EXAMINING OLDER USERS' ONLINE PRIVACY-ENHANCING EXPERIENCE FROM A HUMAN-COMPUTER INTERACTION PERSPECTIVE

BY

HSIAO-YING HUANG

DISSERTATION

Submitted in partial fulfillment of the requirements
for Doctor of Philosophy in Informatics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2019

Urbana, Illinois

Doctoral Committee:

Assistant Professor Masooda Bashir, Chair
Associate Professor Nikita Borisov
Professor Wendy Rogers
Professor Michael Twidale

ABSTRACT

The advancement of Internet technologies, including instant and unlimited access to information and services, has been an excellent source of support for older adults. However, pervasive and continuous online tracking can pose severe threats to older adults' information privacy. Surprisingly, very few empirical studies have focused on older users' online privacy-enhancing experience from a Human-Computer Interaction perspective. Therefore, it remains unclear how older users protect their online information privacy and what factors influence their online behaviors. Thus, my thesis aims to study older users' online privacy-enhancing experience by examining the following questions: 1) what older users know and do to protect their online information privacy, 2) how their emotional state influences their adoption of privacy-enhancing technologies (PETs), and 3) what usability challenges they encounter while using one of the most popular PETs currently available to the public. To examine these questions, a diverse set of empirical approaches was adopted, including a survey, a quasi-experiment, and a usability study.

My research findings suggest that three are three elements that play a crucial role in older users' online privacy-enhancing practices. First, older users' knowledge of online privacy has a significant influence on their daily online privacy protection behaviors. In addition, there seems to be a privacy knowledge gap among older users that reveals the phenomenon of 'Privacy Divide.' Second, the design of privacy-enhancing features affects older users' emotional state and their attitudes regarding their future adoption of the tool. Third, the findings of usability study indicate that the current design of a privacy-enhancing browsing tool, Tor Browser, poses particular challenges for older users. For instance, the technical terminologies and recurring warning messages have made Tor Browser more difficult for older users to use. These usability challenges not only decrease older users' satisfaction in but also deter their future adoption of the tool. Therefore, it is crucial that current design of PETs considers older users' needs.

My thesis research contributes to the privacy literature in several ways. First of all, this is the first empirical research examining older users' actual online privacy protection behaviors. In addition, this thesis includes the very first empirical study that illustrate the importance of the role of emotion in users' adoption of a privacy-enhancing tool. Furthermore, this thesis provides usability recommendations that can improve the current design of Tor Browser for older user audiences.

As the world's aging population continues to grow and advances in Internet technologies progress rapidly, the design of future technologies, from smart homes to self-driving cars, has to adopt user-centered approach, which consider end-users' needs of all age groups. Also, information privacy has become a significant aspect in our digital world, which makes the design of user-friendly privacy-enhancing tools an essential mission ahead of us. Moreover, knowledge and awareness are a key factor in older users' online privacy-enhancing practices. Henceforth, creating educational programs for older adults is extremely important in protecting their online privacy.

ACKNOWLEDGEMENTS

This journey would not have been made possible without the help from many people. First and foremost, I am extremely grateful to my advisor Dr. Masooda Bashir, for her guidance and encouragement throughout these years. She has been a role model both as a teacher and a researcher. She is one of the most knowledgeable experts in many domains, yet remains an open-minded, humble, compassionate, and caring academic advisor. Her kindness and big-heartedness have given me unconditional support throughout this process.

I am really thankful to my amazing thesis committee members for their guidance and support. Dr. Michael Twidale, who is one of the most distinguished scholars in information sciences and Human-Computer Interaction research, has always inspired me to think out-side-of-box; Dr. Wendy Rogers who is the most prestigious and distinguished leader in the field of aging and HCI research, has been supportive and providing resources whenever I needed; and Dr. Nikita Borisov who is one of the most incredible and excellent scholars in the field of privacy-enhancing technologies research, has always been encouraging and had great faith in this research. Their work has provided invaluable inspiration for my research, and their constructive feedback has led this work to a better stage.

This thesis benefited greatly from the help of many brilliant undergraduate research assistants, including Victoria Pierce, Tanisha Afnan, Shao Yie Soh, and Maya Rafalowicz. I thank them for their diligence and excellent work.

My friends and cohorts at UIUC have been my emotional support during the journey. My friends Shadi Rezapour, Wei-Ting Liao, Yuan-Ning Chu, Carmen Cheh, and Usawadee Chaiprom provided great companionship and encouragement. I am really grateful for their support and friendship for these years. Thanks to the Internet, I could get remote support from my friend Yi-Ting Wu. I thank her for spending numerous sleepless nights for lending her ears for me across the Pacific Ocean. I am so fortunate to have my sister,

Hsiao-Chu Huang, being a great company with me during this journey. Her patient and love have supported me until the end of this journey. Another important person who accompanies me during this journey is Chao-Hung Chen. He has always been my rock whenever I felt lost. I am so blessed to have his love and support that helped me overcome numerous difficulties.

Finally, my sincerest gratitude goes to my dearest parents, Pi-Tseng Huang and Hui-Chu Lin, for their unconditional love and support during this journey. Whenever I felt frustrated or lost my confidence, they always encouraged and had faith in me throughout this journey. Without them, I would never become who I am today. Walking to the end of this journey, I hope that their little girl has grown up to be someone whom they can be proud of.

Dedicated to my family

TABLE OF CONTENTS

Chapter 1. Introduction

For the first time in the history of technology, the Internet can interconnect almost everything in our daily lives. The constant and ubiquitous connectedness made possible by the Internet not only transforms the development of digital infrastructure (e.g., smart homes, smart cities) but also offers new opportunities for geriatric care in countries with increasing numbers of elderly citizens. According to a United Nations report in 2017, the number of people in the world aged 60 years or over is 962 million, and by 2050, the global population of older people is expected to reach nearly 2.1 billion. This increase in the number of older adults will have a significant impact on nearly all aspects of society, such as community, housing, and healthcare facilities, labor markets, and the cost of social security. Supporting the healthy aging of older adults is a practical and beneficial approach to confronting such issues and challenges.

From the perspective of older adults, healthy aging means having the ability to adapt to aging changes and connect with others in a supportive social environment (Koelen et al., 2017). In this context, the advancement of Internet technologies becomes an excellent source of support for healthy aging among older adults, because it provides instant and unlimited access to information, services, and social contacts. For instance, the smart home technology provided by the Internet of Things infrastructure can provide a safer home environment by connecting older adults with emergency help systems, vital signs monitoring, and fall detection systems (Peek et al., 2015). This can further mitigate the frailty of older adults and enhance their autonomy and quality of life. Moreover, older adults can also use a variety of online tools to support the self-management of their health (Oh et al., 2005).

Many people assume that older adults are inclined to avoid Internet technology. In reality, the percentage of older Internet users has been rapidly growing over the past decade. A survey by Pew Research Center (Pew, 2018) reports that in 2018, 66% of U.S.

older adults were Internet users, showing an increase of approximately 50% compared to 2001. The use of Internet technology can be beneficial for older adults, especially for those who feel socially isolated or have health problems (Choi and DiNitto, 2013). When using the Internet, older adults can communicate with other family members or friends through social networking sites; they can search for both health-related and non-health-related information on their own; they can keep learning and educating themselves via online courses; they can increase social connections by engaging in online communities; and they can shop, do their banking, make travel arrangements, or find entertainment (Choi and DiNitto, 2013). In general, the application of Internet technology provides excellent opportunities for older adults to age healthily without compromising their independence.

However, the convenience offered by Internet technologies is a double-edged sword, because its pervasive and continuous data collection come with threats to the privacy and security of older adults' information, such as online fraud, phishing attacks, and email scams. As shown in Figure 1.1, in 2017 21.2% of Internet crime victims in the U.S. were over 60 years old; an increase of around 6% since 2013 (FBI Internet Crime Report, 2013-17). Also, the total monetary loss reported by these older adult victims was $342 million in 2017, accounting for about 31% of total monetary loss reported by all victims, which reached its highest point in the past five years (see Figure 1.2). According to FBI Internet Crime reports, the total number of older adult victims decreased in 2017, yet the total amount of their financial losses increased. This means that older adult victims are experiencing more dangerous Internet crimes with greater financial risks. Furthermore, this type of cyber threat can have a disastrous impact on older adults' physical and mental health. For instance, manipulation of their medical services could negatively influence their physical health, or a privacy breach could induce psychological distress.

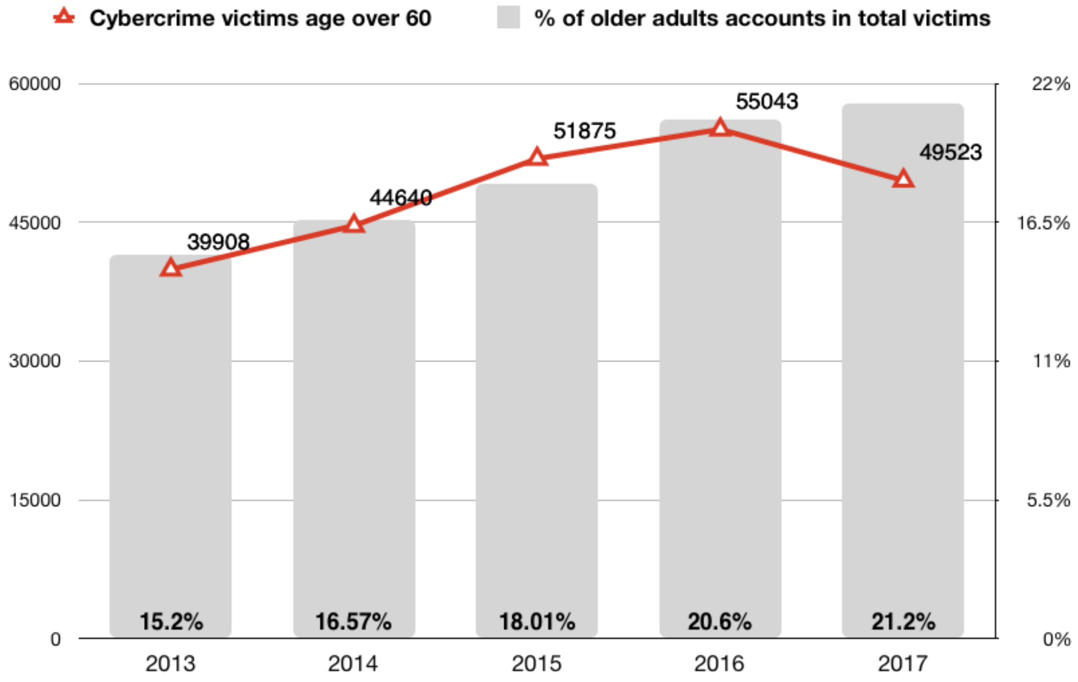


Figure 1.1: According to the FBI Internet Crime Report, the percentage of total cybercrime victims that are older adults has increased since 2013. (Data source: FBI IC3 reports from 2013 - 2017)

Approximately one-fifth of Internet crime victims are older people, who may face greater risk in terms of financial loss or physical and mental harm. Although previous research has not reached a consensus about whether older adults are more likely to become victims of Internet crime than members of other age groups, based on the current statistics, there seems to be a pattern indicating that the probability of older adults becoming Internet crime victims is higher than that of younger people. This may result from older users' lack of Internet knowledge and skills, cognitive decline, and loneliness, all of which are factors that attackers can leverage (Garg et al., 2011). Considering that online privacy and security risks can seriously impair healthy aging, protecting older adults from online threats becomes an urgent and critical mission.

