*.

[20] Xianyi Gao, Yulong Yang, Huiqing Fu, Janne Lindqvist, and Yang Wang. 2014. Private browsing: An inquiry on usability and privacy protection. In *Proc. WPES*.

[21] Google Chrome. 2017. Google Chrome privacy notice. (April 25, 2017). https://www.google.com/chrome/browser/privacy/.

[22] Google Chrome. Accessed July 7, 2017. Incognito mode (landing page). (Accessed July 7, 2017).

[23] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *Proc. CHI*.

[24] Chris Hoffman. 2012. How private browsing works, and why it doesn't offer complete privacy. How-To Geek. (June 30, 2012). https://www.howtogeek.com/117776/htg-explains-how-private-browsing-works-and-why-it-doesnt-offer-complete-privacy/.

[25] Balachander Krishnamurthy and Craig Wills. 2009. Privacy diffusion on the web: A longitudinal perspective. In *Proc. WWW*.

[26] Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. What do online behavioral advertising privacy disclosures communicate to users?. In *Proc. WPES*.

[27] David Meyer. 2016. Opera makes major push for private browsing. *Fortune*. (September 19, 2016). http://fortune.com/2016/09/20/opera-vpn-privacy/.

[28] Microsoft Edge. Accessed July 7, 2017. In-Private mode (landing page). (Accessed July 7, 2017).

[29] Mozilla. Accessed 2017. Add-ons: private-browsing. MDN web docs. (Accessed 2017). https://developer.mozilla.org/en-US/Add-ons/SDK/High-Level_APIs/private-browsing.

[30] Mozilla. Accessed July 7, 2017. Private browsing - Use Firefox without saving history. (Accessed July 7, 2017). https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history.

[31] Mozilla Firefox. Accessed July 7, 2017. Private browsing mode (landing page). (Accessed July 7, 2017).

[32] Nick Nguyen. 2015. The Mozilla Blog: Firefox now offers a more private browsing experience. (November 3, 2015). https://blog.mozilla.org/blog/2015/11/03/firefox-now-offers-a-more-private-browsing-experience/.

[33] Opera. [n. d.]. Free VPN in Opera browser. Surf the web with enhanced privacy. ([n. d.]). http://www.opera.com/computer/features/free-vpn.

[34] Opera. Accessed July 7, 2017. Private browsing. (Accessed July 7, 2017). http://help.opera.com/Mac/12.10/en/private.html.

[35] Yohko Orito, Kiyoshi Murata, and Yasunori Fukuta. 2013. Do online privacy policies and seals affect corporate trustworthiness and reputation. *International Review of Information Ethics* 19, 7 (2013), 52–65.

[36] Kiavash Satvat, Matthew Forshaw, Feng Hao, and Ehsan Toreini. 2013. *On the privacy of private browsing: A forensic approach.* Computing Science, Newcastle University.

[37] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Proc. SOUPS*.

[38] Chris Smith. 2014. Even Eric Schmidt has no idea how privacy works on one of GoogleâĂŹs top products. (December 17, 2014). http://bgr.com/2014/12/17/eric-schmidt-on-google-chrome-incognito-mode/.

[39] Christopher Soghoian. 2011. Why private browsing modes do not deliver real privacy. *Center for Applied Cyber security Research, Bloomington* (2011).

[40] Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. L. Rev.* 154 (2005), 477.

[41] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 2012. On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings. In *Proc. SOUPS*.

[42] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying wolf: An empirical study of SSL warning effectiveness. In *Proc. USENIX Security Symposium*.

[43] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22, 2 (2011), 254–268.

[44] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2011. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proc. SOUPS*.

[45] Anthony Vance, Brock Kirwan, Daniel Bjorn, Jeffrey Jenkins, and Bonnie Brinton Anderson. 2017. What do we really know about how habituation to warnings occurs over time?: A longitudinal fMRI study of habituation and polymorphic warnings. In *Proc. CHI*.

[46] Shomir Wilson, Florian Schaub, Rohan Ramanath, Norman Sadeh, Fei Liu, Noah A. Smith, and Frederick Liu. 2016. Crowdsourcing annotations for websites' privacy policies: Can it really work?. In *Proc. WWW*.

[47] Meng Xu, Yeongjin Jang, Xinyu Xing, Taesoo Kim, and Wenke Lee. 2015. Ucognito: Private browsing without tears. In *Proc. CCS*.

[48] Bin Zhao and Peng Liu. 2015. Private browsing mode not really that private: Dealing with privacy breach caused by browser extensions. In *Proc. DSN*.