Private Browsing: an Inquiry on Usability and Privacy Protection

Xianyi Gao†, Yulong Yang†, Huiqing Fu†, Janne Lindqvist†, Yang Wang⋆
†Rutgers University, ⋆Syracuse University

ABSTRACT

Private browsing is a feature in web browsers to prevent local users from gaining information about browsing sessions. However, it is not clear how well people interpret private browsing's functionalities and what are the privacy gains from using it. Towards studying people's understanding of private browsing, we conducted a survey on Amazon Mechanical Turk. Our survey results show that (1) one third of our participants were not aware of this privacy-enhancing feature, and (2) for people who knew or even used this feature, they had various misconceptions which could put them at risk. In the end, we provide design suggestions to help address these misconceptions.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues—Privacy; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

Keywords

Private Browsing; Incognito Browsing; InPrivate Browsing; Web Privacy; User Privacy

1. INTRODUCTION

Modern web browsers provide rich features for their users' browsing experience. These include features for both security and privacy. One such feature is private browsing, which allows users to browse the web without leaving usual traces in their computers. Generally, browsing history, search history, cookies, and temporary web files are not saved after browsing sessions in the private browsing mode. However, it does not prevent, for example, Internet service providers or employers from tracking the network traffic and pages users are viewing online. In this paper, we look into the following five major browsers having the private browsing feature: Firefox, Opera, Safari, Internet Explorer, and Chrome. To complicate things, different browsers have different names for this browsing feature. In Firefox, Opera, and Safari, it is called "Private Browsing". In Internet Explorer, it is referred to as "InPrivate Browsing". In Chrome, it is known as "Incognito Browsing".

WPES'14, November 3 2014, Scottsdale, AZ, USA

ACM 978-1-4503-3148-7/14/11 ...$15.00.
http://dx.doi.org/10.1145/2665943.2665953.

At the time private browsing was first introduced in 2005, it was mainly aimed to prevent people who share the same computer from viewing the browsing history and other related browsing traces. After being adopted by other popular browsers, private browsing did well in clearing out related histories to prevent local attackers and deleting cookies to prevent future linkage of current browsing activities. However, it had less of a guarantee of preventing the web attackers while surfing the Internet.

Although there have been studies focusing on exploring the exact functionality of the private browsing features in different web browser [1, 18], examining what files were left in the disk or cache for possible recovery [16, 17], and testing its privacy protection level [9, 22], to date there are no studies on how people perceive the private browsing features and whether their understanding matches its actual functionality. If people's mental models about private browsing do not match with how it actually works, the false sense of privacy and security might lead to privacy violations. For example, if users overestimate the privacy and security protection of private browsing, they may, for example, reveal sensitive personal information to otherwise untrustworthy websites or Internet connections. Therefore, studying users' actual perceptions toward this newly adapted private browsing feature is essential.

To the best of our knowledge, we present the first study of people's understanding of private browsing. We were interested in how many people are actually using the private browsing feature. We further probed into how private browsing users know about what private browsing does, and the degree of protection it provides. Understanding users' perceptions of private browsing can benefit further work on how to inform people about privacy features of their browsers. Our main contributions in this paper are as follows:

1. Our results show that one third of our participants were not aware of the private browsing feature.

2. For people who knew or even used this feature, they had various misconceptions which could put them at risk.

3. We provide design suggestions for web browsers to help address these misconceptions.

2. PRIVATE BROWSING IN DIFFERENT BROWSERS

Since private browsing feature was first introduced in Safari 2.0 in 2005, similar features have been adopted in other popular browsers: Google Chrome's Incognito Browsing in 2008, Internet Explorer's InPrivate Browsing in 2009, Mozilla Firefox's Private Browsing in 2009, and Opera's Private Browsing (also called Private Window) in 2010. What is common to these features that they allow users to browse the Internet without storing the historical data in the local computer.

Although the general goal is similar (e.g. trying to clear out related local files after each browsing session), private browsing varies in different web browsers. We summarized this feature from five different browsers based on how it was described by the corresponding browser [14, 15, 12, 11, 13]. Table 1 shows the private browsing feature in these browsers, as well as the comparison in the private browsing name, indicator, starting process, and what it actually does.

Internet Explorer, Chrome, and Safari have indicators showing the browser is in private browsing mode using the text or the hacker icon, while the indicator in Firefox or Opera seems subtler (e.g. small mask icon or the small sun glass icon on the top bar). The differences between the visual indicator determines whether a casual observer can tell easily if the user is in private browsing mode, as also pointed out by one earlier study by Aggarwal et al. [1]. However, they also showed that hiding the visual indicator caused users to forget to turn it off after turning on. Their study was based on older versions of Internet Explorer, Chrome, Firefox, and Safari. They showed that Safari 4 had almost no visual indicator, while as we see now, Safari 5 has the text indicator added. For the starting process comparison shown in the table, Safari changes all windows into private browsing mode when it is triggered, not allowing both normal browsing and private browsing open simultaneously.

The key feature of private browsing is to clean out the trace of browsing in the local computer, however, what files are deleted vary in different browsers. Table 1 only shows what has been publicly described within the browser description on private browsing. All five browsers have webpage history and cookies deleted after private browsing sessions. Internet Explorer and Firefox mention that online passwords are not saved by the browser while in private browsing mode [12, 13]. Safari does not explicitly mention passwords, but it has auto-filled information and entries in the download list deleted [15]. In contrast, Opera's private browsing allows users to save passwords [14]. Opera also deletes some items in the cache but does not specify what those items are. Chrome does not mention whether passwords are saved or not. Instead, it disables extensions in private browsing mode by default, allowing users to manually enable them [11]. Other browsers do not explicitly mention how extensions work in private browsing mode.

Aggarwal et al. performed a comprehensive analysis on private browsing modes in different browsers: Internet Explorer 8, Firefox 3.5, Safari 4, and Google Chrome 5 [1]. They examined private browsing's protection level against local attackers who had control over the computer after the user quits the browser, and web attackers who controlled the web sites the user was visiting. To summarize their findings, private browsing generally aims to delete changes that are initiated by a web site without the user interaction such as adding of cookies and history files to prevent local attackers. Private browsing in some browsers also tries to delete changes initiated by a web site but requiring user interaction such as saving a password for automatic login. However, it usually does not delete the changes initiated by the user such as saving a bookmark or downloading a file. Private browsing also provides some protection against web attackers although it is mainly designed to prevent local attackers. By deleting cookies, a web site cannot link a user in current private browsing session to previous private browsing sessions. However, a web site is still able to monitor the current browsing session, obtain the user's IP address, and perform online attacks such as phishing.

The implementation details of private browsing varies with different browsers and a lot of information is still recoverable from the leftover files in the physical memory. According to Aggarwal's study [1], for example, Firefox 3.5, Chrome 5, and IE 8 block data about history, cookies, HTML5 local storage from public modes to make it harder for web sites to link user's information while in private mode. However, Safari 4 does not concern about it. For browsing history recovery, Said et al. did a forensic analysis of private browsing artifacts, also mentioned in related work, showing that traces left by different browsers were different, but part of the data was usually recoverable [17].

3. RELATED WORK

The studies so far on private browsing have focused on the security and privacy functionalities or the detailed feature examination of the private browsing mode on different browsers. The earliest study was done by Aggarwal et al. in 2010 [1]. As mentioned previously, they analyzed private browsing modes in four popular web browsers and suggested that private browsing was used differently from how it was marketed. In the same year, Soghoian's work pointed out that people were ignoring browser warnings about the limitation of the private browsing feature [21]. They concluded that private browsing primarily protected users from local adversaries while paid less attention on online tracking by third party. Later in 2011, Said et al. were able to restore part of the browsing history based on the traces left in the physical memory by the private browsing mode in three web browsers [17]. Similar work was also done by Ohana and Shashidhar who tried to discover residual artifacts from private and portable browsing sessions [16]. They claimed that "artifacts must contain more than just file fragments and enough to establish an affirmative link between user and session." Their results indicated that some browsers such as Internet Explorer left enough information to establish an affirmative link and some did not. In 2013, Lerner et al. studied how the private browsing mode impacted browser extensions [9]. They created a system to analyze JavaScript extensions and observe under the private browsing mode, monitoring the degree of violation of the private browsing guarantee in extensions and notifying the user with a small annotation overhead. Motivated by Aggarwal's work, Satvat et al. also did an analysis of the private browsing in the four popular browsers with a more detailed threat mode [18]. They reported the vulnerabilities of private browsing under all these browsers and highlighted the complexity of the subject and calls for more attention about online security. In 2014, Satvat et al. further developed their work and provided

Browser	Private browsing name	Private browsing mode indicator	Starting private browsing mode	What private browsing does (Files deleted or not saved)
IE 10	InPrivate Browsing	"InPrivate" text in the front of the searching bar	Tools -> Safety -> InPrivate Browsing A new window pops up, keeping old windows open in the normal mode	Webpage history, Cookies, Temporary Internet files, Form data and passwords
Firefox 30	Private Browsing	A small mask icon on the right side of the top menu bar	Menu -> New Private Window A new window pops up, keeping old windows open in the normal mode	Webpage history, Cookies, Temporary Internet files, Form data and passwords, and Download list entries
Chrome 35	Incognito Browsing	A hacker icon on the left side of the top menu bar	Menu -> New Incognito Window A new window pops up, keeping old windows open in the normal mode	Webpage history, Cookies, and extensions disabled
Opera 22	Private Browsing or Private Window	A small sun glass icon in the browsing tab	Menu -> New Private Window A new window pops up, keeping old windows open in the normal mode	Webpage history, Cookies, and Items in cache
Safari 5	Private Browsing	"PRIVATE" text at the end of the searching bar	Settings -> Private Browsing Change all windows into private browsing mode	Webpage history, Cookies, AutoFill information, and Download list entries

Table 1: Table shows the comparison of private browsing mode in five popular browsers: Internet Explorer 10, Mozilla Firefox 30, Google Chrome 35, Opera 22, and Safari 5.

full technical details for private browsing attacks [19]. In addition, based on the responses of relevant browser vendors, they re-tested all the attacks against the newest versions of browsers and refined the suggestions for countermeasures.

The studies discussed above contributed greatly on analyzing the private browsing features of different web browsers. However, unlike our study, these studies did not probe into people's understanding of private browsing.

To further explore the background of privacy and security related features, we also looked into several studies about users' perceptions and misconceptions on other aspects of computers and web browsing. Bravo-Lillo et al. [2] conducted a study investigating how users perceived and responded to computer alerts. They found out that users frequently ignored computer warnings. Then, a mental model was built and several approaches to bridge the knowledge gap were also discussed. Chiasson et al. [4] did a usability study of two password managers that were used to generate strong passwords for web accounts. They found users having inaccurate mental models of the software and ordinary users were reluctant to use them. Another study was done by Ha et al. [6] about Internet cookies. Due to the dual property of cookies being both beneficial and malicious, they suggested users to increase awareness to prevent private issues with cookies. Friedman et al. [5] probed users about their conceptions of web security. They conducted an interview on web security and found many users mistakenly evaluated whether a connection was secure or not. Wash [22] studied folk models of security threats used by home computer users to decide which security software to use. The author used the models to illustrate why home computer users constantly ignored expert security advice and became attackers' targets. Leon et al. conducted a usability study on tools that limit online behavioral advertising [8]. They investigated nine tools and found serious usability flaws in all of them. Similar to these studies, we aim to discover false mental models about private browsing and reveal potential privacy risk due to misconceptions.

4. METHOD

In order to gather data about people's understanding of private browsing, during October 2013, we conducted a survey on Amazon Mechanical Turk with 200 participants across the United States. In this section, we discuss in detail the demographic characteristics of survey participants and our study procedure. The study was approved by the Institutional Review Board (IRB) of Rutgers University.

	Chrome	Firefox	IE	Safari	Opera
Survey result	48.5% (N=97)	38% (N=76)	8.5% (N=17)	4% (N=8)	1% (N=2)
W3Schools	54.1%	27.2%	11.7%	3.8%	1.7%

Table 2: Browser popularity from our survey result and w3schools's measurement

4.1 Participants

We recruited 200 participants to answer our survey through MTurk with 49% (N=98) female and 51% (N=102) male. All participants, who were 18 or older, were required to have some Internet browsing experience as stated in the survey description. All participants resided in the United States. 33% (N=66) of them were age 18-27, 35% (N=70) were age 28-37, 21.5% (N=43) were age 38-47, 6% (N=12) were age 48-57, and 4.5% (N=9) were age 58-68. The mean age was 35. Their highest level of education ranged from no high school to graduate degree (Master's, PhD, or Medicine). One participant did not go to high school. 10.5% of them were high school graduates. One third of them had some college experience but no degree. 35% of them had a Bachelor's degree. 8.5% had a graduate degree. The rest of them had an Associate (two year) degree. For convenience of referring to participants, we mark them from P1 to P200.

We grouped participants based on their most used web browser. Table 2 shows the distribution of participants over five different browsers, which is similar to the browser usage statistics made by W3Schools in October 2013 [10]. We did not get enough responses from Safari and Opera users. Therefore, as shown in result section, we focused on the comparison among Firefox, Chrome, and Internet Explorer. Firefox and Chrome had relatively more responses than Internet Explorer.

All participants were compensated with $0.50.

4.2 Procedure

We investigated private browsing in five different web browsers for their well-known popularity. In order to guarantee the quality of our survey result, we required workers to have 95% or higher approving rate in MTurk to answer the survey. Workers who had not completed 100 tasks could not answer the survey. We also set up timer in each survey page to count the answering time. If a participant answered our survey in rush and tried to cheat for fast completion, this participant would be disqualified.

Before taking the survey, participants were only told to complete a survey about web browsing experience. In other words, the "private browsing" idea was not revealed to participants before taking the survey. This ensured our participants to be from general population and not the particular group of people who knew about private browsing. After examining the qualifications, participants were directed to the first question asking which web browser they used most. The available options were Chrome, Firefox, Internet Explorer, Safari, and Opera. Based on their answers, questions about private browsing mode in the corresponding browser were brought up. For example, if a participant picked Internet Explorer as the most used browser, the second question would be asking "Do you know about InPrivate Browsing?" If a participant picked Chrome as the most used browser, the second question would be asking "Do you know about Incognito Browsing?" instead. All 200 participants were asked to explain what InPrivate (Private, or Incognito) Browsing does.

The survey included both multiple choice and open-ended questions. Based on whether participants knew about private (incognito, InPrivate) browsing, they were divided into two groups: the ones who did not know about private browsing (N=65), and the ones who knew about private browsing (N=136). The participants who did not know about private browsing only needed to answer one open-ended question "Please explain what InPrivate (Private, or Incognito) does", providing a chance to describe their guesses and opinions. From the group who knew about the private browsing, the ones who have used it (N=81) were required to answer five additional questions indicated below:

- "Why do you use InPrivate (Private, or Incognito) browsing?"
- "When do you use InPrivate (Private, or Incognito) browsing?"
- "Do you use InPrivate (Private, or Incognito) browsing for any specific websites?"
- "Are there any benefits of using private browsing?"
- "Are there any drawbacks of using private browsing?"

Among these five questions, four of them were open-ended questions. Only one question, "When do you use InPrivate (Private, or Incognito) browsing?" was multiple choice question for easy categorization in later analysis. The available options were morning before work, at work, at night, late at night, and other. Participants were allowed to specify the time or other explanation in "other" option (e.g. some people may not work at daytime). To help with the accuracy of our results on open-ended questions, we first read through all the responses to familiarize the range of ideas mentioned. For coding, we used a grounded theory approach [3]. We started with open coding and from 10 to 20 codes merged. Then we used axial coding for further categorization. The coding was proofread several times to ensure the correctness by two research members. In the result section, both the categorization and some samples of quoted words are shown for comparison.

5. RESULTS

In this section, we review and analyze the survey responses. We investigated participant's awareness of private browsing, reasons for using it, websites visited with this mode, time periods of usage, and benefits and drawbacks considering private browsing. Responses from different browsers were also compared.

5.1 Were people aware of private browsing?

We wanted to know whether people were aware of the private browsing feature in web browsers. After selecting the most used web browser in first question, we asked "Do you know about InPrivate (Private, or Incognito) browsing?" From overall 200 participants, about one third of them (65 out of 200) did not know about this feature in their most used web browser.

Participants' responses varied with the web browser that they were using. Figure 5.1 shows the responses of participants in different browsers. Only two participants used Opera most, and they did not know about "Private Browsing". Most Safari participants did not know about private browsing as well. However, their results might not be representative since we only had a few Safari and Opera users. Chrome had the highest percentage of users who knew about its incognito browsing feature. Firefox's responses were very close to Chrome with 68.8% (52 out of 76) users knowing private browsing. Although this result still needs further verification due to the lack of participants in Opera and Safari, the difference in the responses shows the varying popularity of private browsing across different browsers.

The result indicated that a lot of people were not aware of private browsing in web browsers. It may be due to people's lack of awareness on Internet privacy and security, or their lack of knowledge on tools that help protecting privacy. Next, we examine whether people understand how private browsing works.

5.2 What were people's understanding about private browsing?

Since in this question we aimed to find out the conceptual understanding of private browsing in the general population, our survey required all participants (N=200) to explain what InPrivate (Private, or Incognito) browsing is. Participants who had not used this feature also had a chance to express their ideas although they were not required to answer other follow-up questions. 158 out of 200 participants (79%) provided their thoughts of private browsing, while the remaining 42 participants (21%) responded "I do not know". Note that there were 65 participants saying they had not heard about private browsing in the previous question. Therefore, 23 participants were guessing based on their knowledge.

We categorized 79% (158 out of 200) responses into following four categories: (1) only browsing history was not saved (32.5%, 65 out of 200), (2) no browsing history was recorded and no cookies were stored (20.5%, 41 out of 200),

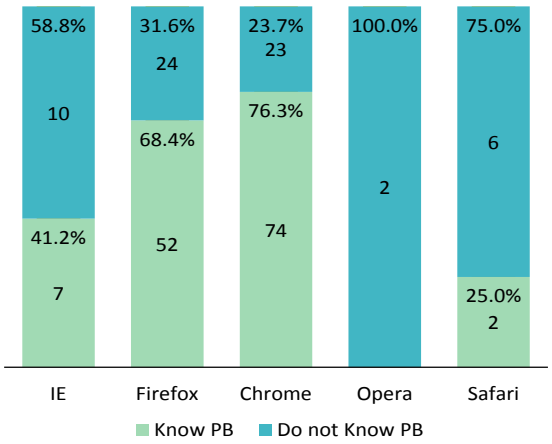

Figure 1: Figure shows response distributions from different web browsers. Both the percentage and the number of responses are shown for each category.

(3) it blocked websites and third party organizations from tracking personal online activity and users were completely anonymous (20.5%, 41 out of 200), and (4) others (5.5%, 11 out of 200) which will be discussed later. Included in these 158 responses, 23 responses were from participants who had not heard about private browsing but provided their thoughts. Nine of them were grouped into (4), six were grouped into (1), five were in (3), and three were in (2).

Browsing history was not saved. About one third of participants (65 out of 200) thought that only browsing history was not saved while using private browsing feature. Seven participants mentioned this feature was to hide their browsing history so other users could not see what had been browsed. Three of these responses are shown below:

- P3 said, "From the browsing history, future users cannot see what you used the internet for."
- P81 said, "I think it makes people on this computer cannot access my history."
- P87 said, "I think it may hide all our browsing history from other people."

Similarly, six participants said no trace or footprint about browsing history was recorded on the computer. For example, P181 said that it was a browser that allowed you to search without saving footprints about browsing history. Two participants were saying that it was a second window that didn't track on browsing history. 50 other participants in this category were also mentioning about the browsing history not being saved. For example, P32 simply said "[it] does not store history." P190 thought it disabled the saving software: "it temporarily disable the software that usually records the websites you visit, on your browsing history."

No browsing history was recorded and no cookies were stored. 20.5% (41 out of 200) of participants thought both browsing history and cookies were not stored. In this category, participants particularly mentioned browsing history and cookies. For example, P53 said "[it] doesn't accept cookies or record browsing history." One participant who used Chrome as the primary browser pointed out, "Incognito browsing doesn't generate any browsing history or tracking cookies, it's as though you're using the browser for the first time every time you use it." P131 thought that cookies and history files were deleted after browsing sessions: "When your browser session ends, the browser will clear all data, cookies and history, associated with that session." There were four participants particularly pointing out that the cookies and browsing history were deleted when window got closed or browsing session ended such as what P131 stated above.

It blocked websites and third party organizations from tracking personal online activity and users were completely anonymous. 20.5% (41 out of 200) of participants believed that private browsing would block websites and third party organizations from tracking their personal online activities. They felt secure when browsing with this feature. The responses include "no personal data is collected by websites", "it prevents other websites entering browsing history and tracking online activity", "IP address gets hidden from others", and "All browsing history, cookies, cache get cleared, making browsing activity anonymous." Some full quotes from participants are shown below:

- P39 said, "I assume private browsing involves automatically deleting cookies, cache, using private proxies. Basically, it makes the whole browsing session completely anonymous."
- P126 said, "I believe private browsing does not send my information to the websites that I am viewing so they cannot collect my data."
- P17 said, "Incognito browsing lets me browse site anonymously. My IP address is hidden so no one can track me."

Generally, participants responses in this category over estimated private browsing's protection against online attacks.

Other responses: 5.5% (11 out of 200) participants having other perspectives about this feature. Their responses include "add-ons and scripts do not work on this feature", "I guess the private mode is on judging from the name", "There is no communication with other browser instance", "It hides my online browsing habits", and others. Most of participants in this category were guessing the functionality of private browsing and not quite sure about it. We can tell by their words saying "I guess...", "I'm not sure, but I think...", and other uncertain tones. None of their responses can be grouped into any of previous categories.

5.3 Why did people use private browsing?

From 135 participants who knew about private browsing, 60% of them (81 out of 135) had used it. We asked them, "Why do you use InPrivate (Private, or Incognito) browsing?" Their responses were categorized into following seven reasons: (1) people did not want to leave any browsing history and cookies in the computer, (2) they wanted to protect their personal information from malicious websites, (3) it was for visiting dating sites and pornography, (4) they used it for online shopping, (5) they did things not related to their jobs on a work computer, (6) some just used it for curiosity and (7) other reasons. (See table 3 for survey responses.)

People did not want to leave any browsing history and cookies in the computer. From those who have used it (N=81), there were 39.5% of participants (32 out of 81)

Why do people use private browsing feature?	Participants who have used this feature (N=81)
Do not want browsing history and cookies saved	39.5%
Protect personal information (Security)	22.2%
Visiting dating or porn websites	11.1%
Online shopping	7.4%
Entertaining online on work computers	4.9%
For curiosity	3.7%
Others	11.1%

Table 3: Table shows participants' responses on why they use the private browsing feature.

said that they did not want to leave any browsing history or cookies in the computer. Most responses in this group only gave the general answer instead of some specific examples. P26 said, "Because there are times when I do not want my history tracked." P80 said, "I do not want someone else in my household to see what I have been looking at." Or some brief answers such as "to hide browsing history", "to stop cookies", and "to do my private things".

They wanted to protect their personal information from malicious websites. About 22.2% of participants (18 out of 81) thought that the private browsing feature could protect their personal information from other malicious websites. For example, P23 said, "[It can] stop malicious sites from tracking me." Also, P187 mentioned, "Sometimes I do not want to allow websites to track me. I feel a little bit more secure that my private information will not be saved in any way where someone can get to it." What P23 said was correct when we consider no tracking cookies were saved from previous browsing sessions in private browsing mode. However, malicious sites are still able to monitor online activity and collect personal information in the current browsing session. Private browsing is not designed to block untrusted websites or prevent any advanced online attacks such as phishing. Although a lot of browsing records are not stored locally, it does not guarantee a secured online browsing as what P187 might think.

It was for visiting dating sites and pornography. There were 11.1% of participants (9 out of 81) said that they used private browsing feature for visiting dating sites or porn websites. They did not want to leave any browsing history about it to prevent their spouse, girlfriend, boyfriend, or parents tracking their browsing habit. For example, P117 said, "I use it so my wife can't find out I was looking at pornography." Although it seems that responses in this category can also be included in the first category saying people did not want to leave any browsing history, this category is for participants who mentioned dating sites or pornography as their main usage. The first category is for participants who only mentioned about browsing history unsaved in general without providing any specific examples.

It was used for online shopping. 7.4% of participants (6 out of 81) said they used private browsing feature for online shopping. They felt safe and thought the personal information was secured in private browsing mode. Some of them wanted to shop online without family members' noticing. For example, participant P64 said, "When shopping for gifts for family members, they cannot trace what they are going to receive." This participant wanted to get a surprising gift for family members. Similarly, P40 said, "When I'm shopping for gifts and I do not want my husband to know." At the same time, some people thought shopping online with private browsing feature on was more secure. For example, P97 said, "I feel safe when ordering online."

Some used it to do things not related their jobs on a work computer. There were 4.9% of participants (4 out of 81) answered they were trying to do irrelevant things online on a work computer for entertainment or others. For example, participant P75 said that he "used it when playing an online game on a work computer." Also, P189 said, "I use it at work if I am doing something not work related."

Some just used it for curiosity. 3.7% of participants (3 out of 81) said that they just wanted to try out this feature to see what it does. Participant P54 said, "I do not use it all the time, but I did use it to check out websites to see if the websites treated it any differently." Participant P68 said, "I wanted to try it out and see what it was all about." And participant P29 said, "I tried it merely out of curiosity."

Other responses: 11.1% of participants (9 out of 81) provided answers such as faster browsing speed in private browsing mode, preventing from computer viruses, reduced number of on-page advertisements in private browsing mode, and tricking some websites having a data limit. In addition, there are two participants used private browsing for banking.

5.4 What websites did people visit in private browsing mode?

23 of 81 participants who have used private browsing said that they did not use it for any specific websites. The remaining 58 participants mentioned some websites they usually browsed with private browsing mode. We recorded the frequency of different websites that participants listed.

In total, 49 different websites were listed by participants: 18 porn and dating sites, nine news and entertainment sites, seven social networking sites, six finance and banking sites, four online shopping sites, two online workforce platforms, two email websites, and one advertisement website. Among the 18 porn and dating websites, Pornhub has the highest frequency of nine, Xhamster has been listed five times, and Xvideos has been listed three times. The seven different social networking websites include Facebook listed five times, twitter listed once, Tumblr and others. The six finance and banking websites were all listed once. These included PNC, Huntington, Chase, US bank, Yahoo finance, and Calcoastcu. Among four online shopping websites, Amazon had the highest frequency (listed four times). Two workforce platforms were MTurk and Swagbucks. Two email websites were Hotmail and Gmail. The advertisement website mentioned by one of the participants was craigslist.

Based on our result, porn and social networking websites were the most popular ones in private browsing mode. There were also some participants using the private browsing feature for banking, thinking private browsing provided high level of protection against online attacks and monitoring. However, private browsing actually does not prevent most malicious third parties except blocking cookies saving into computers. Our survey result indicated some misconceptions of the private browsing functionality by some people.

5.5 When did people use private browsing?

We were also interested in when people usually use this feature during web browsing. Is there any time period that people used this feature the most? In the survey, we asked "when do you use InPrivate (Private, or Incognito) browsing?" The options we gave were "morning before work", "at work", "at night after work", "late at night after 11pm", and "others (please specify)". This question was required for 81 participants who have used private browsing feature to answer. Each participant was allowed to select more than one options. 21% of them (17 out of 81) selected "morning before work". 28.4% of them (23 out of 81) used it "at work". 39.5% of them (32 out of 81) used it "at night after work". 28.4% of them (23 out of 81) selected "late at night after 11pm". And 13.6% of participants (11 out of 81) selected others. Those who selected others usually specified as "random time", "anytime", and "not specialized time". From the result, the distribution among these four time periods is quite equivalent. However, there were more participants using this feature at night than other periods.

5.6 What were the benefits and drawbacks of private browsing?

We wanted to know whether people like private browsing. Is it useful and necessary for Internet browsing? Therefore, we asked the 81 participants who had used private browsing whether there were any benefits and drawbacks of using it.

5.6.1 Benefits

The benefits can be categorized into following based on participants responses: (1) it helped protect personal privacy by not saving browsing history, (2) no cookies were saved, (3) it brought convenience of keeping computer clean, (4) it prevented malicious websites from collecting personal information, (5) it speeded up the webpage loading, (6) it prevented system from virus attack and helped blocking ads online, (7) there was no benefit, and (8) others.

It helped protect personal privacy by not saving browsing history. There were 48 out of 81 (59.3%) participants mentioned the benefit of keeping personal privacy from other computer users when using private browsing. The responses include "history is not seen by others", "keep browsing secret", and "there is more confidentiality when history not saved". P102 was happy about people not seeing what websites visited while sharing the computer. Another response from P190 mentioned, "[It benefits] if you do not want someone to access your history, like if you are buying a gift for someone you live with." They all specifically mentioned browsing history.

No cookies were saved. There were 11 out of 81 (13.6%) participants saying the benefit was that no cookies were saved. The responses in this category were relatively simple. Most participants only answered "no cookies", "prevent cookies from being made", or "tracking cookies are not saved". About four participants also mentioned their online activity was not traced since no cookies were saved.

It brought convenience of keeping computer clean. There were four out of 81 (5%) participants saying that private browsing brings them convenience by automatically deleting browsing history and cookies. Participants mentioned that it saved time for users who needed to delete browsing history constantly and saved space in computer by not saving cookies and cache files.

It prevented malicious websites from collecting personal information. There were four participants saying that private browsing was more secure and it protected users from malicious websites. Participant P48 said, "It gives me additional security. It prevents websites from getting my information."

It speeded up the webpage loading. There were three participants thought private browsing speeded up the webpage loading. P4 thought that the browser did not slow down because some images, add-ons, and scripts were disabled. P90 said, "I feel like the online videos load faster in it." P43 had similar experience: "I use it for reading articles in New York time. Web pages load faster in it."

It prevented system from virus attack and helped blocking ads online. There were three participants thinking private browsing benefits system security by avoiding virus attack or blocking ads online. For example, P193 said, "It really does seem to reduce the amount of spam and ads." In addition, P20 pointed out, "My system won't be attacked easily when I search online." However, these are not part of private browsing's functionalities.

There was no benefit. Surprisingly, there were four out of 81 (5%) participants saying there was no benefit at all. They doubted about what private browsing feature actually does. For example, P198 said, "Doubt it. That's why I rely on clearing my search history and passwords and setting the browser to erase them each day."

Other responses: Three responses were not falling into any of these categories. Their responses included a simple answer of "yes", a not so sure answer saying only "use it for curiosity", and a response saying "not sure what it does."

5.6.2 Drawbacks

81 participants who have used private browsing were required to answer the possible drawbacks of private browsing. Majority of them (38 out of 81, 46.9%) said (1) there was no drawback for private browsing feature. 28.4% of participants (23 out of 81) said they (2) could not view browsing history when needed. Seven out of 81 (8.6%) participants said their (3) sign-in information not saved. Four out of 81 (4.9%) participants felt that (4) some of the browsing functions might not work in private browsing mode. (5) There were nine other responses providing different options which will be shown next.

Browsing history was not available when needed. 23 participants said that they could not view the browsing history when needed. Although this is the major functionality of private browsing feature, it can also be a drawback sometimes, as what P31 and P190 mentioned:

- P31 said, "If I see something I like and cannot recall what it is, it can be difficult sometimes to find it again."
- P190 said, "The opposite side of not retaining history is that you can't access things you may have closed accidentally. Sometimes, I'll end up browsing in an incognito window, accidentally closing a recipe or something I want to come back and find again, but then I have no way of figuring out what it was."

Sign-in information was not saved. Since private browsing feature blocks cookies and some temporary Internet files from saving to computers, sign-in information is usually not stored in most browsers. This can be a drawback as pointed out by seven participants. For instance,

P79 said, "Sign-ins can be annoying. Stuff isn't saved, so in the future if I want to visit the same site, it's hard to find." Also, P187 said, "Since no passwords or history or cookies is saved, the next time I visit the site, I would have to re-enter all of my information. On retail sites, the sites would not know my preferences."

Some of the browsing functions might not work in private browsing mode. Four participants thought private browsing might not provide a full featured browsing experience. P56 said, "It's not a full featured browser. I have to fill in form data [every time]." What P56 meant was auto-fill data not saved by the browser in private browsing mode. He interpreted it as part of browser's feature. P147 doubted about whether some websites would work well on private browsing: "I'm not sure if website would work with private browsing. I turn it off when working on MTurk in case it could cause problems." In addition, P48 said, "Some of my browsing functions such as plug-ins and add-ons do not work."

Other responses: There were nine other responses on drawbacks that did not fall in any of the previous category. The ideas can be summarized into following: a) some agencies can still track on personal online activities, b) no options available to save information such as no bookmark available for videos, c) it encourages secrecy and dishonesty in a relationship, and d) not sure whether there is any drawback or not. Following shows responses from three participants:

- P38 said, "Yes, there are certain agencies that can still view what you do online regardless of any security measures you take."
- P70 said, "I can't bookmark my favorite videos."
- P175 said, "It encourages secrecy and dishonesty in relationship."

5.7 Were there any noticeable difference among responses for different browsers?

In our survey, we were using different names referring to the private browsing in different browsers. We grouped participants into five groups based on their most used browser to learn whether they had different perceptions for the private browsing feature in different browsers. Therefore, we compared participants responses from different browsers.

Response difference in what InPrivate (Private, or incognito) browsing does: There were 200 participants responded about what private browsing does. We grouped participants based on their most used browser. 97 participants were in the Chrome group. Secondly, 76 participants were in Firefox group. Then, 17 participants were in the Internet Explorer group. Only eight participants were in the Safari group, and the remaining two were in the Opera group. Table 4 shows the responses comparison across Firefox, Chrome, Internet Explorer, Safari, and Opera. The categorization is the same as when has been presented previously regarding the same question about what private browsing does.

The number of responses from Safari and Opera browser was too small to address meaningful conclusion. Therefore, we focused on comparing the results of the remaining three sets of survey responses from Chrome, Internet Explorer, and Firefox. Only 15.5% of Chrome participants (15 out of 97) did not know about "Incognito Browsing". However, almost half (47%, 8 out of 17) of Internet Explorer participants did not know about "InPrivate Browsing". Since the number of responses for Internet Explorer (N=17) is much smaller than Chrome and Firefox, we are uncertain whether it is the number of responses or the browser difference causes the variation of result comparing to Chrome and Firefox. The distribution of responses for Chrome and Firefox was very similar although slightly more Chrome users thought only browsing history was not saved in private browsing mode.

What private browsing does	Firefox (N=76)	IE (N=17)	Chrome (N=97)	Safari (N=8)	Opera (N=2)
No Browsing History	27.6%	35%	36%	25%	0%
No History and Cookies	28.9%	5.9%	16.5%	25%	0%
Completely Anonymous	19.7%	5.9%	24.7%	12.5%	0%
Others	5.3%	5.9%	7.2%	0%	0%
I do not know	18.4%	47%	15.5%	37.5%	100%

Table 4: Table shows different response distributions for the private browsing feature in five different browsers.

Why do you use private browsing?	Firefox (N=30)	IE (N=3)	Chrome (N=48)
Do not want to store history and cookies	40%	33.3%	40%
Protect Personal Information Online (Security)	23.3%	33.3%	20.8%
Visit dating sites and pornography	10%	0%	12.5%
For online shopping	6.7%	0%	8.3%
Just for Curiosity	0%	0%	6.25%
Do irrelevant things on work computer	6.7%	33.3%	2.1%
Others	13.3%	0%	10.4%

Table 5: Table shows response distributions for private browsing modes for Firefox, Internet Explorer and Chrome. No participants have used private browsing in Safari or Opera.

Response difference in why people used InPrivate (Private, or incognito) browsing: There were 81 participants answering this question. 30 of them were required to answer this question with "Private Browsing" in Firefox. 48 of them were required to answer this question with "Incognito Browsing" in Chrome. Only three of them were required to answer with "InPrivate Browsing" in Internet Explorer. For Safari and Opera, no participants were qualified to answer this question because they had not used the private browsing feature in the corresponding browser. Although there were two participants in Safari group said they had heard about private browsing, they had never used it. As shown in Table 5, the response distribution over the seven themes were very similar to each other for Firefox group and Chrome group. We did not see any noticeable difference between them. However, the "InPrivate Browsing" responses for Internet Explorer were different from others. Since there were only three participants in Internet Explorer group, we could not really derive any conclusion based on its result.

6. DISCUSSION AND CONCLUSIONS

In this section, we discuss our major findings from our survey responses. Then, we point out our survey limitations.

To conclude the paper, we provide design implications that give some suggestions to help address user misconceptions.

6.1 Discussion

One third of participants were not aware of this privacy-enhancing feature. 65 out of 200 participants that we recruited did not know about private browsing although it has been several years since private browsing was first introduced in 2005. All of our participants had some Internet browsing experience. This may reflect a fact that a lot of Internet users are not aware of online security and privacy. They are not well informed about the importance of privacy and the tools available for protection against local or online attacks. Ever from those (N=135) who knew about private browsing feature, only 81 of them had used private browsing feature, which implies that 54 of them had only heard about it and never tried to use it.

Depending on the where people learn about private browsing, they may have different understanding about it. Some of them may not feel the need of using the feature (e.g. they care less about browsing history being seen by others or they does not have any sensitive information stored by cookies). Some of them may not trust the feature.

Most participants used private browsing to protect from other local computer users. We asked participants what they use private browsing for. Most of them (about 60%) mentioned it is for protecting privacy against other local computer users. They did not want their browsing history saved. They were mainly using it for porn or dating sites and online shopping sites, and they wanted to keep online activity private from others. Some of them (about 22%) used it for protecting personal information from other web attackers. This was mainly due to misunderstanding of the private browsing functionality. This means that some of the participants overestimated the protection that private browsing provides.

Most private browsing users thought that this feature benefited them in some way. This conclusion is driven from the questions asking for benefits and drawbacks of private browsing. Most participants agreed with the benefit of protecting privacy and adding a little security for browsing. The major benefits included browsing history not saved and some tracking cookies not saved. Some of them felt more comfortable using private browsing mode online. For drawbacks, most of them (47%) said "no". Others with majority said it did not keep the history when needed. Depending on the situation, deleting browsing history and cookies can either be a benefit or a drawback.

Private browsing users in Firefox and Chrome have similar responses about their perceptions on the private browsing. After comparing participants responses for different browsers, Firefox and Chrome had similar response distribution about their users' perceptions on the private browsing. Although the responses from Internet Explorer were quite different, the number of users that we recruited was not sufficient to draw a strong conclusion. Same as for Safari and Opera users, we received even fewer responses about them than Internet Explorer. The major difference was that the percentage of participants using Internet Explorer who knew about private browsing was much less than Firefox and Chrome. Further studies are warranted to study the differences between users of different browsers.

For people who knew or even used this feature, they had various misconceptions which could put them at risk. The survey responses suggested that most of our participants who had used private browsing feature knew its main functionality as deleting browsing history and cookies. However, there were about 41 participants who believed private browsing could protect from third parties getting their information and making their online activity completely anonymous. When asked about why they were using the private browsing feature, 22.2% (N=18) participants said it protected personal information from malicious websites. Unfortunately, deleting cookies and browsing history, as what private browsing mainly does, does not help protecting personal information against most online attacks.

About 7% of participants used private browsing for online shopping. Shopping for surprise gifts was actually one of the private browsing usages that were advertised by different browsers, since automatic deletion of browsing history would keep the shopping secret. Some of our participants did mention this advantage although a lot of participants mainly used private browsing while visiting porn and dating sites. There were also two participants whose particular misunderstandings of the feature led them to feel comfortable when providing credit card information on the web.

In summary, the main purpose of the private browsing feature is to protect the user's privacy against other local computer users. This is common with the different web browsers we focused on in our study. Private browsing also helps preventing websites from linking information in previous private browsing sessions by deleting cookies, but it is not meant to protect against most online attacks. Instead, it would usually delete auto-login information and passwords so that other users sharing the same computer cannot access the accounts. It is less effective forhiding browsing activity from websites.

6.2 Limitations

The survey's sample of participants was limited to the US and the survey was conducted in MTurk. Although MTurk has great diversity with workers, it still has some biases on some particular groups of workers. Recent studies have indicated that MTurk workers have more privacy concerns than the larger U.S. public [7], and that they are heavy Internet users, early technology adopters, and techno-optimists when comped to workers by other survey providers [20].

Also, we could not conclude any noticeable differences with people's perception across all different browsers. This limits our findings. It would be better to have similar number of responses for each browser to conclude some findings about response variations in different browsers. However, this requirement is hard to achieve given that differences of the browsers popularity.

Our survey did not find out why people had various misconceptions about private browsing. They may generate from users own mental assumptions on what private browsing is based on its name or false suggestions from friends and family. Further studies should address.

6.3 Design Implications

Our survey result shows that about one third of our participants did not know about private browsing. This implies that browsers do not effectively inform their users about their private browsing features. To increase the awareness of

private browsing, browser designers could use various ways to inform users. For example, knowing porn and dating web sites are popular in private browsing mode, the browser could pop up a one-time reminder about private browsing or a notification about private browsing feature when users are visiting a porn or dating site. In addition, web browsers can put private browsing option in the main tool bar, making it more obvious visually and easier to trigger.

We also found that about 20% of private browsing users misinterpreted private browsing's main functionality. To avoid misconceptions and potential online risk, developers should highly emphasize the private browsing for local protection rather than avoiding external monitoring online. Most browser designers use paragraphs of text to inform users about private browsing features when a new private browsing window is opened. Recently, some browsers such as Firefox use videos to introduce private browsing, but they only appear when users explicitly search for private browsing online or in the help pages. A more systematic approach, based on analysis of, for example, when and how the information should be shown, should be used to inform users about what private browsing does and does not do.

Finally, one implication could be that the names of the features would be changed to something else. We leave these for the topic of further studies.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant Numbers 1223977 and 1228777. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

7. REFERENCES

[1] G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh. An analysis of private browsing modes in modern browsers. In *USENIX Security'10*, 2010.

[2] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE SP '11*, 2011.

[3] K. Charmaz. *Constructing Grounded Theory, 2nd Edition*. SAGE Publications Ltd, Mar. 2014.

[4] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *15th USENIX Security Symposium*, 2006.

[5] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. Users' conceptions of web security: A comparative study. In *CHI EA '02*, 2002.

[6] V. Ha, K. Inkpen, F. Al Shaar, and L. Hdeib. An examination of user perception and misconception of internet cookies. In *CHI EA '06*, 2006.

[7] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of mechanical turk workers and the u.s. public. In *SOUPS '14*, 2014.

[8] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor. Why johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *CHI '12*, 2012.

[9] B. S. Lerner, L. Elberty, N. Poole, and S. Krishnamurthi. Verifying web browser extensions' compliance with private-browsing mode. In *ESORICS '13*. 2013.

[10] Browser Statistics and Trends. What is the trend in browser usage? `http://www.w3schools.com/browsers/browsers_stats.asp`, 2013-10.

[11] Google Chrome Incognito Browsing. Browse in private (incognito mode). `https://support.google.com/chrome/answer/95464?hl=en`, 2014.

[12] Internet Explorer InPrivate Browsing. What is inprivate browsing? `http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing#1TC=windows-7`, 2014.

[13] Mozilla Firefox Private Browsing. Browse the web without saving information about the sites you visit. `https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info`, 2014.

[14] Opera Private Browsing. Stay secure with private browsing. `http://help.opera.com/opera/Windows/1471/en/private.html`, 2014.

[15] Safari Private Browsing. Safari 5.1: Browser privately. `http://support.apple.com/kb/ph5000`, 2014.

[16] 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. *IEEE SPW '12*, 2012.

[17] H. Said, N. Al Mutawa, I. Al Awadhi, and M. Guimaraes. Forensic analysis of private browsing artifacts. In *IIT '11*, 2011.

[18] K. Satvat, M. Forshaw, F. Hao, and E. Toreini. On the privacy of private browsing–a forensic approach. In *the 8th international Workshop on DPM'13*, 2013.

[19] K. Satvat, M. Forshaw, F. Hao, and E. Toreini. On the privacy of private browsing–a forensic approach. *Journal of Information Security and Applications*, 2014.

[20] S. Schnorf, A. Sedley, M. Ortlieb, and A. Woodruff. A comparison of six sample providers regarding online privacy benchmarks. In *SOUPS Workshop on Privacy Personas and Segmentation*, 2014.

[21] C. Soghoian. Why private browsing modes do not deliver real privacy. Technical report, 2010.

[22] R. Wash. Folk models of home computer security. In *SOUPS '10*, 2010.