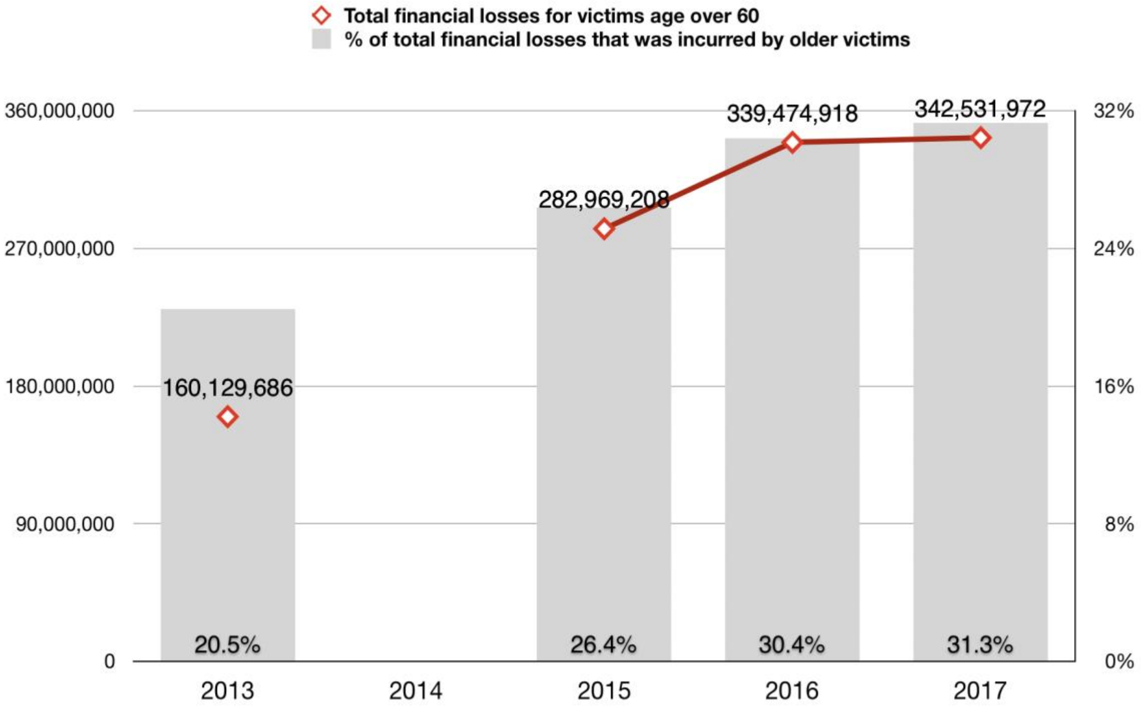


Figure 1.2: The percentage of the total financial losses reported by older adult victims has risen since 2013. Data from 2014 is missing from the report. (Data source: FBI IC3 reports from 2013 - 2017)

As mentioned above, online privacy is a critical aspect to consider when introducing Internet technologies to older adults. The pervasive data collection, sharing, and monitoring made possible by the Internet means that older adults' online activities can disclose not only information that they are aware of having shared, but also personal information they do not intend to disclose. For example, if older adults live in a smart home online environment, various types of personal information (e.g., daily routine, home address) can be collected and analyzed by malicious entities. Online privacy is a complicated and multilayered concept that requires multidisciplinary efforts from different professional domains (Solove, 2009; Nissenbaum, 2010). To protect users' online privacy, technologists, psychologists, legal scholars, and policymakers have collaborated and made efforts to incorporate privacy into the designs of technologies. A variety of privacy protection approaches have been developed, such as the Fair Information

Practices Principles (FIPPs) proposed by FTC, Privacy by Design (PbD) for system engineering (Langheinrich, 2001), and the framework of Do Not Track (DNT). From a technical perspective, one of the significant efforts is the development of Privacy-Enhancing Technologies (PETs) (Goldberg et al., 1997).

PETs are technical tools that can protect users' information privacy by minimizing online entities' possession of personal data, without losing the functionality of the system. PETs include a wide range of online applications, including anonymous web browsers, email/communication encryption, network anonymization, and password management. Although PETs protect users from online risks, the use of PETs usually requires a high level of proficiency with computer technologies, often proving to be too difficult and complicated (Wang, 2009; Fabian et al., 2010; Norcie et al., 2014) especially for novice users (Gallagher et al., 2017). When it comes to the older adult population, it becomes even more critical to design technology that is usable and easy to learn because of the decline in cognitive and physical ability that comes with natural aging. Although online PETs can be useful and practical tools for protecting older adults' online privacy, these tools may not have high usability and learnability, which can hinder the adoption of PETs by older adults.

As stated above, with an increasingly aging population and the growing usage of the Internet by older adults, it is imperative to empower older users with useful and user-friendly privacy-enhancing tools. In order to encourage and facilitate the use of PETs by older adults for their online activities, it is essential to understand both how older adults protect their online privacy and what they experience while using privacy-enhancing tools. However, to the best of my knowledge, very few empirical studies focus on older adults' use and adoption of online privacy-enhancing tools. There is a lack of comprehensive understanding regarding how older adults think, what they know, and how they behave regarding the privacy and security of their information while using the Internet. It also remains unclear whether or not the current design of privacy-enhancing tools is usable enough for older users to protect their online privacy. In this thesis, I have adopted an interdisciplinary approach and a variety of empirical methods to investigate these questions. In the next section, I will review the prior works and concepts that are most related to this research.

Chapter 2. Related Work and Concepts

When examining older adults' experience with online privacy-enhancing tools, additional aspects must be considered. The first consideration is that older adults' experiences using technology may be quite different from those of their younger counterparts due to natural changes in their physical or cognitive abilities. Therefore, it is important to understand what types of difficulties older adults may encounter when browsing on the web. In addition, while older adults can instantly access information of almost any kind (such as commercial and healthcare services) via the Internet, the pervasive online tracking mechanisms used by such sites pose threats to older adults' information privacy. As a result, it is essential to review what types of online privacy threats exist and understand what tools are available for protecting privacy. In this section, my review will focus on research related to three aspects, which are: 1) older adults as web users, 2) privacy threats to web browsing, and 3) tools for privacy-enhancing browsing.

2.1 When older adults become web users

Older adults, just like everyone else, would like to use the Internet to keep up-to-date on important issues announced by their government, to participate in education, and in some cases to contribute to the web via social media platforms. More and more older adults are using the Internet, which makes this group the fastest-growing population of Internet users (Kisekka et al., 2015). According to Pew Research (2018), 66% of people over age 65 use the Internet. The Internet enhances older adults' independence by providing them with access to a variety of online services and activities, such as communicating via email, connecting with family or friends on social media, online banking, online shopping, and searching for information (Vuori & Holmlund-Rytkönen, 2005; Wagner, Hassanein & Head, 2010). Although online activities have become an increasingly essential part of the lives of older adults, they still face certain difficulties and risks while using the Internet.

2.1.1 Consideration of the physical and cognitive challenges for older web users

When it comes to web browsing, older adults have concerns and needs different from those of younger adults due to the natural physical and cognitive changes that come with aging (Arch, 2009). The type and level of these changes have important effects on the web browsing experiences of older adults. As exhibited in Table 2.1, physical changes associated with aging include declines in vision, hearing, psychomotor coordination, and cognitive ability (Hawthorn, 2000; Arch, 2009). These normal age-related changes in visual perception, auditory perception, or motor skills may complicate web use, especially for poorly designed sites (Dickinson et al., 2007). Although many older adults experience no special difficulties while browsing the web, poorly designed sites or applications may discourage use by older adults, or make it impossible for them to do so (Dickinson et al., 2007). Therefore, in order to make the design of a web site more appropriate and usable for older adults, interfaces should use larger fonts, sounds within certain frequency ranges, and layouts that require less precise mouse movement (Fisk et al., 2009; Wagner, Hassanein & Head, 2010). Similarly, interfaces need to accommodate older web users' cognitive changes (such as declines in memory, reduced attention span, and changes in spatial abilities) by having fewer unnecessary distractions, providing memory cues, and being easy to learn and understand (Hawthorn, 2000; Fisk et al., 2009).

Table 2.1: Physical and cognitive changes with the aging process (Hawthorn, 2000; Arch, 2009)

Natural changes with aging	Signs	Affected aspect of web browsing
Vision decline	• Decreasing ability to focus on nearby tasks, including a computer screen and keyboard • Changing color perception and sensitivity, making it easier to see reds and yellows than blues and greens, and often making darker blues indistinguishable from black	Screen and keyboard use
Hearing decline	• An overall decline, but mainly an increasing inability to hear higher-pitched sounds	Audio and multimedia use
Psychomotor skill diminishment	• Slowness of movement • Joint stiffening • Trembling	Mouse and keyboard use
Cognitive decline	• Short term memory problems • Concentration difficulties • Distraction	Overall web use

In addition, differing levels of web experience must also be considered when it comes to understanding older adults' web browsing needs. While some older people are skillful at web browsing, many of them, especially old-older users, may spend less time online and have far less experience with web browsing than their younger counterparts. As a result, what younger adults take for granted can still be complicated and frustrating for older adults. While older adults may be increasingly familiar with the web, they may still find themselves perplexed as the interfaces change and evolve. Accordingly, it is necessary to consider the needs and preferences of older web users throughout the whole design process.

2.1.2 Privacy concerns and risks of older web users

Older web users are concerned about their online privacy. According to a survey (AARP, 2017), approximately 75% of older people expressed concerns about their online privacy, and 86% of them were concerned about their personal data being compromised. However, it remains unclear whether older adults exhibit higher levels of concern for their online privacy than younger adults, because while some studies found that older adults tend to have more privacy concerns (Zukowski & Brown, 2007; Blank, Bolsover, & Dubois, 2014; Miltgen & Peyrat-Guillard, 2014; van den Broeck, et al., 2015) some studies did not find a significant difference (Hoofnagle et al., 2010; Taddicken, 2014). One explanation for these differences is that privacy concerns are contextually dependent. Bergström (2015) found that older users are more concerned about the misuse of their financial information, whereas younger users are more worried about the misuse of their personal information on social networking sites.

Although older adults, in general, express concern about online privacy, they seem to take fewer online protections than their younger counterparts (Blank, Bolsover, & Dubois, 2014; Miltgen & Peyrat-Guillard, 2014; van den Broeck, et al., 2015). This contradiction between attitude and behavior may result from a lack of knowledge and skills pertaining to the Internet (Garg et al., 2011). Also, older adults may be more vulnerable to online attacks because they generally trust in online information more and perceive fewer potential privacy risks when compared with other age groups (Grimes et al., 2010). Finding ways to empower older web users to protect their online privacy is becoming an urgent need, as older people are using the internet in greater numbers.

2.2 Online privacy threats

Tracking technology used by web browsers poses various risks to individuals' online privacy. Next, I will review the online tracking mechanisms currently applied to web browsers by online services and then discuss the potential threats they pose to one's information privacy.

2.2.1 Online tracking mechanisms on web browsers

Online tracking mechanisms are used to identify or monitor users' web browsing behaviors across multiple websites (Krishnamurthy et al., 2007). The goal of online behavioral tracking is to create a profile of a user's online activities. When a user visits a web page, the content of the page can come from both a first party (the page that the user is intentionally visiting) and third parties (companies that are associated with the first party, allowing them to place content on that page). Third parties include analytic companies, advertising networks, and social networking sites that contract with first-party websites. Both first and third parties can place a unique identifier on a user's computer. Then, if the user visits different websites that contain content from the same third party, that third party can link these visits to the same computer. Currently, a small number of third parties have content on a large number of pages, allowing these third-party companies to track and profile users' web browsing activities (Krishnamurthy & Wills, 2009).

Online tracking can be accomplished in many technical ways via web browsers (Jackson et al., 2006). Table 2.2 exhibits different types of online tracking mechanisms proposed by Jackson et al. (2006). The most common approaches are using cookies[1] and tracking scripts[2]. Cookies allow users to visit the site again and have their profile re-used without them having to re-enter information (Krishnamurthy et al., 2007). Both first and third parties send cookies. A website can place a cookie with a unique identifier on a user's computer, and then track browsing activities via that unique identifier (Krishnamurthy & Wills, 2009). A tracking script is often a JavaScript file downloaded to a user's browser, which can then gain access to browser information, such as cached objects and the history of visited pages (Krishnamurthy & Wills, 2006). Then, the scripts can send information back to the tracking site via identifying URLs that are then used to pass information to the server (Krishnamurthy et al., 2007).

[1] Please see Appendix D for the definition of cookies.

[2] Please see Appendix D for the definition of tracking scripts.

Table 2.2: Online tracking mechanisms (Jackson et al., 2006)

Type of Tracking	Mechanism
Single-session tracking	Websites can embed query parameters in URLs to identify users as they click around the site and track them as they follow links to other cooperating sites.
Multiple-session tracking	A single website can identify a visitor over multiple visits.
Cooperative tracking	Multiple cooperating sites can build a history of a visitor's activities at all of those sites, even if the user visits each site separately. It allows the user's personal information at one site to be linked together with activities at a different site that appears to be unrelated.
Semi-cooperative, single-site tracking	A tracking site can determine information about a visitor's activities at another "target" site, by convincing the target site to embed content that points to the tracking site.
Semi-cooperative, multiple-site tracking	Similar to semi-cooperative, single-site tracking, except that the tracking site can follow users across multiple target sites.
Non-cooperative tracking	A tracking site can determine information about a visitor's activities at another target site without any participation from the target site.

Numerous unique tracking mechanisms have also been developed, such as browser fingerprinting, or using web bugs, Flash Local Shared Objects (LSOs), HTML5 local storage, and other methods to track users' browsing activities over time (Eckersley, 2010; Acar et al., 2014; Krishnamurthy & Wills, 2009; Mayer & Mitchell, 2012; Ur et al., 2012). Even though many of these techniques focus on linking browsing activities to a particular computer instead of to a user's real identity, it is still possible to distinguish between users even if multiple users are behind the same address by examining the access patterns over time, and the frequency and duration of access periods (Jackson et al., 2006; Krishnamurthy et al., 2007).

With cookies and the results obtained by executing scripts, the tracking site can gain information available in a user’s typical online request, such as the user's IP address, current and previously visited pages, email address, language preference, and so forth. Under certain circumstances, the information about a user’s search strings, passwords, and account numbers may also be available to the tracking sites (Krishnamurthy et al., 2007). Users’ information privacy can be under threat while browsing on the Internet.

2.2.2 Information privacy threats in web browsing

Users browse and share information online with the expectation that their information will not be shared with other sites. However, both first- and third-party websites can utilize online tracking mechanisms to monitor users' web browsing history, which can then be used to aggregate one’s sensitive personal information (SPI) and reveal their personally identifiable information (PII). Although web browsing is one of the most popular and ordinary online activities, it also poses a threat to users' information privacy.

a) Aggregating sensitive personal information

One's web browsing history can reveal personal information. For instance, the websites a user visits can disclose user’s location, purchases, employment, interests, sexual orientation, financial status, medical conditions, and more. By tracking and collecting users' browsing history, first and third parties can easily profile users and analyze the patterns of their online activities for more inferences (Mayer and Mitchell, 2012). Thus, it is possible for first and third parties to collect and expose SPI about users. A study by Mayer and Mitchell (2012) discovered that a third-party tracker publicly exposed users' SPI, such as whether or not they were going through menopause, getting pregnant, repairing bad credit, and seeking debt relief. They also found that a free online dating website sent information to a third-party data provider regarding how often its users drank, smoked and used drugs. Another research (Krishnamurthy et al., 2011) also found that third-party websites could learn and collect information from what users search on health websites. The collection of personal information via web browsing history can compromise users' personal privacy without their awareness.

b) Revealing personally identifiable information

Most web browsing happens in a pseudonymous mode. However, an individual's PII, such as their real name, birth date, and demographics can still be revealed by their web browsing history. Previous research has discovered five means by which a pseudonymous browsing history might become identifiable (Narayanan, 2011; Mayer and Mitchell, 2012). First is if the first-party website turns itself into a third party. For instance, Facebook requires users to provide their real name to the service. Then when a website includes a third-party Facebook social widget, Facebook can still identify users to personalize the widget even though users do not disclose who they are. Users' PII can also be sold by first-party websites to a third-party data company. Additionally, if a website puts PII in a URL or page title, it may accidentally leak the information to third parties (Krishnamurthy et al., 2011). The unauthorized third party may also exploit a cross-site security vulnerability on a first-party website in order to access the user's PII. Yet another approach is to re-identify users by matching their browsing history to identifiable datasets (Narayanan and Shmatikov, 2008). A third party, for example, may compare one's browsing activity to the times and locations of links publicly shared on social networking sites.

One approach to protecting users from these online privacy threats is the use of privacy-enhancing browsing tools. In the next section, I introduce two different types of tools that will be investigated in this study.

2.3 Privacy-enhancing browsing tools

Due to privacy concerns about behavioral profiling by online entities, people are increasingly seeking ways to protect their information privacy while browsing online. As a result, researchers have been dedicated to developing a variety of Privacy-Enhancing Technologies (PETs) to protect users' information privacy. In terms of web browsing, privacy-enhancing mechanisms can be applied at a browser or proxy[3] level. Browser-Based Protection (BBP) approach focuses on disabling tracking mechanisms (e.g., cookies, JavaScript execution, third parties' contents etc.) and using plug-in applications to filter or block advertising (Krishnamurthy et al., 2007). Most modern browsers allow users to enable BBP by adjusting a built-in privacy setting or using a private browsing mode. Another privacy-enhancing mechanism for web browsing is to use a Proxy-Based Protection (PBP) approach. The PBP approach allows users to access web pages via a proxy server without revealing their IP address, and also protects users from malicious traffic attacks. There are various types of PBP approaches and a virtual private network (VPN) is one of the most frequently used. Another popular PBP approach is the employment of an anonymous proxy network, such as Tor, which can hide the source of requests and make online tracking or surveillance more difficult. To have more users take advantage of privacy-enhancing browsing, technologists have combined these approaches into their browser designs. Two of the most-used cases of this are reviewed in this thesis, including 1) private browsing mode, and 2) anonymous browsers.

[3] Please see the explanation of "proxy" in Appendix D.

2.3.1 Private browsing mode

A private browsing mode has been offered as a built-in function in most of today's leading browsers, including Google Chrome, Mozilla Firefox, Apple's Safari and Microsoft Edge/IE. The goal of private browsing mode is to prevent one's browsing history and personal information from being accessed by either local adversaries or tracking sites (Liou et al., 2016). Although most leading browsers provide similar features in private browsing mode, the interface design and privacy functionality still vary among these browsers.

a) Functionalities of private browsing mode

Previous studies of private browsing modes have focused on inspecting their functionality as pertaining to security and privacy or examining the detailed features of private browsing modes on different browsers (Gao et al., 2014). Aggarwal et al. (2010) conducted the earliest research on private browsing modes. They analyzed private browsing modes from four popular web browsers (Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft IE) and found that web extensions can compromise private browsing. Satvat et al. (2013) further examined the detailed threat model in private browsing model of these four browsers. They reported vulnerabilities of private browsing in all four browsers and stressed the necessity of improving security for private browsing mode. Satvat et al. (2014) further examined technical details for attacks on private browsing. Based on the responses of browser providers, they re-examined the attacks against the newest versions of the browsers' private browsing modes and refined their suggestions for countermeasures. Other studies also revealed the vulnerabilities of private browsing modes. Said et al. (2011) found that traces left in the physical memory (RAM) by private browsing can be used to restore a part of the browsing history. Liou et al. (2016) conducted a case study and found that users' private information can be retrieved from private browsing mode. The level of vulnerability of privacy and security while in private browsing mode varied by browser (Ohana & Shashidhar, 2013). Lerner et al. (2013) studied how browser extensions were violating private browsing by analyzing JavaScript extensions, and notifying users via a small annotation. The studies mentioned earlier prominently contributed to analyzing the functionalities and vulnerabilities of private browsing modes on different web browsers. However, these studies focused on the technical aspects of private browsing instead of human aspects, such as how people perceive and understand private browsing modes.

b) Users' perceptions of and behaviors toward private browsing mode

How users perceive and understand a tool can affect their adoption and usage of the tool. Previous research on tools for privacy and security found that users' misconceptions and inaccurate mental models can decrease the effectiveness of these privacy-enhancing tools. For instance, Bravo-Lillo et al. (2011) investigated how users perceived and responded to computer warnings and found that users frequently ignored the warnings due to a lack of understanding of their meaning. Chiasson et al. (2006) conducted a usability study of two security programs, and they discovered that users have inaccurate mental models of the different kinds of security software, and as a result are reluctant to use them. Another study by Ha et al. (2006) used a focus group to study users' awareness of web cookies, and found that most users were confused by their benefits and disadvantages. Friedman et al. (2002) conducted an interview about users' conceptions of web security, and the results showed that many users were unable to correctly identify whether their Internet connection was secure or not. Wash (2010) identified eight folk models of security threats used by home computer users and how these models are used to decide which security software to use while browsing online. In addition, the interface design and usability of privacy-enhancing tools can affect users' understandings of the tool. Leon et al. (2012) conducted a usability study on tools employed to limit online behavioral advertising and found that users were unable to understand the tools' meanings and functions. Without an accurate understanding of the tools, users cannot operate them appropriately.

When it comes to private browsing mode, only four studies have examined users' perceptions and behaviors. A study by Soghoian (2010) pointed out that people primarily use private browsing to protect themselves from local adversaries, and pay less attention to online tracking by third parties. People thus tend to ignore browser warnings about the limitations private browsing modes while using them. This phenomenon can be explained by users' misconceptions about private browsing modes. Gao et al. (2014) conducted a survey study to probe users' understandings of private browsing. They found that many users incorrectly believed that private browsing mode can provide them with full online anonymity and protect them from malicious privacy attacks. These false mental models and misconceptions regarding private browsing modes may lead users to perform activities with high privacy risks.

To prevent user misconceptions of private browsing modes, a recent study tested 13 different browsers explanations of their private browsing modes (Wu et al., 2018). They found that browsers' disclosures fail to correct users' misconceptions, such as the false belief that private browsing mode would protect them from geolocation, advertisements, viruses, and online tracking. Moreover, their results found that certain disclosures were likely to lead users to have misconceptions about private browsing. That is, the current browsers' disclosures and explanations are insufficient in changing users' false beliefs regarding private browsing modes.

Another study conducted by Habib et al. (2018) examined users' private browsing behaviors by using software to monitor their daily usage. They found that users make use of private browsing to protect not only their privacy, but their security as well. Similar to previous studies, their findings also suggest that while private browsing decreases users' privacy and security concerns, users also overvalue its protection from online tracking and behavioral advertising.

2.3.2 Anonymous browsers

Anonymous browsers incorporate both browser-based and proxy-based protection approaches, thus providing a higher level of network privacy compared to the private browsing mode on leading browsers. One of the most popular anonymous browsers is Tor Browser, a modified Firefox browser that encompasses a built-in Tor network.

Tor is an acronym for The Onion Router, a network that enables online users to browse the internet anonymously. Tor is currently in use worldwide. Based on estimates by the Tor Project (Tor Metrics, 2018), Tor has around 2 million unique global daily users. Applying the concept of onion routing (Goldschlag et al., 1996), Tor network routes traffic via three-layered volunteer-run nodes, including the guard node, the middle node, and the exit nodes. Each node only knows the identities of the previous sender and the next receiver. Hence, no node knows both what the message is, and where it was sent from and to whom it is going. Then, the exit node delivers the messages to the destination in plain text. Furthermore, with the support of Onion Services, a server and a client can contact each other via the Tor network without knowing one other's IP addresses.

One simple way to use Tor is through Tor Browser (Perry et al., 2018), a modified Firefox browser with a built-in Tor network. In Tor Browser, there is a functionality called Tor Launcher, which configures and controls the operation of Tor. Tor Launcher provides a graphical user interface that allows users to select whether or not to configure a proxy and bridge before connecting to Tor. Additionally, users' browsing behaviors on the Tor Browser are augmented through the Tor button extension, which shows users their routing path on Tor for each web page. Tor browser also protects users from potential eavesdropping by malicious exit nodes by automatically including the HTTPS Everywhere, which encrypts users' traffics, and NoScript, which prevents Cross-Site Scripting (XSS) attacks (which allows an attacker to steal users' authentication credentials by adding malicious code from a specific site into a different site).

Overall, the Tor Browser provides the highest available level of online anonymity to protect users' privacy and security. Nevertheless, the use of Tor Browser requires that users be knowledgeable about certain technical concepts, such as bridges, proxies and traffics routing, which can be difficult for older users to use. In this research, I will conduct a user study to evaluate the usability of Tor Browser from older users' perspective.

Chapter 3. Research Framework and Overview

More and more older adults are encouraged to use the Internet and become online users. However, pervasive and continuous online tracking poses a threat to older adults' information privacy. There is an urgent need to empower older adults with privacy-enhancing browsing tools so that they can actively protect their information privacy while browsing online. As mentioned in the previous section, these two types of privacy-enhancing browsing tools are used the most: the private browsing mode built into the leading browsers, and anonymous browsers. The purpose of this study is to investigate older adults' experiences with these two Privacy-enhancing Browsing Tools (PeBTs).

From the perspective of older users, the biggest challenges in adopting today's privacy-enhancing tools are their complex designs and lack of usability (Fabian et al., 2010). Most users will not utilize a browser with poor usability even when it offers the highest level of privacy protection. More importantly, the complicated designs of these tools may result in greater risk or harm to users' information privacy. For example, previous research has pointed out that users in general lack understanding of and have misconceptions about private browsing mode, which leads to them doing activities with high privacy risks. When it comes to the use of technologies, older adult users may encounter more difficulties and be more confused than their younger peers due to changes that come with the natural aging processes (Hawthorn, 2000; Rogers & Fisk, 2010). Therefore, making PeBTs more learnable and usable is critical, especially for older adults' adoption of them.

Designing technologies for older adults is a multifaceted process that requires interdisciplinary approaches in order to understand what older adults need, identify their capabilities and limitations, and reveal their preferences for the designs of tools (Lindsay et al., 2012). As a result, a research framework with an interdisciplinary perspective is proposed for this research project. As presented in Figure 3.1, the framework encompasses three dimensions, including information privacy, psychological states, and design of PeBTs.

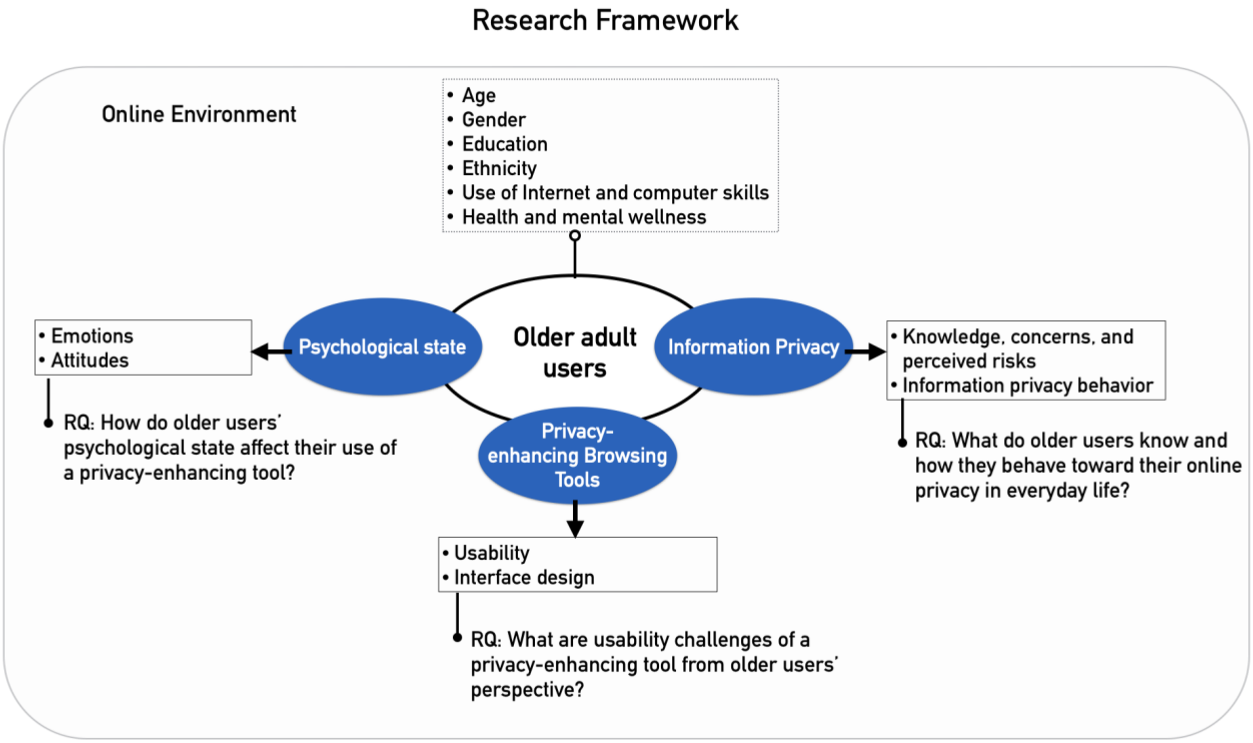

Research Framework
Online Environment
• Age
• Gender
• Education
• Ethnicity
• Use of Internet and computer skills
• Health and mental wellness
Older adult users
Psychological state
Information Privacy
Privacy-enhancing Browsing Tools
• Emotions
• Attitudes
RQ: How do older users' psychological state affect their use of a privacy-enhancing tool?
• Knowledge, concerns, and perceived risks
• Information privacy behavior
RQ: What do older users know and how they behave toward their online privacy in everyday life?
• Usability
• Interface design
RQ: What are usability challenges of a privacy-enhancing tool from older users' perspective?

Figure 3.1: Research framework for older users' experience with online privacy-enhancing browsing tools

Based on the framework, three research aspects will be assessed and integrated throughout this thesis.

1) **Understanding older adults' experience with, knowledge of, and behavior regarding information privacy and the use of privacy-enhancing browsing tools**: From an information privacy perspective, older adults' experiences, knowledge, and skills can influence both their ability to control and what they perceive as risk for information privacy breaches. When it comes to technology, older adults seem to be willing to give up their privacy in exchange for independence, although privacy still concerns them (Fisk et al., 2009). On the other hand, once they experience an incident with privacy or security, they may

refuse to use the technology or other new technologies because of fear or uncertainty resulting from the lack of knowledge. Thus, understanding both what older adults know and experience with regards to their information privacy and PeBTs and how they act online is important, in order for us to recognize what makes older adults vulnerable in an online environment.

2) **Assessing how the use of privacy-enhancing browsing tools influences the psychological state of older adults':** From a psychological perspective, older adults will naturally experience a decline in their body sensations, motor skills, and cognitive abilities (Hawthorn, 2000; Arch, 2009; Fisk et al., 2009; Wagner, Hassanein and Head, 2010), which can further affect their perceptions and behaviors regarding their information privacy and their use of online tools. Since the psychological state of older adults impacts their perceptions and behaviors, it is important to examine how psychological factors, such as attitudes, memories, and mental model, influence older adults' perceptions and behaviors pertaining to both online risks and their willingness to learn and adopt privacy-enhancing tools. In addition, personal characteristics, such personality traits and trust disposition, will also be investigated. By understanding the effects of the psychological state on online risk perception and technology adoption, we may discover individual patterns among older adults, which can help us to tailor their online experience based on their preferences.

3) **Testing the usability of a current privacy-enhancing browsing tool**: When it comes to PeBTs, whether older adults think a tool is learnable, usable, and useful becomes a critical factor in their adoptions. Since many privacy and security incidents occur during web browsing (e.g., phishing attack and advertising scams), this thesis research focuses on testing two privacy-enhancing tools for web browsers. The first tool is the built-in private browsing mode on the leading browsers. The second is the anonymous browser. We will test these two tools with older adults and investigate the usability issues and their acceptance of tools.

To the best of my knowledge, there are no empirical studies focusing on older adults' usage and adoption of PeBTs. Although previous studies have examined users' mental models of PeBTs, what the usability problems of PeBTs are, and what the solutions to these problems might be, none of them examine their design issues from older adults' perspective. We still have a lot to learn about how older adults think, what they know, and how they act in regard to their information privacy while browsing online. It also remains unclear whether the current design of PeBTs is usable and/or useful for older adults for protecting their information privacy. Given that older adults' use and adoption of technology involves various factors (Fisk et al., 2009; Park et al., 2010, Kim et al., 2016; Renaud, 2008), an interdisciplinary approach is essential. Therefore, the aims of this research project are to answer the following research questions from an interdisciplinary perspective, including the fields of psychology, technology, and information privacy:

- RQ: What do older users know and how do they behave toward their online privacy in everyday life?
- RQ: How do older users' psychological state (e.g., emotions, attitudes) affect their behavioral intentions toward using a privacy-enhancing browsing tool?
- RQ: What are the usability challenges and problems of a privacy-enhancing tool from the perspective of older users?

In summary, the primary objective of this research is to gain an understanding of older adults' user experiences with PeBTs, and to advance the design of current tools for older adults. This research includes three projects. In the first study, older adults' knowledge, experiences, and behaviors regarding online privacy and security will be examined through online and offline surveys. In the second study I will investigate how older adults' psychological state (e.g., their attitudes and emotions) affect their behavioral intentions toward using a built-in private browsing feature, via an online quasi-experiment. Then, in the third study I will evaluate the usability aspects of a privacy-enhancing browser, Tor

Browser, from the perspective of older users by performing a user study. Table 3.1 provides an overview of research questions and related chapters.

Table 3.1: Overview of research questions and chapters

#	Research questions / goals	Chapter	Method
Study 1	What do older users know and how do they behave toward their online information privacy?	4	Survey
Study 2	How do older users' psychological state (e.g., emotions, attitudes) affect their behavioral intention to use a privacy-enhancing browsing tool?	5	Quasi-experiment
Study 3	What are usability challenges and problems of a privacy-enhancing browsing tool from older users' perspective?	6	Usability testing

Chapter 4. Older Users' Online Privacy Protection Behavior and Knowledge[4]

4.1 Introduction

The world population is increasing at an exponential rate. By 2050, the global population of older adults is expected to reach nearly 2.1 billion, which is double the number of older adults in 2017 (United Nations, 2017). The rapid growth of the aging population presents both opportunities and challenges for nearly all aspects of society, such as social support, economic, and healthcare systems. The current and future advancement of Internet technologies will soon connect almost every device in our daily lives, from smart homes to self-driving cars. Therefore, supporting older adults in the use of Internet technologies is increasingly important.

Many people may assume that older adults tend to avoid adopting Internet technologies. In fact, the percentage of older Internet users has been rapidly growing over the past decade. A survey by Pew Research Center reports that in 2016, 64% of U.S. older adults are Internet users, an approximately 50% increase compared to 2001 (Pew, 2017). In addition, studies have shown that frequent use of Internet technologies among older adults has been associated with their broader social networks, independent lifestyle, and wellbeing (Wagner, Hassanein and Head, 2010; Choi and DiNitto, 2013; Hills et al., 2015). For instance, when using the Internet, older adults can communicate with others through social media; they can keep learning and educating themselves via online courses; and they can increase social connections by engaging in online communities (Choi and DiNitto, 2013). Therefore, Internet technologies are not only a significant source of support for healthy aging among older adults but also offers new opportunities for geriatric care in countries with increasing numbers of older citizens.

[4] This chapter is adopted from a published paper: "Huang, H. Y., & Bashir, M. (2018, Nov). Surfing Safely: Examining Older Adults' Online Privacy Protection Behavior. In Annual Meeting of Association Information Science & Technology (ASIS&T), Vancouver, 2018."

The convenience provided by Internet technologies, however, is a double-edged sword because its pervasive and continuous data practices come with risks for information privacy and security, especially for older adults. According to the Internet Crime Report in 2016 (IC3, 2016), around 20.6% of Internet crime victims are aged over 60, and their financial losses account for 339 million of dollars in losses, which is the highest among all age groups. In addition, online privacy and security incidents can have disastrous impacts on older adults' physical and mental health. For instance, the manipulation of medical services could negatively influence their physical health, or a privacy breach could induce psychological distress. Consequently, protecting older adults' online information privacy is critical while developing technologies.

The pervasive and continuous data collection, sharing, and monitoring that occurs on the Internet means that older adults' online activities not only disclose information they are aware of having shared, but also personal information they do not intend to disclose. Since privacy is a complex and multilayered concept (Solove, 2008; Nissenbaum, 2009), technologists, psychologists, and legal scholars have used a variety of strategies to incorporate privacy into the design of socio-technical systems. For example, privacy protection guidelines and approaches have been developed, such as the Fair Information Practices Principles (FIPPs), Privacy by Design (PbD) (Langheinrich, 2001), the Do Not Track (DNT) policy and Privacy-Enhancing Technologies (PETs) (Goldberg et al., 1997).

In order to protect and enhance older adults' online information privacy, it is important to understand what older adults know about existing tools and how they behave online to protect their information privacy. Most studies have examined the influence of older adults' privacy attitudes and perceptions on their technology adoption. Yet, very few empirical studies have focused on older adults' actual behavior in protecting online information privacy. Furthermore, it still remains unclear whether cognitive factors, such as older adults' concerns, knowledge, and perceived risks impact their protective behaviors for online information privacy. Accordingly, the aim of this exploratory study is to investigate how older adults protect their online information privacy and the cognitive impacts on their behaviors. In next section, we review prior literature related to this study.

4.1.1 Prior literature in older users and online privacy

Several empirical studies have focused on how older adults' privacy perceptions and attitudes influence their acceptance and adoption of emerging technologies, such as online social networking sites (McNeill et al., 2017; Chakraborty et al., 2013), health monitoring systems (Caine et al., 2006; Wild et al., 2008; Demiris et al., 2009; Lorenzen-Huber et al., 2011; McNeill et al., 2017; Boise et al, 2013), and robotic technologies (Kahn et al., 2007; Caine et al., 2012). In this section we review prior work on older adults' perceptions, behaviors, and potential cognitive impacts on their online privacy.

4.1.1.1 Older adults' online information privacy perceptions

Previous research has found that older adults have a more specific definition of "information privacy" than younger adults (Kwasny et al, 2008). For instance, older adults tend to define information privacy in terms of specific information categories, such as legal documents, health information, social security numbers, or a secret that a friend discloses to them, while younger adults have broader definitions of information privacy (Kwasny et al., 2008). When it comes to information privacy, older adults do show concerns about their information privacy while connected to the Internet (Hoofnagle et al., 2010). For example, a survey study conducted by Hoofnagle et al. (2010) indicates that older adults expressed more concerns about Internet privacy issues than their younger counterparts. A recent study (Walters, 2017) also indicates that approximately 75% of older people expressed concerns about their online privacy and 86% of them were concerned about their personal data being compromised. In addition, it is important to note that each older adult's privacy concerns may be influenced by their mental and physical wellbeing. For example, a survey experiment by Caine et al. (2006) revealed that older adults with lower mental functioning express lower levels of privacy concerns.

Therefore, considering the impacts of cognitive factors on older adults' privacy perceptions and behaviors is essential.

4.1.1.2 Older adults' online privacy behaviors

When examining privacy behaviors in the literature, the majority of studies do not clearly distinguish between actual behavior and intended behavior. Nevertheless, privacy behavioral intentions do not necessarily lead to actual privacy protection behaviors (Kokolakis, 2017). In this study, we focus on older adults' actual privacy protection behaviors instead of behavioral intentions. As far as we know, very few empirical studies have investigated older adults' actual online privacy behaviors. The most relevant work is an observational study by Chakraborty et al. (2013). Chakraborty et al. (2013) analyzed 134 profiles of older adults on Facebook and observed their privacy-preserving actions. They found that older adults are more inclined to not sharing personal information if their friends did the same. In other words, older adults' decisions in taking privacy-preserving action can be affected by their social peers. Caine et al. (2012) investigated whether older adults engage in privacy-enhancing behaviors while interacting with monitoring devices. Their study suggests that older adults engage in more privacy-enhancing behaviors while being monitored by camera rather than when interacting with embodied robots. One potential explanation is that older adults may not be familiar with robots and, therefore, may be less cautious about their monitoring capabilities (Caine et al., 2012). This suggests that older adults' mental models of a technology impact their privacy behaviors.

4.1.1.3 Cognitive impact in older adults' online privacy

In reviewing privacy literature for all age groups, researchers have found that while users are highly concerned about their information privacy, they are still willing to disclose a substantial amount of personal information online (Kokolakis, 2017). This dichotomy of attitudes and behaviors in information privacy has been termed the "privacy paradox" (Norberg et al., 2007). Prior research has also indicated this paradoxical phenomenon in older adults' online information privacy. For instance, older adults make less online privacy protections than their younger counterparts, though they express higher levels of information privacy concern (Grimes et al., 2010; Miltgen et al., 2014; Blank et al., 2014). In addition, older adults seem to be willing to give up their personal privacy to maintain their independence and autonomy while adopting new technologies (Fisk et al., 2009). One possible explanation for these contradictions in privacy attitudes and behaviors in older adults may be related to cognitive factors, such as limited knowledge and mental models about online environments and current data practices (Garg et al., 2011; Lorenzen-Huber et al., 2011). Also, older adults perceive fewer privacy risks in online activities; therefore, they are more vulnerable to online privacy violation (Grimes et al., 2010). In other words, whether older adults take actions to protect their information privacy depends heavily on cognitive factors, such as concerns, knowledge, and, perceived risks.

In summary, previous research findings regarding older adults' online information privacy has pointed out the following:

- Older adults are equally as concerned about their information privacy as younger adults;
- Older adults seem to engage less in online privacy protection behaviors;
- Cognitive factors, such as concerns, knowledge, and perceived risks, can impact older adults' privacy protection behaviors.

However, we still have very little knowledge about what older adults do to protect their online information privacy, and how older adults' cognitive factors affect their privacy protection behaviors. Hence, this exploratory study aims to answer the following research questions:

- RQ1: What do older adults do to protect their online information privacy?
- RQ2: How do older adults' concerns, knowledge, and perceived risks regarding online information privacy impact their privacy protection behaviors?

4.2 Method

In this study, a survey methodology was adopted to investigate older adults' online privacy protection behaviors and how their concerns, knowledge, and perceived risks toward online information privacy impact their behaviors. In the following sections, we will refer to "Online Information Privacy" as "OIP".

4.2.1 Survey recruitment and procedure

According to the definition from the World Health Organization (2012), older adults in the developed countries represents people who are 65 years old and above. However, previous studies have found that including "pre-older adults" who are aged between 55 and 64 years old can be beneficial because this age range is when older adults start the transitioning phase into older adults (Bures, 1997; Li et al., 2016). It is during this phase, when adults' cognitive functions may start to decline gradually (Brown et al., 2017); yet, at the same time, the majority of them are still in the workforce and have opportunities to learn new technologies. Considering that the development of cognition is a continuous and evolving process across lifespan (Fisher et al., 2019), pre-older adults' use of technologies can also provide more cohesive and deeper understandings about older users' needs. In addition, previous research has also suggested that older adults' Internet usage is influenced by age-related change in interpersonal and functional factors (Friemel, 2016). As the first study examining older users' actual online privacy behaviors, it is beneficial to include both pre-older adult and older adult participants so that we can compare if there is any difference or similarity in terms of online privacy protection behaviors during these two stages of development. For example, most pre-older adults who are between 55-64 years old are still in the workforce, which may have them more familiar with Internet technologies. I postulate that participants between 55-64 years old may have different online privacy protection behaviors than those who are over 65 years old. Thus, both older adult participants (aged 65 and older) and pre-older adult participants (aged 55 to 64) were recruited in this study.

In addition, prior to conducting the large survey, I did two pilot studies to test the survey questionnaire with twelve older participants. Since the dataset was collected through the same assisted living facility, the results of pilot studies reveal homogeneity among participants' responses. To minimize the homogeneity bias, I decided to recruit participants via different venues. The survey was distributed via both online (n=125) and offline (n=44) venues. For the online survey, participants were recruited via a crowdsourcing platform, Amazon Mechanical Turk, and online mailing lists. Participants could access the online survey page via the recruitment post on the crowdsourcing platform or emails. For the offline survey, we used a snowballing approach and flyers to recruit participants from local communities, such as senior centers, local communities. After completing the survey, participants were given an educational handout about how to protect their online privacy and security. For compensation, participants recruited from the crowdsourcing platform were paid $1.75 for their participation, and other participants could select if they would like to participate in the lottery for a $25 gift card, which was given for every 25 participants. All participants were from the United States. Table 4.1 gives demographic information about our participants.

Table 4.1: Main characteristics of participants

Age	Pre-older adults (55-64)	66 (39.1%)
	Older adults (>=65)	103 (60.9%)
Gender	Female	103 (60.9%)
	Male	66 (39.1%)
Education	Some high school	1 (0.6%)
	High school	16 (9.5%)
	Some college	42 (24.9%)
	Associate's degree	22 (13%)

Table 4.1 (cont.)

Education	Bachelor's degree	39 (23.1%)
	Graduate or Professional degree	36 (21.3%)
	Doctoral degree	13 (7.7%)
Internet use	Several times a day	157 (92.9%)
	About once a day	7 (4.1%)
	A few times a week	2 (1.2%)
	About once a week	1 (0.6%)
	About once a month	1 (0.6%)
	Just a few times a year	1 (0.6%)
Living alone or with others	Living alone	60 (35.5%)
	Living with significant others	67 (39.6%)
	Living with family members	34 (20.1%
	Living with non-family members	3 (1.8%)
	Other	4 (2.4%)

4.2.2 Measurement

The survey questionnaire includes 3 segments. In the first segment, participants were first asked about their use of the Internet. Then they were asked about their perceived risks of online activities, online privacy concerns, awareness of online privacy and security, as well as their privacy protection behaviors. In the final segment, participants were asked to provide demographic information, such as their gender, age, educational level, and living alone or with others.

4.2.2.1 Online privacy protection behavior

The main goal of this study is to understand older adults' privacy protection behaviors while browsing online. Considering that the privacy-protective behaviors encompass with the various social and technical skills (Turkle, 1995; Park et al., 2012), we categorized privacy protection behaviors into 3 levels: passive, active, and proactive. The definition and measurement for each protection behavior are described below.

- *Passive protection behavior* is defined as 'using avoidant or social approaches to passively protect one's OIP', such as not registering to or purchasing on a website if users have privacy concerns about it. Eight items were adopted from Park et al. (2012) to measure older adults' protection behavior.

- *Active protection behavior* is defined as 'using functioning approaches to actively protect one's OIP', such as clearing browsing history, and removing cookies. Four items were adopted from Park et al. (2012) and used to measure active protection behaviors.

- *Proactive privacy protection* is defined as 'using advanced technical approaches, such as privacy-enhancing technologies to proactively protect one's OIP'. We select 9 types of online privacy-enhancing technologies that are popular and listed by Electronic Privacy Information Center.

Participants were asked to indicate if they have taken any of these approaches to protect their online privacy in the past. More details of the results of each privacy protection behavior are presented in Table 2.

4.2.2.2 Knowledge of online information privacy

As indicated by Park (2013), knowledge of OIP can be operationalized as user awareness in two aspects: (a) technical understanding and (b) awareness of data practices. In this study, we adopted 11 true-false items to measure for technical understanding and 8 true-false knowledge items for data practices awareness from Park (2013). The answers were later recoded as “1” for correct answers and “0” assigned to all other responses. Each aspect of user knowledge was combined to create an index. The Cronbach’s alpha of knowledge is 0.82.

4.2.2.3 Concerns of online information privacy

Considering that concerns about OIP include multiple aspects, we measured users’ privacy concerns about the use of online personal information and online data practices. For concerns about personal information, we adopted 6 items from Angulo and Ortlieb (2014) and asked participants to rate on a 5-point scale (from “Strongly disagree” to “Strongly agree”). The Cronbach’s alpha of privacy concerns of personal information is 0.82. For concerns about online data practices, we adopted 9 items from Angulo and Ortlieb (2014) and Buchanan et al. (2007) and asked participants to rate how worried they are about each statement on a 5-point scale. The Cronbach’s alpha of privacy concerns of data practices is 0.83.

4.2.2.4 Perceived risk of online activities

To measure perceived risk of online activities, we generated 25 types of online activities based on Pew Research Center’s report in 2010 (Pew, 2010). Participants were asked to rate how risky each online activity is on a 5-point scale. The Cronbach’s alpha of perceived risk is 0.94.

4.3 Results

4.3.1 RQ1: What do older adults do to protect their online information privacy?

Our first research question is how older people protect their OIP when they are concerned about it. We categorized privacy protection behaviors into 3 categories, including passive, active, and proactive behaviors. The Pearson Chi-square test was conducted to test whether the proportion of protective behaviors is the same for each type of privacy protection. As shown in Figure 4.1~4.3, the proportion of protective behaviors has significant differences in passive (X^2 =245.26, df = 8, p< .0001), active (X^2 =176.4, df = 3, p< .0001), and proactive (X^2 =308.5 df = 7, p< .0001) privacy protection. These results indicate that, for each type of privacy protection, participants reported to use certain approaches more than others.

For example, in terms of passive privacy protection, over half of participants reported that they had stopped visiting the websites, not registered, not purchased, asked online services to remove or not share personal information, and used secondary email(s). In addition, less than 50% of participants gave false personal information to websites, and/or made complaints to consumer or government agencies. For active privacy protection, over 65% of participants reported having experiences in clearing their browsing history, using tools to block unwanted emails, and/or clearing cookies. On the other hand, only about 25% of participants had experience in installing software to hide their computer identities from online services.

When it comes to proactive approaches, over 90% of participants did not have experiences in using an anonymous browser, a third-party blocking plugin, an https-enforcement plugin, an anonymous search engine, email encryption, or disconnecting social media tracking plugins. Furthermore, only about 30 to 40% of participants have used an ad-blocking plugin, cookies/Cache/Online history cleaners, and online tracker management. Overall, most participants had experiences in taking passive or active approaches to protect their online privacy. However, most older adults have no experiences in proactive privacy protection.

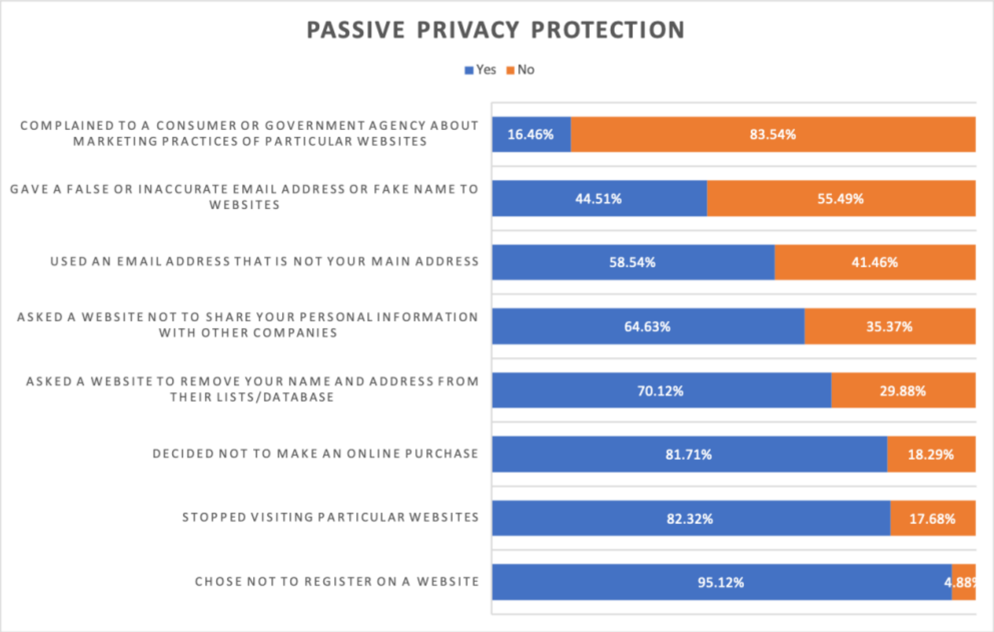


Figure 4.1: Distribution of passive privacy protection

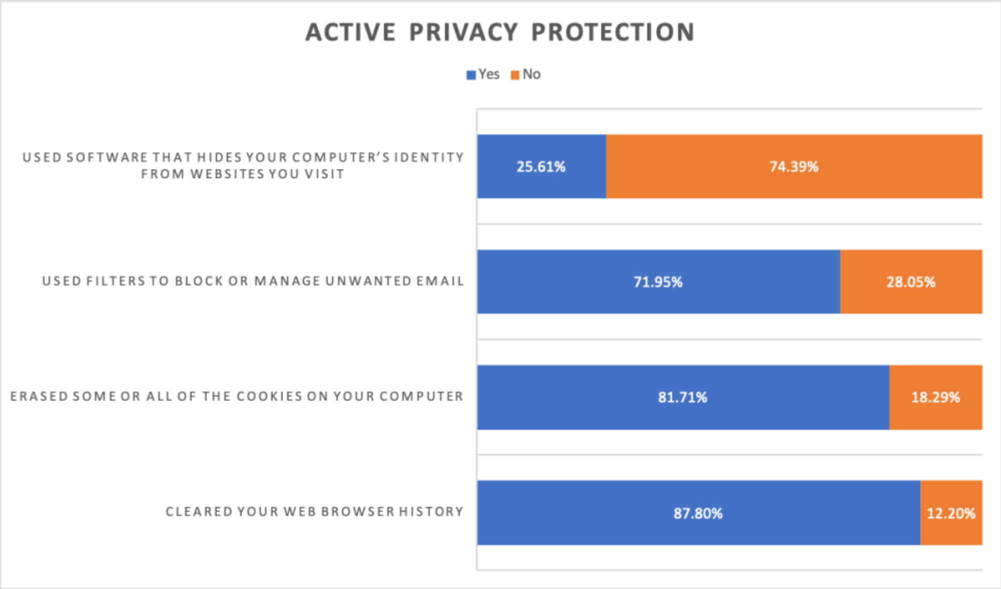


Figure 4.2: Distribution of active privacy protection

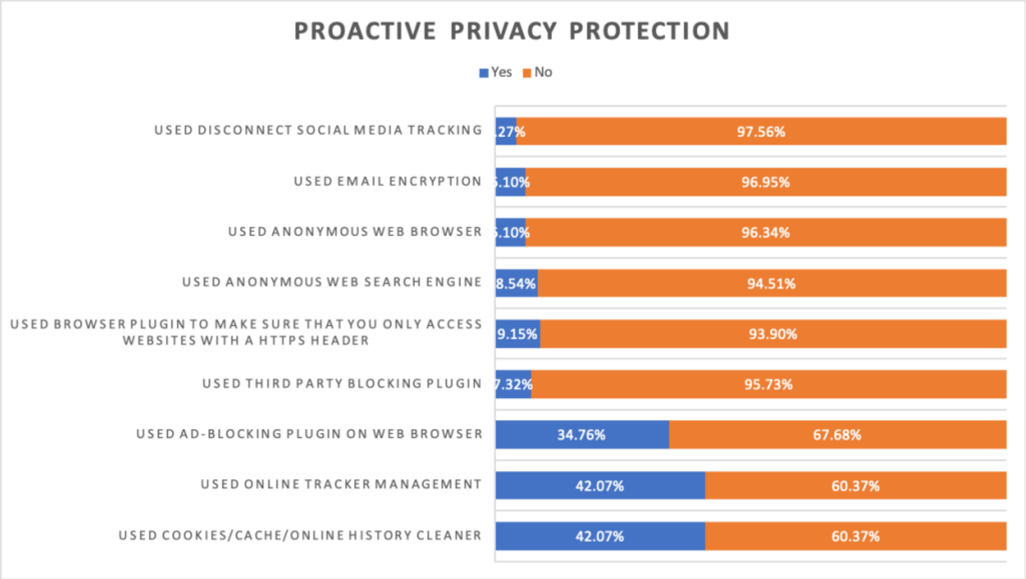


Figure 4.3: Distribution of proactive privacy protection

4.3.1.1 Categorization of online privacy protection behaviors by multiple correspondence analysis

We further explore the pattern of who takes what type of privacy protection. Since older adults are a diverse population, we think that age and familiarity with the Internet may affect how older adults approach their OIP. For instance, we postulate that participants recruited from the crowdsourcing platform may be more familiar with the Internet than those whom are not. Therefore, we categorized our participants based on their age and the medium of recruitment, which results in four groups: (1) aged 55-64; (2) aged 65 and older; (3) crowdsourcing (mTurk); and (4) general public (non-mTurk). To explore the relationship among categorical variables of privacy protections and demographics, we conducted Multiple Correspondence Analysis (MCA) by using R package FactoMineR.

MCA is a statistical technique to analyze the pattern of relationships between multiple categorical variables (Abdi & Valentin, 2007). More specifically, MCA model analyses associations between the frequencies of binary categorical variables and spatially projects the positions of variables in two dimensions. Therefore, MCA is a convenient tool for visualizing the associations between multiple categorical variables (Sourial et al., 2013). Considering that all of our variables were coded as binary variables, MCA is an adequate technique to explore the relationship between privacy protection and the population. Furthermore, MCA can add supplementary variables to the visualization without interfering the primary analysis (Sourial et al., 2013; Clausen, 1998).

In MCA, supplementary variables are projected onto the dimensions after the original analysis of the variables of interest is implemented. In this technique, supplementary variables do not affect the original results, but their position on the graph still allows us to see how the primary variables of interest are associated with supplementary variables. In our research context, the primary variables of interest are privacy protection approaches and the supplementary variables are age group and recruitment type. Next, MCA models for each type of privacy protection with supplementary variables will be presented individually.

1) MCA of Passive Privacy Protection

According to our analysis, the two-dimensional solution accounts for 71% of the total inertia, which provides sufficient explanation for the model of passive privacy protection. In addition, Dimension 1 explains the most variance in the model (57.6%), followed by Dimension 2 (13.4%). Table 3 shows the summary of the model. Figure 1 shows the symmetric map of two-dimensional solution.

As shown in Figure 1, five passive approaches were close to each other, including: stopping visiting websites, not purchasing, not registering, use secondary email, and give false information. Considering the avoidant nature of these approaches, we categorized these behaviors as ‘Avoidant strategies’. In addition, participants who had experiences in asking websites to remove personal information and asking websites not to share their information were also inclined to take action in filing complains to authorities as they had privacy concerns. We characterized these two approaches as ‘Expression strategies’. It is worth noting that the squared correlation (COS²) of complaining to authorities is relatively low (Table 4.2). This suggests that this approach is not an appropriate indicator to represent how older people protect their online privacy.

Furthermore, based on the location of two supplementary variables (age and recruitment), two clusters emerge on the map, Cluster-A and Cluster-B. As shown in Figure 4.4, Cluster-A, located on the top-right of the map, shows that older participants who were above 65 years and among the general public (non.mturk), tended not to use avoidant strategies to protect their privacy. On the other hand, pre-older adult participants who were between 55-64 years old and recruited via the crowdsourcing platform, were inclined to use both avoidant and expression strategies (see Cluster-B on Figure 4.4).

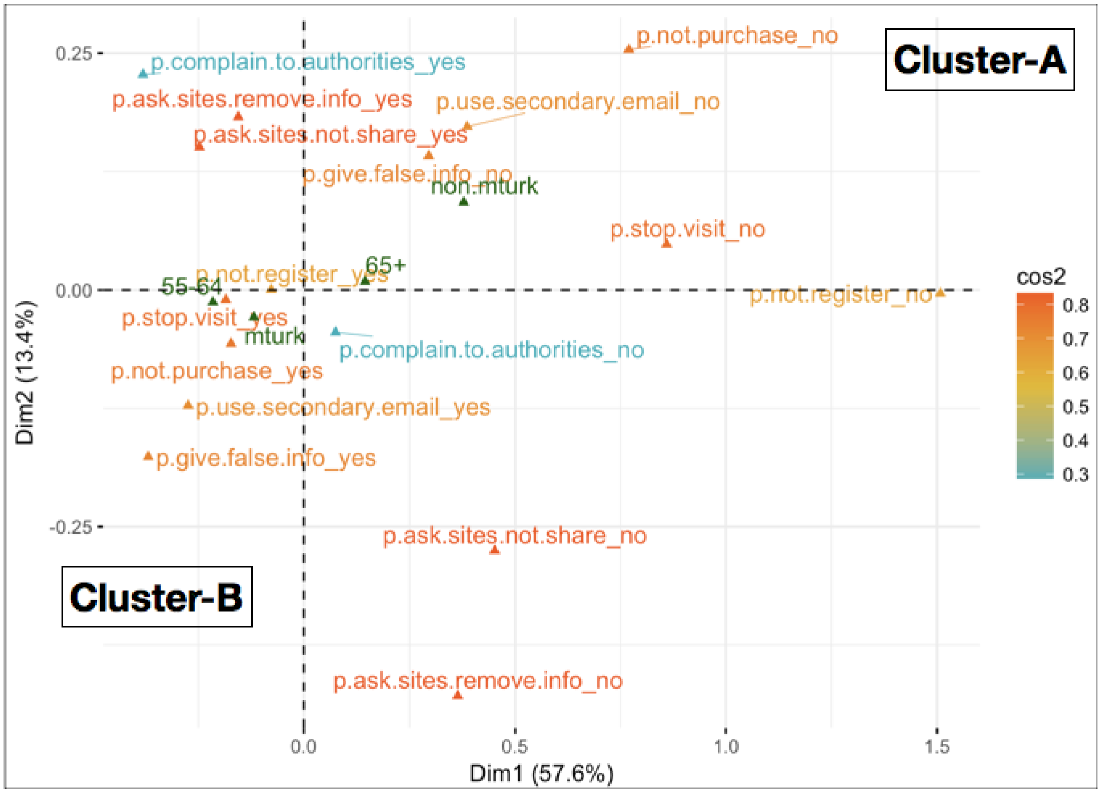


Figure 4.4: MCA map of passive privacy protection

2) MCA of active privacy protection

Similarly, the two-dimensional solution is generated and accounts for 92.3% of the total inertia, which is also sufficient for explaining the model of active privacy protection. Dimension 1 explains the most variance in the model (79.9%), followed by Dimension 2 (12.4%). Figure 2 exhibits the symmetric map of two-dimensional solution for active privacy protection and demographics. According to the map, two active approaches are close to each other, including clearing browsing history, removing cookies, and blocking unwanted emails. We categorized these three active approaches as 'Clearing strategies'. Moreover, we termed the behavior of using software to hide Internet identity as 'Hiding strategies'. The square correlation of these four categories are above 0.8 in Dimension 1, representing the adequate quality of active privacy protection. That is, the category of active privacy protection is well-presented by these four variables.

As shown in Figure 2, a salient Cluster-C is located on the left side of the map, suggesting that pre-older adult participants between 55-64 years old and in the mTurk group tended to take clearing strategy to protect their OIP. In addition, participants of all ages did not report experience in using software to hide their computer ID from online services. In another word, participants were not familiar with this type of active protection.

3) MCA of proactive privacy protection

For proactive privacy protection, the two-dimensional solution is also generated and accounts for 77.3% of the total inertia. Dimension 1 explains the most variance in the model (64.4%), followed by Dimension 2 (12.9%). As shown in Figure 3, the majority of participants had no experience in most proactive approaches, such as using an anonymous browser, third-party blocking plugins, and email encryption. However, participants who reported using a cookies cleaner were more likely to use an online tracker management tool. Hence, we categorized these two proactive approaches as 'Anti-tracking strategies'. Yet, the general public (non.mturk) were disinclined to use anti-tracking strategies when compared to crowdsourcing participants.

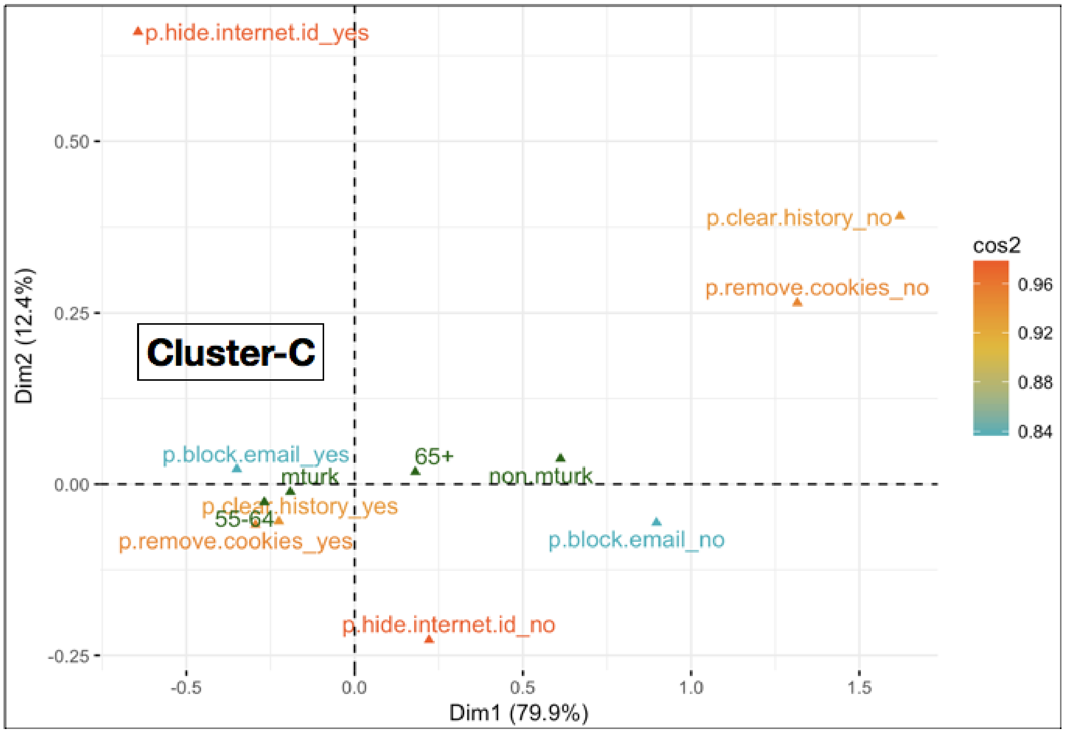


Figure 4.5: MCA map of active privacy protection

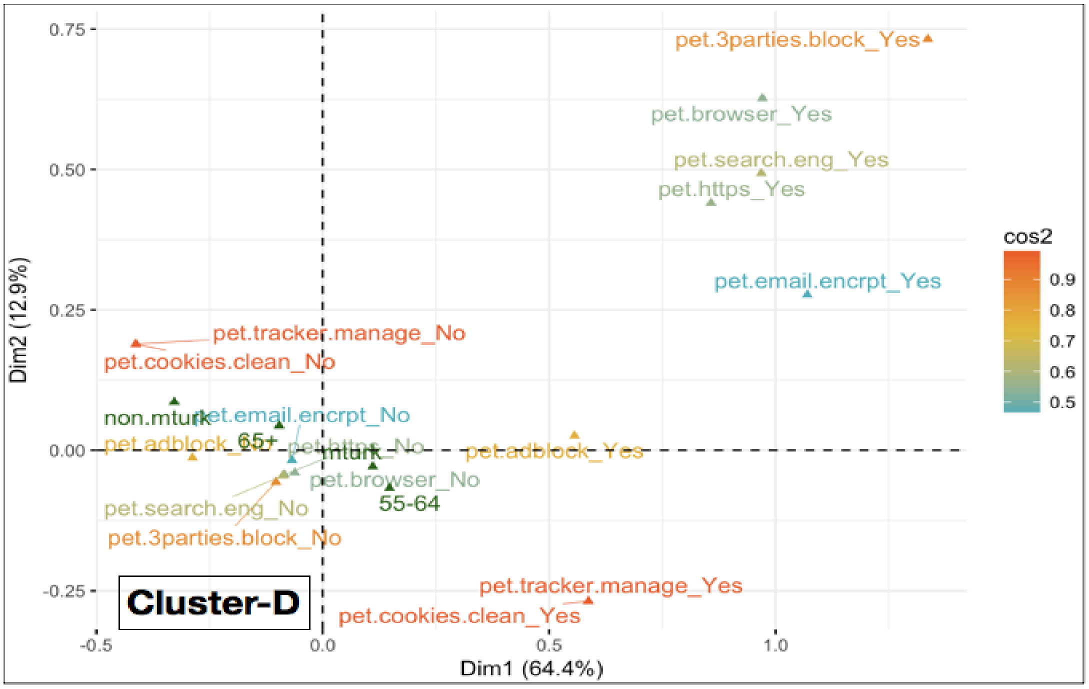


Figure 4.6: MCA map of proactive privacy protection

Table 4.2: Summary of multiple correspondence model for online privacy protection behaviors

	Dimension 1			Dimension 2		
Passive privacy protection	**Coordinate**	**COS^2**	**Contribution**	**Coordinate**	**COS^2**	**Contribution**
p.stop.visit_no	0.860	0.784	15.937	0.048	0.002	0.215
p.stop.visit_yes	-0.185	0.784	3.423	-0.010	0.002	0.046
p.give.false.info_no	0.296	0.594	5.916	0.141	0.136	5.810
p.give.false.info_yes	-0.369	0.594	7.375	-0.176	0.136	7.243
p.not.purchase_no	0.770	0.684	13.220	0.254	0.074	6.169
p.not.purchase_yes	-0.172	0.684	2.960	-0.057	0.074	1.381
p.not.register_no	1.508	0.648	13.523	-0.004	0.000	0.000
p.not.register_yes	-0.077	0.648	0.693	0.000	0.000	0.000
p.complain.to.authorities_no	0.075	0.208	0.574	-0.045	0.074	0.880
p.complain.to.authorities_yes	-0.381	0.208	2.911	0.227	0.074	4.464
Active privacy protection	**Coordinate**	**COS^2**	**Contribution**	**Coordinate**	**COS^2**	**Contribution**
p.clear.history_no	1.621	0.886	26.493	0.391	0.051	9.899
p.clear.history_yes	-0.225	0.886	3.680	-0.054	0.051	1.375
p.block.email_no	0.898	0.834	18.686	-0.056	0.003	0.470

Table 4.2 (cont.)

Active privacy protection	**Coordinate**	**COS^2**	**Contribution**	**Coordinate**	**COS^2**	**Contribution**
p.block.email_yes	-0.350	0.834	7.285	0.022	0.003	0.183
p.remove.cookies_no	1.316	0.913	26.200	0.264	0.037	6.803
p.remove.cookies_yes	-0.295	0.913	5.866	-0.059	0.037	1.523
p.hide.Internet.id_no	0.222	0.476	3.020	-0.227	0.500	20.423
p.hide.Internet.id_yes	-0.644	0.476	8.771	0.660	0.500	59.324
Proactive privacy protection	**Coordinate**	**COS^2**	**Contribution**	**Coordinate**	**COS^2**	**Contribution**
pet.browser_No	-0.062	0.385	0.335	-0.040	0.160	0.698
pet.browser_yes	0.971	0.385	5.253	0.627	0.160	10.955
pet.adblock_No	-0.288	0.763	5.085	-0.013	0.002	0.055
pet.adblock_Yes	0.556	0.763	9.813	0.026	0.002	0.106
pet.3parties.block_No	-0.103	0.668	0.925	-0.057	0.201	1.389
pet.3parties.block_Yes	1.336	0.668	11.945	0.723	0.201	17.941
pet.https_No	-0.085	0.446	0.607	-0.043	0.118	0.801
pet.https_Yes	0.858	0.446	6.150	0.441	0.118	8.115
pet.search.eng_No	-0.089	0.491	0.669	-0.045	0.128	0.870
pet.search.eng_Yes	0.968	0.491	7.316	0.494	0.128	9.506

4.3.2 RQ2: How do older adults' knowledge, concerns, and perceived risks regarding online information privacy impact their privacy protection behaviors?

We further examined the effects of four cognitive factors on older adults' privacy protection approaches. These four factors include: 1) knowledge of privacy and security, 2) concerns about personal information, 3) concerns about online practices, and 4) perceived risks of online activities. Considering the variables of privacy protection behaviors are count data, the Generalized Linear Model with Poisson distribution was conducted for analyses.

The first model is calculated to predict four cognitive effects on older adults' passive privacy protection behaviors, which explains 80.3% of variance (R^2) of the model. As shown in Table 4.3, the only significant predictor in Model 1 is knowledge of privacy and security, which estimated β is larger than 0. This indicates that the more knowledge participants had, the more expected number of passive approaches participants would take to protect their online privacy. More specifically, for one unit of increase in the knowledge, the number of taking passive approaches will increase and be multiplied by 1.04 times (*exp(*0.04)).

Model 2 (see Table 4.3) is conducted to predict cognitive effects on older adults' active privacy protection, which explains 85.7% of variance (R^2) of the model. Similarly, only knowledge is a significant predictor of taking active privacy protections. This suggests that participants with more knowledge about privacy and security will take more active protection for their online privacy. More precisely, for one unit of increase in the knowledge, the number of taking active approaches will increase and be multiplied by 1.08 times (*exp*(0.079)).

Model 3 is analyzed to predict cognitive effects on older adults' proactive privacy protection, which explains 43.8% of variance (R^2) of the model. The only significant predictor is also knowledge of privacy and security. Since the estimate β is positive, participants with more knowledge will take more proactive privacy protection. Furthermore, for one unit of increase in knowledge, the number of taking proactive approaches will increase and be multiplied by 1.18 times (*exp*(0.162)).

Since the knowledge of privacy and security is the only significant predictor of older users' actual privacy protection behaviors, a further analysis is conducted to examine older users' knowledge in each aspect of privacy and security.

Table 4.3: Generalized linear model of online privacy protection behaviors

	Model 1: Passive		**Model 2: Active**		**Model 3: Proactive**	
	β	z-value(*p)*	β	z-value(*p)*	β	z-value(*p)*
Intercept	.751	2.26 (*p*=.024)	-.310	-0.66 (*p*=.509)	-.976	-1.79 (*p*=.074)
Knowledge of privacy and security	.040	3.34 (*p*=.0008)	.079	4.60 (*p*<.0001)	.162	6.88 (*p*<.0001)
Concerns about personal information	-.023	-0.43 (*p*=.668)	.016	0.21 (*p*=.835)	.012	0.13 (*p*=.898)
Concerns about online data practices	.118	1.62 (*p*=.106)	.113	1.10 (*p*=.272)	-.121	-1.06 (*p*=.287)
Perceived risks of online activities	.008	0.15 (*p*=.882)	-.047	-0.58 (*p*=.559)	.115	1.10 (*p*=.272)

4.3.3 Older adults' knowledge of online privacy and security

4.3.3.1. Security-related knowledge

The average mean of score for security-related knowledge is 0.715, meaning that participants answered correctly 71.5% of security-related knowledge. Overall participants showed the understandings of the basic knowledge about Internet security. However, pre-older adult (M=4.03) and mTurk (M=3.92) participants show significantly higher score in security-related knowledge than their older (M=3.83, t=-5.26, p<.0001) and non-mTurk (M=2.95, t=-5.52, p<.0001) peers. As shown in Table 4.4, above 80% of participants answered correctly all statements except for the second one. Only 12.5% of participants answered correctly in whether IP addresses can be used to uniquely identify computer.

4.3.3.2. Privacy-enhancing-tool related knowledge

The average mean of score for privacy-tool-related knowledge is 0.447, meaning that participants answered correctly 44.7% of privacy-related knowledge, which is much lower than security-related knowledge. This may indicate that although older people may have quite sufficient knowledge about Internet security, they may not have the sufficient knowledge about how to apply online tools to protect their Internet privacy. Also, the results show that mTurk participants (M=3.14) displayed more knowledge in privacy-enhancing tools than non-mTurk participants (M=1.36, t=7.18, p<.0001).

As shown in Table 4.5, only 17.9% of participants knew about what Tor is, and 11.8% of them know what virtual private network is. However, we found that participants aged between 55-64 showed more knowledge about the VPN that participants aged above 65. About 78.6% of participants had knowledge about what encryption does and 68.8% of participants showed knowledge about HTTPS. In general, participants showed less knowledge in privacy-enhancing tools.

Table 4.4: % of people who answered correctly for security-related knowledge

Security-related knowledge	% of people who answered correctly				
Statement	All (n=169)	Older group (n=103)	Pre-older group (n=66)	Mturk (n=125)	Non-mturk (n=44)
S1: Public Wi-Fi is as secure as private Wi-Fi.	142 (84.0%)	78 (75.7%)	64 (97.0%)	119 (95.2%)	23 (52.3%)
S2: Internet Protocol addresses can be used to uniquely identify your computer.	19 (11.2%)	7 (6.8%)	12 (18.2%)	14 (11.2%)	5 (11.4%)
S3: When you visit a website, the site can store a cookie so it can recognize your device in the future.	149 (88.2%)	83 (80.6%)	66 (100%)	122 (97.6%)	27 (61.3%)
S4: Phishing scams are usually fraudulent email messages appearing to come from a legitimate entity (e.g., charity, bank, government).	148 (97.6%)	86 (83.5%)	62 (93.9%)	117 (93.6%)	31 (70.5%)
S5: Malware can cause your device to crash and can be used to monitor and control your online activity.	146 (86.4%)	84 (96.7%)	62 (94.2%)	118 (94.4%)	28 (63.6)

Table 4.5: % of people who answered correctly for privacy-tool-related knowledge

Security-mechanism-related knowledge	Number (%) of people who answered correctly				
Statement	All (n=169)	Older group (n=103)	Pre-older group (n=66)	Mturk (n=125)	Non-mturk (n=44)
PT1: Most browsers provide private browsing mode, which can prevent websites from collecting your information. (TRUE)	81 (47.9%)	43 (41.7%)	38 (57.6%)	75 (60%)	6 (13.6%)
PT2: ToR is software that enables you to send anonymous requests to online services. (TRUE)	20 (17.9%)	10 (10.3%)	10 (6.6%)	19 (15.2%)	1 (2.3%)
PT3: A Virtual Private Network cannot allow you to access the Internet privately. (FALSE)	49 (11.8%)	23 (22.3%)	26 (39.4%)	44 (35.2%)	5 (11.4%)
PT4: A website with a HTTPS address is less secure than a website with a HTTP website. (FALSE)	99 (58.6%)	58 (56.3%)	41 (62.1%)	86 (68.8%)	13 (29.5%)
PT5: Encryption can protect your email or device from snooping. (TRUE)	120 (71.0%)	70 (68%)	55 (83%)	99 (79.2%)	21 (47.7%)
PT6: When Two-Factor Authentication (TFA) is applied, it requires not only something you know (e.g., your password or username), but also something you have (e.g., your phone). (TRUE)	84 (49.7%)	51 (49.5%)	33 (50%)	70 (56.0%)	14 (31.8%)

4.3.3.3. Data-practices-related knowledge

The average mean of score for data-practices-related knowledge is 0.596, meaning that participants averagely answered correctly 59.6% of data-practices-related knowledge, which is slightly higher than privacy-tool-related knowledge. In addition, the results show that pre-older adult (M=4.23) and mTruk (M=4.07) participants exhibited more knowledge in online data practices than older (M=3.17, t=-4.57, p<.0001) and non-mTurk group (M=2.18, t=7.16, p<.0001). I found that most participants understood that online services would have the ability to collect their personal data online (DP1 and DP3). However, only about half of our participants knew that online services can still collect their personal data via tracking technologies (DP2 and DP6). Furthermore, about 48.5% of participants knew that online services can disclose their personal information to law enforcements (DP4). Interestingly, the results show that over 60% of older and non-mturk participants thought that online companies will not share personal information with other third parties, and their personal data is protected by privacy policy. These findings indicate that older and offline users are more likely to have misconception toward the data use by online companies.

Table 4.6: % of people who answered correctly for data-practices knowledge

Data-practices-related	**% of people who answered correctly**				
Statement	All (n=169)	Older group (n=103)	Pre-older group (n=66)	Mturk (n=125)	Non-mturk (n=44)
DP1: Companies today have the ability to place an online ad that targets you based on information collected about your web-browsing behavior (TRUE)	158 (93.5%)	95 (92.2%)	64 (97.0%)	123 (98.4%)	35 (73.3%)

Table 4.6 (cont.)

Data-practices-related	**% of people who answered correctly**				
Statement	All (n=169)	Older group (n=103)	Pre-older group (n=66)	Mturk (n=125)	Non-mturk (n=44)
DP2: A company can tell if you have opened an email even if you do not respond (TRUE)	86 (50.9%)	49 (47.6%)	37 (56.1%)	68 (54.4%)	18 (40.9%)
DP3: When you go to a website, it can collect information about you even if you do not register (TRUE)	131 (77.5%)	73 (70.9%)	58 (87.9%)	105 (84.0%)	26 (59.1%)
DP4: Online business sites may exchange your personal information with law enforcement and credit bureaus without your awareness (TRUE)	82 (48.5%)	39 (37.9%)	43 (65.2%)	79 (63.2%)	3 (6.8%)
DP5: If a website has a privacy policy, it means the site will not share your information with other websites or companies (FALSE)	72 (42.6%)	32 (31.1%)	40 (60.6%)	68 (54.4%)	4 (9.1%)
DP6: Social networking sites cannot collect your web browsing information when you are not logged into the service. (FALSE)	76 (45.0%)	39 (37.9%)	37 (56.1%)	66 (52.8%)	10 (4.4%)

4.4 Discussion

4.4.1 Older users' behavioral strategies

In this empirical study, we investigated older adults' online privacy protection behaviors via survey methodology. The findings show that, in general, participants had more experiences in taking *passive* or *active* privacy protections than *proactive* approaches. We categorized older adults' protection behaviors using Multiple Correspondence Analysis. This analysis revealed five main strategies used by older adults within three protection approaches, which are summarized in Table 4.7.

For passive approaches, older adults tend to avoid using online services or express their concerns directly with online service providers. For active approaches, older adults try to clear or hide themselves from tracking capacities. As for proactive approaches, the main strategy adopted by older people is to use privacy-enhancing tools to prevent online tracking.

4.4.2 Privacy divide among older users

In addition, our results also reveal a phenomenon of '*Privacy Divide*' among our study participants. We found a pattern that participants who were in the pre-older adult group of our sample (55-64) and recruited via a crowdsourcing platform were inclined to take more privacy protections than participants aged above 65 and recruited among the general population. This phenomenon corresponds to previous research that has indicated the digital divide among older adults (Friemel, 2016). One possible explanation is that older adults who are still under 65 and using an online crowdsourcing platform may already have more Internet skills and knowledge to protect their OIP. In other words, older adults who are 65 years old and over and of the general public could be more vulnerable to online privacy attacks due to the lack of privacy protection behaviors.

Table 4.7: Categories of older adults' online privacy protection behaviors

Behavior	Strategy	Item
Passive protection	Avoidance	• Stopped visiting particular websites • Gave a false or inaccurate information • Decided not to purchase • Chose not to register • Used secondary email
	Expression	• Asked a website to remove personal information • Asked a website not to share personal information
Active protection	Clearing	• Cleared browsing history • Removed cookies • Blocked unwanted emails
	Hiding	• Used software to hide computer/Internet ID
Proactive protection	Anti-tracking	• Installed cookies cleaner plug-in • Used online tracker management

We also investigated how older adults' cognitive factors (concerns, knowledge, and perceived risks) impact their protection behaviors. Corroborating previous studies (Garg et al., 2011; