Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing

Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman,
Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{htq, jcolnago, vidyag, spearman, thomasjm, acquisti, nicolasc,
lorrie}@andrew.cmu.edu

ABSTRACT

Previous research has suggested that people use the private browsing mode of their web browsers to conduct privacy-sensitive activities online, but have misconceptions about how it works and are likely to overestimate the protections it provides. To better understand how private browsing is used and whether users are at risk, we analyzed browsing data collected from over 450 participants of the Security Behavior Observatory (SBO), a panel of users consenting to researchers observing their daily computing behavior "in the wild" through software monitoring. We explored discrepancies between observed and self-reported private behaviors through a follow-up survey, distributed to both Mechanical Turk and SBO participants. The survey also allowed us to investigate why private browsing is used for certain activities. Our findings reveal that people use private browsing for practical and security reasons, beyond the expected privacy reasons. Additionally, the primary use cases for private browsing were consistent across the reported and empirical data, though there were discrepancies in how frequently private browsing is used for online activities. We conclude that private browsing does mitigate our participants' concerns about their browsing activities being revealed to other users of their computer, but participants overestimate the protection from online tracking and targeted advertising.

1. INTRODUCTION

Private browsing mode is a feature offered by most major web browsers. These modes promise users an increased level of privacy for their browsing activities. Typically, browsers clear data associated with a user's activities once they close a private browsing window. Though private browsing is an important tool for users, prior work has found that it does not address some major user privacy concerns, nor does it offer privacy protections that many users expect [10, 16, 41, 42]. Furthermore, though users may have privacy concerns regarding their online activities, they frequently fail to navigate privacy decisions to meaningfully address them [1].

Prior user studies have examined different aspects of private browsing, including contexts for using private browsing [4, 10, 16, 28, 41], general misconceptions of how private browsing technically functions and the protections it offers [10,16], and usability issues with private browsing interfaces [41, 44]. A major limitation of much prior work is that it is based on self-reported survey data, which may not always be reliable. In answering surveys, participants may not remember all past activities, may be too embarrassed to report some of their private browsing behavior, or may misinterpret survey questions [23]. Moreover, it is unclear whether users' misconceptions reported in prior work are relevant to users' motivations for engaging private browsing mode, and thus, lead to privacy harms.

Our study builds on prior work to provide a better understanding of how people use private browsing, and identify the gaps that exist between users' perceptions of the privacy protections afforded by private browsing and the reasons they use it. To do so, we analyzed browsing data contributed by 451 participants over a three-year period to the Security Behavior Observatory (SBO), a longitudinal panel study actively collecting data related to privacy and security behaviors from participants' home Windows computers [7, 13, 14, 36]. We supplement this analysis with a survey which explored reasons for using private browsing, and common misconceptions about its actual protections. Our survey was distributed to both SBO and Amazon Mechanical Turk[1] participants so that we could compare our findings with the misconceptions explored in prior work [16], and determine whether our findings hold across two demographically different populations.

Our work contributes the following: 1) We leverage SBO browsing data to explore patterns in private browsing usage, such as how browsing activity differs between normal and private browsing modes. 2) We examine to what degree private browsing activities observed by the SBO differ from those reported in our survey, in order to investigate the impact of self-reporting bias on prior work. 3) We provide insights into why people use private browsing for specific use cases, and explore to what extent misconceptions about private browsing may be harming private browsing users.

Overall, private browsing occurred in only 4% of the 167,128 browsing sessions observed in the SBO, indicating that users likely only switch to private browsing to complete a specific

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

[1] Amazon Mechanical Turk: https://www.mturk.com/

task. The most common use cases for private browsing include using a service which required a login and performing a search engine query. We observed that websites categorized as adult content constituted a larger percentage of domains visited in private browsing than in normal browsing. Proportionally, participants also conducted searches about sensitive topics and watched age-restricted YouTube videos more frequently in private browsing mode than in normal browsing. We found discrepancies between the private browsing usage reported by SBO participants and that empirically observed, though overall, the most common activities observed were similar to those reported.

Similar to Gao et al., our survey found that although participants had misconceptions about the technical mechanisms behind private browsing, they did find utility in this tool. The most commonly reported use of private browsing was to prevent browsing or search activities from being stored to their device, and potentially being seen by other users. However, we found that some participants overestimated the protections offered by private browsing for the specific use cases they reported, which could lead them to use private browsing in potentially harmful ways. For example, some participants reported that their credit cards were better protected in private browsing mode during online shopping and that their social media activities were hidden from their employers when browsing at work. Identifying such misconceptions is necessary to educate users about the actual protections offered by private browsing, and help them navigate the privacy decisions they make online. We conclude with a discussion about the implications of our findings for browser design and usability.

2. BACKGROUND & RELATED WORK

In this section we present relevant literature and background information related to our study. We focus on prior literature examining privacy concerns of internet users, as well as that studying typical use cases for private browsing. Additionally, we provide a description of private browsing functionalities available in major web browsers currently offered on the market to better highlight user misconceptions observed in our study.

2.1 Privacy Sensitive Online Activities

Prior work has explored users' privacy concerns when they use the internet. Angulo studied users' concerns in "online privacy panic situations" such as account hijacking, leaking of data online, and identity theft. He found that financial harm, embarrassment, and reputation loss were users' primary concerns [5]. A 2013 Pew Research Center survey of 1,002 U.S. adults about online privacy and security concerns and behaviors found that 50% of participants reported being concerned about the amount of personal information collected about them online, and 59% did not believe it is possible to be anonymous on the internet. Most commonly, survey participants expressed a desire to hide their activities from hackers and advertisers, and more participants reported taking steps to avoid advertisers and uncomfortable social situations than to avoid employers or the government from knowing their activities [39].

Prior work has also found that users are willing to take measures to protect their privacy. In the same 2013 Pew survey, 86% of participants had taken steps to remove or hide their online activities, including clearing cookies or browser history and disabling cookies in their browser [39]. An interview study conducted by Kang et al. found that 77% of their non-technical participants reported taking some action to hide or delete their "digital footprints," including using private browsing mode [21].

Other research has highlighted that certain online activities, such as visiting adult content, performing search engine queries, and receiving targeted advertising, may be particularly sensitive. The Pew Research Center found that only 13–15% of their participants reported that they visited adult websites or shared adult content online [15]. Another Pew Research Center survey found that 73% of participants viewed the storing of searches by search engine providers, such as Google, as an invasion of privacy, and 68% opposed receiving targeted advertising [37]. Similarly, a study conducted by Panjwani and Shrivastava analyzing whether users are willing to trade off search personalization for privacy found that 84% of their participants considered at least one of their observed Google searches as sensitive and preferred personalized results for fewer than 20% of these types of searches [35]. In a vignette survey, Rader found that advertisements were a concern related to search engine queries, but participants viewed advertisements in Facebook as even more concerning [38]. However, the findings from an interview study conducted by Agarwal et al. suggest that though users are concerned about tracking on some types of websites, they generally may be more concerned with embarrassment stemming from particular types of advertisements, such as those promoting sexually explicit content, dating sites, or lingerie. The authors also observed that videos viewed by the participants were also often reported as sensitive [3].

Altogether, this prior work highlights reasons why users may choose to use private browsing mode when performing certain activities online. In our study we aim to explore these reasons in more detail to identify whether there are common misconceptions among online users about the protections provided by private browsing. Though users have concerns regarding their online privacy and try to take steps to protect it, they may often make mistakes in doing so [2].

2.2 Private Browsing Functionalities

Each major web browser has a private browsing mode. However, different browsers refer to it using different terms. Google Chrome call private browsing "Incognito Mode" [17], Internet Explorer and Microsoft Edge refer to it as "InPrivate Browsing" [25,26], and Firefox, Opera, and Safari each refer to it as "Private Browsing" [6,29,34]. Generally, when users browse in private browsing mode, their browsing history, logins, form data, and cookies are not stored in their browser. Additionally, in some browsers, the files a user downloads during a private browsing session do not appear in their downloads list [6]. Table 1 summarizes the private browsing functionalities of each browser.

Primarily, private browsing prevents a user's browsing and search activities from being seen by other users of the device. It also provides some protection against online tracking and targeted advertising. Private browsing windows do not replay the cookies and other trackers previously placed by websites in normal browsing mode. Additionally, any

Browser	Browsing History Not Stored	Cookies Not Stored*	Login Info Not Stored	Form Data Not Stored	Tracking Protection Enabled	Downloaded Files Hidden
Safari 11.0.3	✓	✓	✓	✓	Do Not Track	✓
Internet Explorer 11	✓	✓	✓	✓	Do Not Track	✓
Firefox 58.0.2	✓	✓	✓	✓	Disconnect	✗
Edge 41.16299.15	✓	✓	✓	✓	✗	✓
Chrome 63.0.3239	✓	✓	✓	✓	✗	✗
Opera 51	✓	✓	✓	✓	✗	✗

Table 1: Summary of private browsing functions of six major web browsers. Safari, Internet Explorer, and Edge are the only browsers in which downloaded files do not appear in the user's downloads list during private browsing. *Cookies are still exchanged in private browsing, but are not stored beyond the session.

new cookies that were set during the browsing session are deleted once the user closes the window. Firefox and Safari also enable additional web tracking protection mechanisms. In Firefox, some web trackers identified by Disconnect[2] are automatically blocked when users enable private browsing mode [30], while Safari enables Do Not Track, a signal that requests websites not to track users [6]. However, private browsing does not prevent websites from seeing a user's IP address, nor does it hide a user's activities from their Internet Service Provider (ISP).

Prior work in the field of computer forensics has found that artifacts that can identify a user's browsing activities do still remain on the user's computer, even if they use private browsing mode [27, 40]. For example, Ohana and Shashidhar were able to recover usernames, cached images, and URL history from RAM for activities conducted in Internet Explorer's InPrivate mode [33]. A study by Aggarwal et al. highlighted that browser extensions could be particularly privacy violating if enabled in private browsing mode [4]. Soghoian argues that private browsing mode does not offer the level of privacy users expect, and may provide users a false confidence that their activities are truly private [42]. In our work, we aim to further explore whether or not users do have misconceptions about private browsing, particularly concerning the most common activities for which private browsing is used.

2.3 Private Browsing Usage

Prior work has explored how people use private browsing and the misconceptions users have about how it works. A recent survey of 5,710 U.S. participants about private browsing conducted by DuckDuckGo,[3] a privacy-protective search engine, found that 46% of participants had used private browsing at least once on their computer and 43% had used it on a mobile device. The survey also revealed that two-thirds of participants overestimated the privacy protections offered by private browsing, the most common misconceptions being that private browsing prevents tracking from websites and online advertisers, and that it hides searches from search engines [10]. This particular survey population may have been more privacy sensitive than the average online user. However, Gao et al. found similar misconceptions regarding online tracking in a survey study, and reported that many participants did not understand the technical mechanisms behind private browsing. Perceived benefits of private browsing mentioned by participants included that it protects against data collection from malicious sites, reduces page load times, and prevents viruses from being downloaded [16].

An interview study conducted by Shirazi and Volkamer highlighted several usability issues participants noted related to private browsing, including determining whether or not private mode was active in Firefox and Chrome, confusion with browser-provided descriptions of private browsing, and perceptions that it was hard to use or that websites would not be fully functional [41]. Similarly, Wu et al. found in an online study that nearly every disclosure of private browsing provided by major browsers failed to dispel common misconceptions about private browsing mode [44].

Common use cases for private browsing reported in these prior studies include performing "embarrassing" searches, visiting pornographic and dating sites, preventing targeted ads, avoiding cookies, accessing social media, browsing on unprotected Wi-Fi networks, and buying presents [4, 10, 16, 41, 44]. A report from Mozilla's Test Pilot study analyzed timing patterns related to private browsing usage and found that there are spikes in usage at lunch time, the end of the work hours, and after midnight. The report also revealed that most private browsing sessions have a duration of about 10 minutes [28].

Our work builds on these prior studies of private browsing. In our survey, we examine more nuanced use cases for private browsing determined from an analysis of actual user data collected through the Security Behavior Observatory. We also seek a deeper understanding of the threats users are seeking protection from specific to particular use cases. Furthermore, we aim to study users' understandings of the technical mechanisms behind private browsing and identify misconceptions that lead users to believe private browsing is protecting them in ways that it is not.

3. METHODOLOGY

In this section we describe our data collection and analysis methodology. Our study incorporates both empirical and survey data, collected from a longitudinal study, as well as Amazon's Mechanical Turk.

3.1 The Security Behavior Observatory

For our analyses of private browsing behaviors, we used browsing data collected from the Security Behavior Observatory (SBO), further described in Section 3.1.1. We provide additional details about the analyses we conducted for this study in Section 3.1.2.

[2] Disconnect: https://disconnect.me/

[3] DuckDuckGo: https://duckduckgo.com/

3.1.1 Data Collection

The Security Behavior Observatory (SBO) is a longitudinal panel capturing the usage and security behaviors of Windows computer users [7, 13, 14, 36]. The study has been continuously recruiting new participants and collecting data since late 2014 and, as of December 2017, has collected data from over 530 machines.

SBO participants' own home computers are instrumented with data collection software that is designed to collect data automatically with minimal effects on users' normal activities. The SBO data collection software includes system-level components, which allow collection of metadata related to system events, installed software, and other system events and user activities. The software suite also includes browser extensions for Google Chrome, Mozilla Firefox, and Internet Explorer that collect browsing history metadata including URLs and titles of pages visited by the user.

The study's protocol is approved by the Institutional Review Board (IRB) at all universities that work with data from the panel. Each participant completes an enrollment phone call with a member of the research team during which they are assisted with reviewing the study description and terms. During that phone call, participants sign a consent form that explicitly states that all browsing activity and network traffic may be subject to monitoring and that the full contents of web pages may be collected, with the exception of a few highly-sensitive data types.

After the participant has asked any questions they may have and has completed the consent form, a researcher assists each participant with installing the SBO system software, as well as the browser extensions for Google Chrome, Mozilla Firefox, and/or Internet Explorer. The researcher and the participant are connected via both phone and remote session during this entire process so that the researcher can explain each installation step and so that the participant may ask any additional questions that arise. In the case of Google Chrome, an explicit opt-in is required in order for the extension to be able to run and collect data in Incognito mode, so participants either observe the researcher enabling it (and have the opportunity to decline this or ask the researcher for more information) or undergo the step of enabling this functionality themselves.

Participants received $30 for enrolling, as well as $10 per month for continued participation, and are free to leave the study at any time. Given the breadth of the SBO's data collection, special considerations are made for the security and privacy of its participants. After collection, SBO data is encrypted in transmission and stored on hardened servers accessible only to research team members and maintenance personnel using a VPN and two-factor authentication.

We utilized data collected by the SBO's Chrome and Firefox extensions. These extensions collect data related to users' browsing histories, including page URLs, page titles, timestamps, and flags indicating the use of private browsing modes. They also collect a variety of metadata regarding browser configuration and preferences, including information about browser settings and extensions present in the browser. We excluded sessions comprised solely of activity from other browsers from our analysis, as only the Chrome and Firefox extensions report a private browsing flag.

3.1.2 Data Analysis

In this section we describe the analyses we conducted using browsing data collected through the SBO. The data was collected between October 15, 2014 and December 19, 2017 and was contributed by 451 distinct SBO participants. While the SBO has collected data from more participants, for our analysis we excluded participants who had technical issues in reporting browsing data. We also did not include those who solely used a browser other than Chrome or Firefox, as the SBO currently only collects private browsing activity from these two browsers. As the browsing data is stored in a MySQL database, much of our analysis was conducted using MySQL queries. To analyze browsing activity at a session level, or period of continuous browsing activity, the data used in our analyses were labeled with a session identifier. We identified browsing sessions as periods of browsing activity such that there was a gap of at least 30 minutes before the session started and ended. Wang et al. used a similar time-based definition to distinguish browsing sessions, with a threshold of 20 minutes [43].

To analyze the contexts in which private browsing was being used, we manually annotated all sessions containing private browsing data with the use cases listed in Table 3. These use cases were determined by annotating a subset of the private browsing data and finding commonly occurring activities. Definitions of what comprised sensitive browsing and sensitive searches were based off of the responses from Mechanical Turk participants to the survey question "What do you consider to be a sensitive search?" which were analyzed prior to manually coding the entire set of private browsing data. In their responses, participants most frequently mentioned the following categories: 1) pornography or adult content, 2) health or medical content, 3) financial activities, 4) terrorism or crime content, 5) illegal activity, 6) political content.

To ensure accuracy and consistency in coding, two researchers independently coded 25% of the private browsing data, achieving an agreement of $\kappa = 0.81$. All conflicting sessions were reviewed and resolved. The remaining data were coded by a single researcher. After coding the private browsing data, we identified the dominant use case for private browsing for each participant who used it. We determined this to be the use case that the participant did most frequently in private browsing and in at least half of their browsing sessions containing private browsing activity.

We also ran several analyses to compare activities in private browsing with those in normal browsing. The four primary attributes we analyzed were the set of domains visited, categories of the websites visited, search engine queries conducted, and types of YouTube videos viewed. We chose to focus on search engine queries and YouTube activity because conducting searches and streaming video or audio are among the most common use cases for private browsing, in both the observed SBO data and survey responses.

To make statistical comparisons between the two browsing modes, we used Pearson's chi-square tests, with $\alpha = 0.05$. We also report the effect size using the phi coefficient (ϕ), if the comparison was between two binary variables, or Cramer's V (V), if the variables compared had more than two levels, for the significant associations we observed. Both measures are reported on a scale from -1 to 1, where -1 indicates complete negative association and 1 indicates complete positive association. Only results with at least a small effect (where the association is at least 0.1) are reported, which is an accepted threshold for reporting statistical results [8].

Domains Visited

In comparing the set of domains visited, we calculated the Jaccard similarity coefficient of the distinct domains (e.g., mail.google.com) visited in private browsing with those visited in normal browsing. Subdomains (e.g., chat.google.com and mail.google.com) were counted as distinct domains. Two sets are completely dissimilar (they have no members in common) if they have a coefficient of 0, and are completely similar (they have all members in common) if they have a coefficient of 1 [18].

Domain Categories

To compare the categories of visited websites, we used Amazon's Web Information Service (AWIS)[4] to classify the domains visited. We reduced the number of AWIS provided categories to those that directly mapped to the common use cases for private browsing identified in the manual analysis. These categories are listed in Appendix A. We chose not to use AWIS categories to identify specific use cases of private browsing as some common use cases, such as bypassing a paywall on a news website, can only be determined by looking at the browsing activity in context.

Search Engine Queries

We also used our manual analysis of private browsing activities to identify keywords that corresponded to search engine queries that people may consider sensitive, based on the definition determined from our Mechanical Turk survey responses. The lists of keywords are provided in Appendix B. We developed a script to compare the presence of these keywords in the queries made in both browsing modes. The results of the script were manually reviewed for searches that would not be considered sensitive, and to ensure searches were correctly categorized. Queries to Google, Bing, or Yahoo were identified using the domain and query parameters in the URL of the browsing activity.

YouTube Activity

To compare the types of videos visited in private browsing with those in normal browsing, we developed a script utilizing the PhantomJS WebKit[5] to parse the HTML of pages containing YouTube videos visited by SBO participants. For each video, we analyzed the element with the "unavailable-message" id, which we determined to be a sort of status indicator for the video. This element provided information about whether the video was blocked in restricted mode (indicating some sort of adult or sensitive content), removed for copyright reasons, or removed for violation of YouTube's site policy on sexual, violent, or deceptive content. A list of these codes are provided in Appendix C. Due to the computing resources required for running the script, we analyzed all unique 2,190 videos viewed in private browsing and 3,158 unique videos viewed in normal browsing (a random sample of 5% of all unique videos viewed in normal browsing).

3.2 Survey

We conducted a survey to better understand why people use private browsing for certain browsing activities and whether users understand how it works. We administered our survey through both the SBO and Mechanical Turk to collect data from a larger population, and to evaluate the generalizability of our findings by comparing the two populations.

3.2.1 Data Collection

The survey developed for this study contained a combination of open-ended response and multiple choice questions. In the survey, participants answered questions about their background and device configurations, such as devices and browsers they typically use, use of private browsing mode, if they shared their computer with others, demographics, their current cookie policy, any privacy-related browser extensions installed, and privacy consciousness (determined from the IUIPC scale for control, awareness, and collection [24].

Additionally, participants answered two open-ended questions asking what they expected to be protected from while using private browsing, and how they thought it functions. To investigate understanding of private browsing more deeply, the survey also presented 14 statements about technical details related to private browsing and participants selected one of the following options for each statement: "definitely correct," "probably correct," "probably incorrect," "definitely incorrect," or "I don't know." While some questions used more general terms, such as "anonymous," others included more specific wording (like "IP address") so that we could explore the consistency of potential misconceptions.

Participants who indicated ever having used private browsing on their browser were asked how frequently they had performed a list of 13 activities in private browsing mode, based on observed use cases from the SBO, during the past month. We chose to ask about activities in the past month to capture a more accurate representation of regular usage of private browsing, instead of activities that participants may have done only once or twice, a long time ago. Participants were asked a follow up open-ended question asking why they chose to use private browsing for each activity they indicated having done at least once in the past month. The list of all survey questions is included in Appendix D.

We first piloted the survey with 10 local participants who provided detailed feedback, and then conducted two rounds of pilot surveys on Mechanical Turk, with 20 participants each. After each round of piloting we improved the clarity of survey questions and developed additional questions. With approval from our IRB, we advertised this survey on Mechanical Turk as a survey about browsing habits, so as to potentially recruit participants who did not use private browsing. Mechanical Turk users who had a HIT approval rate of over 90% and were residents of the United States, over the age of 18, and not active military were eligible to take the survey. The survey was completed by 309 participants on Mechanical Turk who were compensated with $2.50.

Active SBO participants with Chrome or Firefox browsing data sent by a current version of the SBO browser extension were also invited to participate in the survey. This survey was optional for all SBO participants and did not affect their participation in the longitudinal panel. The survey contained the same questions that were distributed to

[4] AWIS: https://aws.amazon.com/awis/

[5] PhantomJS: http://phantomjs.org/

the Mechanical Turk sample. In keeping with the approved IRB protocol for optional surveys distributed to this panel, SBO participants received $7.50 for completing the survey. Survey invitations were sent to 344 participants, and 227 participants completed the survey.

3.2.2 Data Analysis

Prior to running our statistical analyses of the survey data, we reviewed for indicators of repeat Mechanical Turk respondents. We removed four responses submitted from IP addresses from which we had previously received survey responses.[6] Thus, we included 305 Mechanical Turk responses in our analyses. We did not have similar concerns about SBO participants completing the survey multiple times, because the SBO infrastructure prevents duplicate responses.

For statistical testing we used $\alpha = 0.05$. In comparisons in which both the independent and dependent variables were categorical, we ran Pearson's chi-squared tests, or Fisher's exact tests if any counts in the contingency table were below five. As in our categorical comparisons of SBO data, we also report the effect size of the association using the phi coefficient or Cramer's V. When testing whether a certain population used private browsing for a particular use case, responses to the question asking participants how frequently did they used private browsing for that use case in the past month were binned as a binary variable where the levels were "never" and "at least once." Responses to this question were confirmed with the participant's answer to the follow up question asking why they used private browsing for that use case. Participants who wrote that they did not use private browsing for that activity, or simply filled in "N/A" were excluded from the count of participants who used private browsing for that use case.

We used a binary logistic regression to test if demographics and privacy sensitivity influenced whether a participant had used private browsing. The independent variables for one regression were the categorical variables age, gender, education, and technical expertise. In another model, we tested for correlations with the IUIPC control, awareness, collection factors. The dependent variable of both regressions was whether or not the participant had used private browsing.

In measuring participants' understanding of private browsing, we used their responses to the 14 statements about the technical details of private browsing. Each participant was assigned a score based on the number of questions they answered correctly, with the "probably" and "definitely" options grouped together. To compare the average score of distinct populations, we ran two-sided t-tests or ANOVA tests, depending on the number of levels in the independent variable. We also used a linear regression to test the impact of demographics on participants' level of understanding, using the same independent variables as the logistic regression.

To analyze our qualitative data, we developed three separate codebooks; the first for the question about expected protections, the second for the question asking how private browsing works, and the third for responses to why private browsing was used for a specific use case. Codebooks were iteratively developed by reviewing a subset of responses to their respective questions for common themes. All responses were coded by two researchers independently, who then reviewed and resolved all conflicts. Our reporting of qualitative data is based on the resolved set of codes.

3.3 Limitations

While our study provides valuable insights into people's usage of private browsing, there are some limitations of our findings. The manual coding of private browsing data could have introduced some errors in our reporting, since there is a large degree of subjectivity in what is considered privacy sensitive. As what constitutes a sensitive activity varies from subject to subject, we cannot be certain that activities coded as sensitive were actually considered sensitive by the participant. Similarly, there may have been activities that participants considered sensitive that were not marked as such during the coding process. This limitation also impacted our analysis of search engine queries conducted in both browsing modes. We attempted to limit this subjectivity by identifying specific categories that survey participants indicated they considered sensitive.

Another limitation of the SBO is that it collects data only from Windows users. Additionally, our study analyzed browsing activities only conducted in Google Chrome and Mozilla Firefox. It is possible that the browsing habits of MacOS users, and users of other browsers, differ from the activities we observed in this population. However, we believe our findings still offer valuable insights into how people use private browsing in their daily lives.

Some of our findings are also impacted by the same limitations as prior work using self-reported methods. As discussed, some of these limitations include the misreporting of prior activities and misinterpretation of survey questions. We attempted to mitigate these potential issues by conducting multiple rounds of piloting and iterating our survey based on the feedback received after each round.

Our study also utilizes two convenience samples, neither of which are representative of the general population. However, Mechanical Turk has proven to be a valid source of high-quality human subjects data [22], and has been used successfully in prior privacy research (e.g., [12,32]). Considering the consistency of reported behaviors across our two, demographically-different samples, we believe our study provides value in understanding how this important privacy enhancing technology is being used.

4. RESULTS

In this section we report findings from browsing activities observed in the SBO and our survey data. Participants were consistent in their usage of private browsing, and generally used it for practical reasons, such as logging into an account without leaving credentials on the computer, as well as for privacy-sensitive activities. Though there were some inconsistencies between observed and reported private browsing behaviors, overall the most common activities matched across the two data sources. We observed that participants were primarily concerned with their activities being revealed to other users of their device, but also desired protection from web tracking and targeted advertising.

[6] Though it is possible that multiple people connected to the same network may have completed the survey, and thus had the same IP address, we thought it was more likely that the participants took our survey more than once under different Mechanical Turk accounts. In these cases, we analyzed only the first response submitted.

4.1 Demographics

Demographics, displayed in Table 2, were significantly different between our two participant groups. The SBO population had a wider age distribution, with 10% of participants reporting to be age 65 or older. Additionally, the SBO group was significantly more educated, and a larger percentage were technical which was defined by ever holding a job or receiving a degree in computer science or any related technology field. The SBO also contained a larger proportion of females (all $p < 0.05$). Mechanical Turk participants were found to be somewhat privacy conscious, based on the IUIPC metrics for control, awareness, and collection factors, while those in the SBO were less privacy conscious.

We did observe some demographic differences in whether or not a participant had used private browsing within both participant groups. Male Mechanical Turk participants were more likely to use private browsing than females ($p = 0.01, \phi = 0.2$); 95% of males reported using private browsing but only 86% of females did. From the SBO survey, those age 45 and older reported using private browsing less than younger participants ($p < 0.001, \phi = 0.5$); 84% of those under 45 had used private browsing compared to only 39% of those older than age 45. Additionally, 93% of technical SBO participants had used private browsing, compared to 66% of non-technical participants, which was also a significant difference ($p < 0.001, \phi = 0.3$).

A significantly larger portion of participants from Mechanical Turk (91%) had used private browsing compared to participants in the SBO (73%), ($p < 0.001, \phi = 0.3$). We also found that Mechanical Turk participants reported using private browsing significantly more frequently than SBO participants ($p < 0.001, \phi = 0.2$). From Mechanical Turk, 28% reported that they had used private browsing at least half of the time in "the past week" (i.e., the week immediately prior to the survey being administered) on their computer and 23% had used it at least half of the time on their mobile device. In contrast, only 16% of SBO participants used it at least half of the time on their home computers and 15% used it at least half of the time on their mobile device.

Neither the participant's primary browsing platform nor operating system of their main home computer impacted whether and how much they used private browsing, in either the Mechanical Turk and SBO populations. Similarly, we found that having a shared computer did not correlate with more usage of private browsing.

4.2 Patterns in Private Browsing Usage

Of the 451 SBO participants whose browsing data was used for this analysis, 184 (41%) had used private browsing at least once. Overall, private browsing occurred in only 4% of browsing sessions captured by the SBO.

4.2.1 Use Cases for Private Browsing

Table 3 displays the results of our manual coding of 6,327 private browsing sessions. Though adult browsing and other sensitive activities were observed in a substantial proportion of private sessions, they were, surprisingly, not the most common use cases. The most common activities were using a service which required a login (38% of sessions) and performing a search query (33%). Activities that did not fall into a specific use case were categorized as "general browsing," which occurred in 37% of private sessions.

Looking at the dominant use case for which our participants used private browsing, 18% of participants most commonly used it for viewing adult content, 15% used it for general browsing, and 11% used it most commonly to log into an account. However, 22% had no discernible dominant use case. This indicates that the majority of private browsing users are generally consistent in their usage of private browsing.

4.2.2 Private vs Normal Browsing Activities

Next, we examined in more detail the differences in browsing activity between normal and private browsing modes. Among 167,128 total observed sessions, 96% contained only normal non-private browsing. Over 3% of sessions contained a mixture of private and normal browsing, and about 0.5% of sessions contained exclusively private browsing. Sessions containing private browsing comprised 6% of the total browsing sessions collected from observed private browsing users.

We found that, on average, "mixed" browsing sessions that contained a combination of private and non-private browsing sessions were longer than other sessions, with an average duration of approximately 1 hour and 44 minutes. Sessions containing only non-private browsing had an average duration of approximately 43 minutes, while sessions containing only private browsing had an average duration of approximately 23 minutes. On average, normal browsing sessions contained 73 page visits, while sessions conducted only in private browsing contained 40. The average mixed session contained 175 page visits, 34% of which were performed in private browsing windows. This suggests that typically, users switch to private browsing mode to accomplish a task and switch back to normal mode to resume their browsing.

We found the distribution of the browsers used in normal browsing to be significantly different than those used in private browsing ($p < 0.001, V = 0.2$). In normal browsing 65% of participants used only Chrome, 7% used only Firefox, and 31% had used both. However, in private browsing 83% used Chrome, 10% used Firefox, and only 7% used both browsers, indicating that some users of both browsers have decided to use one or the other for private browsing.

The set of domains visited in private mode was found to be dissimilar to those visited in normal browsing, with a Jaccard similarity coefficient of 0.02. The distribution of website categories between normal and private browsing was also found to be significantly different ($p < 0.001, V = 0.1$). Of the most common AWIS categories, email, news, portal, shopping, and social media domains comprised a larger proportion of domains visited in private browsing than in normal browsing. Financial, health, political, search, software, and streaming domains comprised a roughly equal proportion. We observed that 6% of all distinct domains visited in private browsing were categorized as an adult content website, while only 1% of domains were such in normal browsing.

The searches conducted in private browsing were significantly different than those conducted in normal browsing ($p < 0.001, V = 0.1$). Altogether, 16% of searches conducted in private browsing were categorized under a sensitive category, while only 2% of searches were such in normal browsing. The most prominent sensitive search categories in private browsing were searches for adult and health-related content. Searches for adult content comprised of 12% of all private browsing search queries, but only made up 0.5% of

Gender			Age			Education			Tech Expertise			IUIPC (average)		
	MTurk	*SBO*		*MTurk*	*SBO*		*MTurk*	*SBO*		*MTurk*	*SBO*		*MTurk*	*SBO*
Female	43%	61%	18-24	9%	32%	High School	16%	3%	Expert	16%	25%	Control	5.8	4.4
Male	55%	38%	25-34	58%	32%	Some college	20%	19%	Non-Expert	84%	75%	Awareness	6.2	4.9
Other	.3%	.4%	35-44	20%	11%	Trade School	2%	2%				Collection	5.6	5.8
No answer	1%	1%	45-54	9%	8%	Associates	13%	6%						
			55-64	4%	7%	Bachelors	40%	37%						
			65-74	1%	8%	Graduate	8%	34%						
			75-84	0%	2%	No answer	1%	.4%						
			No answer	0%	.4%									

Table 2: Demographic breakdown of our 305 Mechanical Turk participants and 227 survey participants from the SBO. A smaller proportion of SBO participants are male and have technical expertise, compared to the Mechanical Turk population. SBO participants are also more varied in age, more educated, and less privacy sensitive, as measured on the seven-point IUIPC scale.

Use Case	% of Private Sessions Activity was Observed	% of Private Browsing Users Who Did Use Case	% of Private Browsing Users - Dominant Use Case
Log into service	38%	57%	11%
General browsing	37%	66%	15%
General searches	33%	61%	6%
Access adult content	24%	49%	18%
Streaming video/audio	19%	41%	5%
Visit social media	15%	35%	3%
Shopping	12%	42%	5%
Adult-content searches	12%	42%	1%
Sensitive browsing	8%	33%	3%
Sensitive searches	5%	30%	0%
Look up someone's name/profile	3%	25%	1%
Pirate content	1%	7%	1%
Bypass news limits or ad-blocking detection	0.9%	5%	2%
Sensitive shopping	0.6%	10%	0%
Other	2%	11%	1%

Table 3: Summary of private browsing usage in the SBO, displaying the percentage of private browsing sessions in which participants used private browsing for that use case, the proportion of private browsing users in the SBO who used private browsing for each use case, as well as the percentage of private browsing users for which the use case was their dominant reason for using private browsing. About 22% of participants had no discernible dominant use case.

normal browsing queries. Health-related searches were 3% of private browsing searches but only 0.4% of normal searches. The distribution of the types of YouTube videos viewed in private browsing also was found to be significantly different from that viewed in normal browsing ($p < 0.001, V = 0.1$). Proportionally, three times as many videos viewed in private browsing were removed for violating the website's policy on nudity and sexual content and twice as many had content warnings indicating age restricted content. However, overall, these videos made up fewer than 5% of YouTube videos viewed in private browsing. Other videos tagged as infringing or graphic content occurred in roughly equal proportions.

4.3 SBO Observed vs Reported Activities

In this section we provide a comparison of the private browsing activities reported by SBO participants in their survey responses and those empirically observed by the SBO software, so that we can better understand the limitations of prior work utilizing only self-reported data. We find that there were discrepancies between the activities reported by participants and those observed by the SBO, which suggests that participants over-reported on the survey, or performed private browsing activities on other devices. However, the overall activities in the two data sources were similar, indicating that self-reported data is still a valuable means to study research problems in this area.

4.3.1 Usage of Private Browsing

As stated in Section 4.1, 166 (73%) of SBO survey participants reported that they had used private browsing mode in the past. However, only 101 (61%) of these participants had private browsing activities observed by the SBO. Some of these discrepancies are due to participants using private browsing on a non-SBO configured device. Of the participants for whom private browsing activity was reported but never observed, 58% also reported that they had used private browsing in the past month to browse or log into their account on a computer they did not own. 62% of these participants had reported using private browsing on their mobile device in the past week.

Thirteen (6%) of the SBO survey participants had reported that they had never used private browsing mode, even though the SBO software reported private browsing activity coming from their computer. Three of these 13 participants appeared to have opened a private browsing window once, perhaps accidentally, and did not actually perform any activities in private browsing. Six of the 13 participants had three or fewer private browsing sessions, most of which included an account login. One explanation for these sessions could be that someone else may have briefly borrowed the SBO participant's computer. The last four participants had between nine and 44 private browsing sessions with various browsing activities, including visits to adult websites. This suggests that very few of our participants intentionally misrepresented their lack of private browsing usage.

4.3.2 *Private Browsing Use Cases*

Our survey participants were asked about the activities they did in private browsing during the past month. There were 21 participants from whom the SBO collected private browsing data from within the 30 days prior to their survey responses, and nine use cases for which we could make direct comparisons between the two data sources. Table 4 displays the discrepancies in the reported and observed private browsing usage of these 21 participants.

Overall, there were discrepancies in the specific activities participants reported doing in private browsing and those they were observed doing. Perhaps surprisingly, participants from the survey were *over*-reporting, rather than under-reporting, their private browsing usage compared to the measurements. Averaged over the nine use cases, only 40% of participants who reported using private browsing for a use case were also observed using it for that purpose within the 30 days prior to their response. Some activities, such as using private browsing to bypass a paywall or ad-blocking detection and pirate content, had particularly large discrepancies. For most private browsing activities compared, the overall total number of participants who reported using private browsing for that activity on the survey was similar to that observed in the SBO.

When considering the entire population of SBO participants, observed behaviors were similar to those reported among the top use cases for private browsing, as shown in Table 5. Conducting searches, accessing adult content, and logging into an account were the most prominent activities in both the observed and reported data.

4.4 Conceptions of Private Browsing

In this section we describe the reasons our participants use private browsing and their understanding of the privacy protections it offers. Participants were most concerned about their browsing and search activities being saved to their computer. Other reasons for using private browsing were to protect their account credentials and personal information. Overall, participants demonstrated a lack of understanding about the technical functions of private browsing, and had misconceptions consistent with those found in prior work.

4.4.1 *Reasons for Using Private Browsing*

In their responses to the open-ended question asking what they expected to be protected from during private browsing, participants were primarily concerned about their browsing history, cookies, and search activities being saved to their device. Specific threats participants frequently mentioned included other potential users of their computers, tracking by websites or search engines, or targeted advertising. Concerningly, 12% of SBO participants and 5% of Mechanical Turk participants expressed that they expected private browsing to protect them from malicious attacks, such as malware and being hacked, highlighting a serious misconception.

Participants also had various reasons for using private browsing in particular use cases, some of which included misconceptions. Of the 144 Mechanical Turk participants and 86 SBO participants who used private browsing for online shopping, 24% of these Mechanical Turk participants and 20% of these SBO participants expressed that they thought private browsing protected their credit card or other private information. 14% of both these populations stated they used private browsing to shop for gifts. Another perceived benefit was avoiding price discrimination while shopping for an item or booking airline travel, which was mentioned by 17% SBO participants and 4% of Mechanical Turk participants who shop online using private browsing. One participant explained, "[private browsing] lets me think I am seeing 'real' prices for tickets/items instead of prices generated for me based on my preferences or visits to competitors' websites."

The primary reason for using social media in private browsing was to access social media profiles or look up someone without it being associated to their account. Some participants also thought that private browsing hides their social media activity from their employers (e.g., "I just get on social media very quickly to access and to see was going on, but again I do this at work and we're not supposed to do that though"), which is not an actual protection it provides.

12% of SBO participants and 9% of Mechanical Turk participants who used private browsing for streaming video or audio stated that they did not want their video recommendations to be impacted, which was the most common reason cited after general privacy concerns. One participant explained, "I don't want my browsing history dictating what videos I might want to watch." Four participants from Mechanical Turk and one from the SBO also mentioned reduced load times when streaming content.

Participants who used private browsing on their computers to log into a service, such as their email, most frequently mentioned that they wanted to protect their passwords or private information. Additionally, 14% of these SBO participants and 9% of these Mechanical Turk participants reported that they used private browsing because they had multiple accounts for a service, and they did not want to log out of their account in their normal browser.

Across all use cases, feelings of privacy or security were mentioned in 11% of Mechanical Turk responses and 10% of SBO responses. A participant captured this sentiment stating that they use private browsing to conduct sensitive searches for "Privacy mostly, I don't know how much more secure it is but it makes me feel better." Some participants also mentioned usability benefits. We observed that 34% of SBO participants and 24% of Mechanical Turk participants who use private browsing to access content with ad-blocking detection specifically mentioned that they switched to private browsing to avoid turning off their ad-blocker.

4.4.2 *Technical Understanding of Private Browsing*

We also asked participants to describe how private browsing worked. Nearly half (47%) of SBO participants and 60% of Mechanical Turk participants correctly conveyed that browsing history was not stored after the session had ended. Many other responses indicated that private browsing did not permanently store other information types such as cookies, login information, and form data. However, 17% of SBO survey

Use Case	Total Reported	Total Observed	% Reported, Not Observed	% Both Observed & Reported	% Observed, Not Reported
General searches	15	10	40%	60%	10%
Access adult content	14	9	36%	64%	0%
Bypass paywall or ad-blocking detection	10	1	90%	10%	0%
Log into service	8	11	25%	75%	45%
Sensitive searches	12	9	42%	58%	22%
Shopping	5	4	60%	40%	40%
Visit social media	7	5	57%	43%	40%
Streaming video/audio	6	7	50%	50%	57%
Pirate content	5	0	100%	0%	NA
Any private browsing usage	21	21	0%	100%	0%

Table 4: Summary of the discrepancies between the observed and reported private browsing activities for 21 participants who sent browsing data to the SBO in the 30-day period prior to their survey response. Of the 14 participants who reported accessing adult content in private browsing, five (36%) were not observed using private browsing for this purpose, while nine (64%) had observed visited to adult websites. All nine participants observed using private browsing for visiting adult content reported their usage.

Use Case	% of PB Users - MTurk	% of PB Users - SBO
General searches	77%	76%
Sensitive searches	71%	64%
Access adult content	66%	52%
Log into service	60%	54%
Shopping	50%	52%
Streaming video or audio	44%	39%
Visit social media	42%	43%
Bypass ad-blocking detection	42%	35%
All browsing	41%	31%
Using a computer they don't own	40%	54%
Bypass news limits	34%	39%
Log into service from a device they don't own	33%	45%
Pirate content	25%	15%

Table 5: Summary of private browsing usage reported by Mechanical Turk and SBO survey participants, displaying the percentage of participants who reported using private browsing for that use case at least once in the past month.

participants and 6% of Mechanical Turk participants indicated they were not sure how private browsing worked.

Responses to this question also revealed a variety of misconceptions about the technical mechanisms behind private browsing. Some responses indicated that private browsing protected their computer's identity, such as their browser version and operating system. Others thought private mode enabled encryption of their browsing activities (e.g.,"history gets more encrypted so that it's not as accessible"). A couple of participants casted doubts that it offered any protection.

Participants in both survey groups, on average, correctly answered between eight and nine of the 14 technical questions about private browsing. These questions also revealed participant misconceptions. One of the most glaring misconceptions indicated as correct by 22% of both Mechanical Turk and SBO participants was that private browsing prevents the browser from sending any cookies to websites. In reality, websites can still place cookies in the browser during a private browsing session but they are deleted after the session has ended. However, an even more alarming misconception is that private browsing allows for browsing the web anonymously, which was answered incorrectly by 39% of both Mechanical Turk and SBO participants. Additionally, 39% of SBO participants and 26% of Mechanical Turk participants thought that private browsing clears all browsing history from their computer after they close the browser window. This is also not correct, as only history from the private browsing session is cleared.

In both survey populations, those who had used private browsing mode answered one or two more questions correctly, on average. As seen in Table 6, the largest gaps in understanding between users and non-users of private browsing were related to information exchange between the user's computer and another entity, such as the ability of the Internet Service Provider to see browsing activity and the computer's IP address being shared with websites. Demographics were not correlated with understanding in the Mechanical Turk survey population, but females and those older than 65 were observed to have answered fewer questions correctly in the SBO survey population. In both survey populations, higher privacy awareness, measured by reported cookie policy, presence of a privacy-related browser extension, and the IUPIC control, awareness, and collection factors, did not correlate with a better understanding of private browsing.

Our results are in line with those observed by Gao et al [16]. Participants in their study showed a similar awareness that browsing history and cookies are deleted in private browsing mode, and desired to keep their activities private from other users of their computer. They also demonstrated similar misconceptions as participants in our study, such as private browsing can block all tracking from websites and will prevent viruses and advertisements.

5. DISCUSSION

Our study accomplishes three goals: investigate how people use private browsing, learn if there are discrepancies between reported and empirically-measured private browsing behaviors, and determine whether private browsing offers users the security and privacy protections they expect to receive. We analyzed a combination of empirical data from the SBO, and survey data from the SBO and Mechanical Turk.

Technical Understanding Question	**% of Users Who Answered Correctly**		**% of Non-Users Who Answered Correctly**	
	MTurk	*SBO*	*MTurk*	*SBO*
Private browsing clears my browsing history for that session from my computer after I close the browser window	89%	85%	81%	69%
Private browsing does not save my login information after I end that session.	87%	84%	77%	64%
Private browsing clears most cookies for that browsing session from my computer after I close the browser window.	84%	81%	88%	69%
Private browsing clears all the information that I fill into forms in that session from my computer.	83%	74%	62%	54%
Private browsing blocks ads on the websites I visit.*	73%	71%	54%	54%
Private browsing does not allow my Internet Service Provider (e.g., Comcast, Verizon) to see which websites I visited during that session.*	66%	69%	38%	33%
Private browsing blocks some tracking by advertisement and social media companies.	62%	60%	85%	67%
Private browsing prevents companies from targeting ads to me based on my browsing history from previous private browsing sessions.	61%	62%	77%	64%
Private browsing does not allow websites to get my computer's IP address or any information about my web browser or computer.*	61%	58%	31%	28%
Private browsing prevents companies from targeting ads to me based on any of my previous browsing history.	60%	49%	77%	62%
Private browsing causes the information I send to websites to be encrypted.*	55%	50%	35%	20%
Private browsing allows me to browse the web anonymously.*	51%	52%	31%	40%
Private browsing clears all my browsing history from my computer after I close the browser window.*	27%	42%	12%	31%
Private browsing prevents my browser from sending any cookies to websites.*	24%	26%	0%	13%

Table 6: Percentage of correct responses by users and non-users of private browsing to the 14 technical understanding questions. Statements marked with a "*" are a false statement about private browsing, while all others are true.

Distributing the survey to two populations, especially ones with different demographics, allows us to consider the generalizability of our results. The Mechanical Turk population was younger and likely more technically savvy than the SBO group. Additionally, Mechanical Turkers, on average, reported higher privacy concern on the IUIPC scale compared to the SBO population, and have been found to be more privacy conscious than the U.S. population as a whole [20]. These two factors likely contributed to why Mechanical Turk participants reported using private browsing more frequently than the SBO participants. Despite the differences in the amount of private browsing usage, the top activities performed in private browsing were the same across both populations. This suggests that the most common activities for which private browsing is used may be universal.

Overall, we observed a variety of activities for which people use private browsing, including log-ins to Internet services and search engine queries. Though there were disparities in the usage reported by SBO participants and that which was observed, the most common private browsing activities were the same across both data sources. Lastly, we found that some participants use private browsing for purposes that do not match with the actual protections it provides.

5.1 Usability and Design Implications

We observed that the typical pattern for private browsing usage is that users start a private browsing session for a specific task, and then switch back to normal browsing mode. This could be due to usability reasons, as users might enjoy the convenience of different functions of their browser, such as password auto-fill or browser extensions. Another explanation is that users realize that the protections offered by private browsing, such as hiding activity from other users or avoiding targeted ads, are diminished if they leave their private browsing window open. Perhaps ironically, some users, especially those of shared computers, may intentionally use normal browsing mode for some of their activities to throw off suspicion about their browsing habits. To better support this usage pattern, browsers could implement functions that automatically close private browsing windows after a certain amount of time, similar to how online banking sites automatically log off users after several minutes of inactivity.

Another usability reason for which people use private browsing is to log into a secondary account on their computer without having to log out of their first. However, it is unclear why this behavior is as prominent as it is, since major online services, such as Google, allow users to link their accounts and be logged into multiple accounts at once. It could be that participants may be unaware of this functionality, or that it is not implemented on many websites they use. Another possibility is that our participants prefer to keep their multiple accounts unlinked.

Participants also cited other reasons for using private browsing related to convenience. For example, many participants choose to use private browsing as an alternative to turning off an ad-blocker browser extension on websites that use ad-blocking detection. This indicates that users might find these interfaces too confusing to be able to efficiently disable it to access content.

Some participants also reported using private browsing because they experienced reduced page load times. Certain browsers, such as Firefox, may run faster in private browsing, compared to normal browsing, as browser extensions are disabled by default. Firefox also blocks certain trackers in private browsing, which could also allow pages to load faster. While this aspect of private browsing is not currently advertised by major desktop browsers, it may become more prominent in the future, as some mobile apps such as Firefox Focus already mention this benefit in their description [31].

Recent work has found landing pages for private browsing to be ineffective for dispelling certain misconceptions [44]. Our findings support the changes to private browsing disclosures recommended by the authors, such as directly stating that IP addresses can still be collected by websites. Additionally, we suggest that browsers clarify that cookies are still used in private browsing, but those placed in the browser during private browsing will not be saved beyond that session.

Our study did not comprehensively examine whether users prefer other privacy enhancing strategies over private browsing mode. While we did not find a correlation between private browsing usage and the usage of privacy and security related browser extensions, it is possible that some tools, such as Tor, lead people to use private browsing less frequently. To explore this further, future work could analyze the use of privacy enhancing strategies at an eco-system level.

5.2 Reliability of Self-Reported Methods

In comparing the observed and reported data for the SBO population, a larger proportion of participants reported using private browsing than were observed using it. Many of these participants could have used private browsing on devices not monitored by the SBO, such as their mobile device, as 62% reported doing in the past week, or on someone else's computer, which 58% reported doing in the past month. Some may have used it prior to joining the SBO. Alternatively, we might be observing a form of the Hawthorne effect, such that participants may have unintentionally reported behaviors that align with their interpretation of the study's goals – in that case, affirming more security- and privacy-concerned behavior than they actually evidence.

On the other hand, very few participants whose computer sent private browsing activity to the SBO reported on the survey that they had never used private browsing mode. Additionally, all of the participants who were observed accessing adult content in private browsing reported that activity on the survey. This seems to indicate that people are willing to report some behaviors truthfully on a survey, even if it requires the revelation of activities some may find private or embarrassing to disclose.

Our findings highlight that there are limitations to both empirical and self-reported methods for studying behaviors such as private browsing. Though empirical data collection, like that implemented by the SBO, can provide ground truth for users' activities, it is very difficult to capture everything they do online, as people tend to use multiple devices. While self-reported methods can capture information about all the activities a user does, they suffer from the biases discussed earlier. Studies should utilize both types of methods to maximize coverage and minimize bias.

5.3 Is Private Browsing Enough?

For many users, private browsing functionality matches the privacy protections they expect. Participants most commonly reported using private browsing to hide their activities from other users of their computer. Interestingly, usage of private browsing was found to be independent of whether or not a participant had a shared computer. In their qualitative responses, those who did not typically share their computers frequently referred to rare occasions in which someone might use their computer. Despite having some protections, users should be aware that there is still privacy risk to their private browsing activities. Though private browsing does not permanently store browsing data that is easily accessible to other users, the browsing activity of a prior user could still be potentially seen if their private browsing window was left open, or if they had logged into an account, such as Google, which synced their browsing activity to their browser.

Another common threat participants seek protection from is tracking by websites or search engines. Private browsing does provide a degree of protection against web tracking, as some tracking information, such as cookies are not persistent once the user closes the browsing window. Additionally, many participants used private browsing so that certain activities were not linked to their Google account, which by default they are logged out from in private browsing mode. However, we found that some participants performed certain tasks to prevent Google and other websites from recording the activity, and not just to prevent it from being linked to their computer or account. Users may not be aware that their search and YouTube activities are still being sent to Google even if they are not logged in, which some might still consider as a privacy invasion. Similarly, websites still record the activities of visitors to their website using various trackers that do not require an account login.

Many participants also expressed concerns about receiving targeted advertising. Though private browsing will prevent access to tracking cookies set in normal browsing mode, it does not prevent new ones from being set. Furthermore, advertisement agencies can still use other practices such as browser fingerprinting [11] and IP targeting [9] to serve targeted advertisements to a user or household. Safari and Firefox do enable some additional tracking protections in private browsing, but they still do not offer full protection against such techniques.

Our results indicate that people also use private browsing for security reasons, beyond generally maintaining their privacy. Some thought that private browsing would prevent attackers from hacking into their accounts or stealing their identity, for which private browsing does provide some protection. For example, private browsing does mitigate session hijacking attacks which use active logins [19]. However, it is likely that users are more concerned about vulnerabilities introduced by forgetting to log out of an account. In some cases, participants overestimated the protection against the security threats. For example, private browsing mode does not prevent users from downloading viruses or malware, nor does it provide additional protections than those offered from normal browsing in the transmission of their credit card and other personal information.

In about 10% of responses, participants were not sure exactly what private browsing protected them from, but expressed that they used private browsing because it provided some feeling of privacy or security. These misconceptions can be especially dangerous if users naively choose to use private browsing to conduct online activities which put them at risk, thinking they are being protected.

6. ACKNOWLEDGMENTS

This work was funded by the National Security Agency (NSA) Science of Security Lablet at Carnegie Mellon University (contract #H9823014C0140). Additional support was provided by the National Science Foundation (NSF) and the

Hewlett Foundation, through the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley. We also would like to thank our reviewers for their feedback.

7. REFERENCES

[1] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[2] A. Acquisti, S. Komanduri, P. G. Leon, S. Wilson, L. F. Cranor, N. Sadeh, Y. Wang, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, N. Sadeh, F. Schaub, M. Sleeper, and Y. Wang. 44 nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(44), 2017.

[3] L. Agarwal, N. Shrivastava, S. Jaiswal, and S. Panjwani. Do not embarrass: Re-examining user concerns for online tracking and advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 8:1–8:13, 2013.

[4] G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh. An analysis of private browsing modes in modern browsers. In *Proceedings of the USENIX Security Symposium*, 2010.

[5] J. Angulo. "WTH..!?!" experiences, reactions, and expectations related to online privacy panic situations. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 19–38, 2015.

[6] Apple Support. Browse in private. `https://support.apple.com/guide/safari/browse-privately-ibrw1069`, November 2017.

[7] C. Canfield, A. Davis, B. Fischhoff, A. Forget, S. Pearman, and J. Thomas. Replication: Challenges in using data logs to validate phishing detection ability metrics. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[8] J. Cohen. Statistical power analysis for the behavioral sciences. *NJ: Lawrence Earlbaum Associates*, 2, 1988.

[9] DBS Interactive. IP targeting 101: Smart display advertising. `https://www.dbswebsite.com/blog/2016/03/16/ip-targeting-101-smart-display-advertising/`, November 2017.

[10] DuckDuckGo. A study on private browsing: Consumer usage, knowledge, and thoughts. Technical report, 2017. `https://duckduckgo.com/download/Private_Browsing.pdf`.

[11] P. Eckersley. How unique is your web browser? In *Proceedings of the International Symposium on Privacy Enhancing Technologies (PETS)*, pages 1–18, 2010.

[12] M. Fagan and M. M. H. Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 59–75, 2016.

[13] A. Forget, S. Komanduri, A. Acquisti, N. Christin, L. F. Cranor, and R. Telang. Security Behavior Observatory: Infrastructure for long-term monitoring of client machines. Technical Report 14-009, Carnegie Mellon University CyLab, 2014.

[14] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. Do or do not, there is no try: User engagement may not improve security outcomes. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 97–111, 2016.

[15] S. Fox. Adult content online. *Pew Research Center*, 2005.

[16] X. Gao, Y. Yang, H. Fu, J. Lindqvist, and Y. Wang. Private browsing: An inquiry on usability and privacy protection. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*, pages 97–106, 2014.

[17] Google Chrome Help. Browse in private. `https://support.google.com/chrome/answer/95464?co=GENIE.Platform{%}3DAndroid{&}hl=en`, November 2017.

[18] P. Jaccard. The distribution of the flora in the alpine zone. *New Phytologist*, 11(2):37–50, 1912.

[19] M. Johns. SessionSafe: Implementing XSS immune session handling. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, pages 444–460, 2006.

[20] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of Mechanical Turk workers and the US public. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 37–49, 2014.

[21] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "My data just goes everywhere": User mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 39–52, 2015.

[22] A. Kittur, E. H. Chi, and B. Suh. Crowdsourcing user studies with Mechanical Turk. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 453–456, 2008.

[23] J. Lazar, J. Feng, and H. Hochheiser. *Research Methods in Human-Computer Interaction.* Morgan Kaufmann, 2017.

[24] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[25] Microsoft Support. Browse inprivate in microsoft edge. `https://support.microsoft.com/en-us/help/4026200/windows-browse-inprivate-in-microsoft-edge`, November 2017.

[26] Microsoft Support. Change security and privacy settings for internet explorer 11 - windows help. `https://support.microsoft.com/en-us/help/17479/windows-internet-explorer-11-change-security-privacy-settings`, November 2017.

[27] R. Montasari and P. Peltola. Computer forensic analysis of private browsing modes. In *Proceedings of the Communications in Computer and Information Science (CCIS)*, volume 534, pages 96–109, 2015.

[28] Mozilla Blog of Metrics. Understanding private browsing. `https://blog.mozilla.org/metrics/2010/08/23/understanding-private-browsing/`, October 2017.

[29] Mozilla Support. Private browsing - use Firefox without saving history | Firefox help. `https://support.mozilla.org/en-US/kb/private-`

browsing-use-firefox-without-history, November 2017.

[30] Mozilla Support. Tracking protection | Firefox help. https://support.mozilla.org/en-US/kb/tracking-protection, November 2017.

[31] Mozilla Support. Firefox focus. https://support.mozilla.org/en-US/kb/focus#w_performance, February 2018.

[32] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh. Privacy expectations and preferences in an IoT world. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[33] D. J. Ohana and N. Shashidhar. Do private and portable web browsers leave incriminating evidence?: A forensic analysis of residual artifacts from private and portable web browsing sessions. *EURASIP Journal on Information Security*, 2013(1):6, 2013.

[34] Opera Help. Private browsing. http://help.opera.com/Mac/12.00/en/private.html, November 2017.

[35] S. Panjwani and N. Shrivastava. Understanding the privacy-personalization dilemma for web search: A user perspective. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 3427–3430, 2013.

[36] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 295–310, 2017.

[37] K. Purcell, J. Brenner, and L. Rainie. Search engine use 2012. *Pew Research Center*, 2012.

[38] E. Rader. Awareness of behavioral tracking and information privacy concern in Facebook and Google. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 51–67, 2014.

[39] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish. Anonymity, privacy, and security online. *Pew Research Center*, 2013.

[40] K. Satvat, M. Forshaw, F. Hao, and E. Toreini. On the privacy of private browsing - a forensic approach. *Journal of Information Security and Applications*, 19(1):88–100, 2014.

[41] F. Shirazi and M. Volkamer. What deters jane from preventing identification and tracking on the web? In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*, pages 107–116, 2014.

[42] C. Soghoian. Why private browsing modes do not deliver real privacy. *Center for Applied Cybersecurity Research*, pages 79–94, 2011.

[43] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao. You are how you click: Clickstream analysis for sybil detection. In *Proceedings of the USENIX Security Symposium*, volume 9, 2013.

[44] Y. Wu, P. Gupta, M. Wei, Y. Acar, S. Fahl, and B. Ur. Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In *Proceedings of the International Conference on World Wide Web (WWW)*, pages 217–226, 2018.

APPENDIX

WARNING: Appendix B contains explicit content relating to search terms used to identify sensitive search engine queries.

A. DOMAIN CATEGORIES

The domain categories returned by AWIS were categorized into the following categories:

- adult
- audio
- education
- email
- financial
- health
- news
- political
- portal
- search
- shopping
- social_network
- software
- video
- other

B. SEARCH ENGINE QUERIES

The following keyword lists were used to identify sensitive searches conducted by SBO participants.

Adult: 2 girls, 4 girls, adult, ageplay, anal, aphrodisiac, asshole, august, bdsm, bikini, blow job, blowback, boob, brenner bolton, chaturbate, cheating, christian mingle, cock, dating site, derpibooru, dick, digital playground, ennio gaurdi, erotic, fetish, fleshlight, foursome, fuck, gay, gaydar, gianna michaels, hentai, horny, jackinworld, lesbiantube, literotica, madison scott, masturbat*, mfc, naked, naughty, nip slip, nipslip, nsfw, nude, nudography, orgasm, osiris blade, pigtails in paint, porn, pussy, reality kings, redtube, riley reid, sex, slut, squirt, strip club, strip poker, strip tease, sucking, threesome, tit, topless, tub girl, upskirt, vagina, virgin, xhamster, xkeezmovies, xtube, xvideo

Health: alcohol tolerance, aloe, anorexia, anxiety, asperger, bedsore, blister, body fat, burn, cabergoline, calories, careprostcanada, colonoscopy, concussion, condom, counseling, creatine, creatinine, cyproheptadine, dht, dim, doctor, dopamaine, dopamien, dry scalp, ephedra, ephedrine, feeling weak, fingering, fingured, glycemic, hair grow, heart beat, heartburn, hepatitis, hernia, hydrocodone, hypogonadism, hypogonadism, hysterectomy, infection, ingrown, insurance, itchy, leprosy, lice, lower back, malaria, medicaid, medical, menstrual, metamucil, minoxidil, mylanta, nose, nurofen, organ, pain, pediatric, penis, physical, pregnancy, proctolgist, prolactin, provider lookup, rohypnol, scar, serotonin, sickness, sneez*, ssri, stomach, sudafed, swollen, tattoo care, testosterone, thalidomide, therapy, tibulus, upset stomach, urine, valtrex, vicodin, yellow fever, zyrtec

Financial: american express, bank, bitcoin, bond, capital one, credit card, fcu, financial, income, interest rate, loan, pnc, salar*, stipend, stock, tax, wells fargo

Copyright: 1337x, dvdrip, ebook, piracy, pirate, piratebay, torrent

Political: bannon, bush email, Donald Trump, election, flag burning, free speech, heavens gate, jared kushner, jeff sessions, kim jung un, march for life, potus, president, protest, scaramucci, science march, spicer, trans murders, trump, vote

Other Sensitive: a joint, abuse, attack, cannabis, darknet, dies, eaze, fire, genocide, parramore, pcp, personal injury, pot, pulse, rape, weapons, weed

C. YOUTUBE ACTIVITY

The text of the element "unavailable-message" from the HTML of YouTube videos returned the following codes which indicated infringing, sensitive, or adult content related videos:

- Content Warning
- Copyright Violation
- Nudity/Sexual Content Violation
- Scam/Deceptive Practices Violation
- Terms of Service Violation
- Violent/Graphic Content Violation
- Community Guidelines Violation

D. SURVEY QUESTIONS

Description **For the duration of this survey we ask that you answer questions based on your behaviors and expectations associated with browsing the internet on your main home computer (desktop or laptop), unless stated otherwise.**

1. Which browsers do you regularly use? Check all that apply.

   □ Chrome
   □ Edge
   □ Firefox
   □ Internet Explorer
   □ Opera
   □ Safari
   □ Other

Every browser listed above has a built-in feature that allows users to engage in private browsing. However, they each refer to it slightly differently.

- Chrome refers to this feature as **Incognito mode**
- Edge and Internet Explorer call it **InPrivate Browsing**
- Firefox and Safari use **private browsing**
- Opera calls it **private tab**

Throughout this survey we will refer to this feature simply as "private browsing."

2. Have you ever used private browsing mode on your web browser?
   ○ Yes
   ○ No
3. Do you share the computer you regularly use for private browsing with other people (e.g. siblings, parents, partners, etc.)?
   ○ Yes, but it is mainly mine
   ○ Yes, and it is mainly someone else's computer
   ○ Yes, and it is a shared/family computer
   ○ No, I am the only user
4. When you use private browsing, which of the following browsers do you use? (If you use more than one browser for private browsing, select the one you use most often.)

   ○ Chrome
   ○ Edge
   ○ Firefox
   ○ Internet Explorer
   ○ Opera
   ○ Safari

Broad Understanding

5. What would you expect to be protected from when using private browsing in the [Q3 response] browser?
6. To the best of your knowledge, what do you think actually happens when you use private browsing in the [Q3 response] browser?

Specific Understanding. Participants were shown the following Likert-style options for the set of statements below:

Definitely correct	*Probably correct*	*I don't know*	*Probably correct*	*Definitely correct*

Please select if the following statements are correct.

7. Private browsing in the [Q3 response] browser causes the information I send to websites to be encrypted.
8. Private browsing in the [Q3 response] browser clears all my browsing history from my computer after I close the browser window.
9. Private browsing in the [Q3 response] browser clears most cookies for that browsing session from my computer after I close the browser window.
10. Private browsing in the [Q3 response] browser blocks some tracking by advertisement and social media companies.
11. Private browsing in the [Q3 response] browser clears my browsing history for that session from my computer after I close the browser window.
12. Private browsing in the [Q3 response] browser does not allow my Internet Service Provider (e.g. Comcast, Verizon) to see which websites I visited during that session.
13. Private browsing in the [Q3 response] browser prevents companies from targeting ads to me based on any of my previous browsing history.
14. Private browsing in the [Q3 response] browser prevents companies from targeting ads to me based on my browsing history from previous private browsing sessions.
15. Private browsing in the [Q3 response] browser blocks all ads on the websites I visit.

16. Private browsing in the [Q3 response] browser clears all the information that I fill into forms in that session from my computer.
17. Private browsing in the [Q3 response] browser does not save my login information after I end that session.
18. Private browsing in the [Q3 response] browser allows me to browse the web anonymously.
19. Private browsing in the [Q3 response] browser prevents my browser from sending any cookies to websites.
20. Private browsing in the [Q3 response] browser does not allow websites to get my computer's IP address or any information about my web browser or computer.

Private Browsing Usage.

Participants were shown the following options for each of the use cases in Q21 below:

- ○ *Never*
- ○ *Once or a few times*
- ○ *A few times each week*
- ○ *Almost every day*
- ○ *Multiple times per day*
- ○ *Prefer not to answer*

21. How often did you perform each of the following activities in private browsing in [Q3 response] during the **past month**?
    (a) Shopping online
    (b) Performing any type of searches
    (c) Accessing social media
    (d) Logging into accounts on someone else's computer
    (e) Using a computer that isn't mine (e.g. public, friend's, or work computer)
    (f) Logging into accounts on my computer
    (g) Performing sensitive searches
    (h) Viewing adult content
    (i) Streaming content (music/video)
    (j) Accessing news websites that have a viewing limit
    (k) Accessing websites that have ad blocking detection (i.e., won't let me me access the content if my adblocker is on)
    (l) Pirating content (software, videos, music, etc)
    (m) Using it for all of of my browsing
22. Are there any other activities for which you use private browsing in [Q3 response]?
    - ○ No
    - ○ Yes, I use it for... ________________
23. What do you consider to be a sensitive search?

Specific Scenarios.

The question below was repeated for each activity the respondent indicated using private browsing in Q21.

24. What are the reasons you use private browsing in [Q3 response] when [Q21 response]?

Cookie Policy

25. What is your current cookie policy for [Q3 response]? Select all that apply.
    - □ Whatever is the default option
    - □ Block all cookies
    - □ Allow cookies from the current website only
    - □ Allow cookies from websites I visit
    - □ Allow all cookies (third-party included)
    - □ Allow session cookies
    - □ Keep cookies only until I close my browser window
    - □ I don't know

Privacy Plugins and Other Steps

26. Please select which of the following types of browser plugins and extensions you use. Select all that apply.
    - □ Protect you from malware or phishing websites
    - □ Browse anonymously
    - □ Block ads
    - □ Encrypt your communications
    - □ Protect children
    - □ Prevent websites from tracking your browsing activity
    - □ Manage passwords
    - □ Other privacy or security functions ________________
    - □ None of the above
27. Do you take any other steps to protect your privacy while browsing (other than private browsing, if you use it)?
    - ○ Yes
    - ○ No
    - ○ I don't know
28. Which steps do you normally take?

IUIPC.

Participants were shown the following Likert-style options for the set of statements below:

- ○ *Strongly agree*
- ○ *Agree*
- ○ *Somewhat agree*
- ○ *Neither agree nor disagree*
- ○ *Somewhat disagree*
- ○ *Disagree*
- ○ *Strongly disagree*

Please select how much you agree with the following statements.

29. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
30. Consumer control of personal information lies at the heart of consumer privacy.
31. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

32. Companies seeking information online should disclose the way the data are collected, processed, and used.
33. A good consumer online privacy policy should have a clear and conspicuous disclosure.
34. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
35. It usually bothers me when online companies ask me for personal information.
36. When online companies ask me for personal information, I sometimes think twice before providing it.
37. It bothers me to give personal information to so many online companies.
38. I'm concerned that online companies are collecting too much personal information about me.

Demographics

39. How often did you use private browsing in [Q3 response] in the **past week** on your **main home computer**?

    ○ Every time
    ○ Most of the time
    ○ About half the time
    ○ Sometimes
    ○ Rarely
    ○ Never

40. How often did you use private browsing in [Q3 response] in the **past week** on your **main mobile device**?

    ○ Every time
    ○ Most of the time
    ○ About half the time
    ○ Sometimes
    ○ Rarely
    ○ Never

41. How similar were the activities you did in private browsing on your mobile device to the activities you did in private browsing on your main home computer?

    ○ Completely the same
    ○ Sometimes the same and sometimes different
    ○ Completely different

42. What was different about the activities you did in private browsing on your mobile device?
43. How old are you?

    ○ 18-24
    ○ 25-34
    ○ 35-44
    ○ 45-54
    ○ 55-64
    ○ 65-74
    ○ 75-84
    ○ 85 or older
    ○ I prefer not to answer

44. How do you self identify?

    ○ Male
    ○ Female
    ○ ___________________ Other
    ○ I prefer not to answer

45. What is the highest level of education you have achieved?

    ○ Less than high school
    ○ High school graduate
    ○ Some college
    ○ Trade/Technical school
    ○ Associate degree
    ○ Bachelor's degree
    ○ Advanced degree (Master's, Ph.D., M.D.)
    ○ I prefer not to answer

46. Which of the following best describes your primary occupation?

    ○ Administrative Support (e.g., secretary, assistant)
    ○ Art, Writing, or Journalism (e.g., author, reporter, sculptor)
    ○ Business, Management, or Financial (e.g., manager, accountant, banker)
    ○ Education or Science (e.g., teacher, professor, scientist)
    ○ Legal (e.g., lawyer, paralegal)
    ○ Medical (e.g., doctor, nurse, dentist)
    ○ Computer Engineering or IT Professional (e.g., programmer, IT consultant)
    ○ Engineer in other field (e.g., civil or bio engineer)
    ○ Other ___________________
    ○ Service (e.g., retail clerk, server)
    ○ Skilled Labor (e.g., electrician, plumber, carpenter)
    ○ Unemployed
    ○ Retired
    ○ College student
    ○ Graduate student
    ○ Mechanical Turk worker
    ○ I prefer not to answer

47. Have you ever held a job or received a degree in computer science or any related technology field?

    ○ Yes
    ○ No

48. Are you either a computer security professional or a student studying computer security?

    ○ Yes
    ○ No

49. Which platform do you use most frequently for web browsing?

    ○ Laptop/Desktop
    ○ Phone/Tablet
    ○ I use both equally

50. Which operating system do you use on your main home computer?

    ○ Windows
    ○ MacOS
    ○ Linux distribution
    ○ Other ___________________

51. If you have any other comments or feedback, please use the space below.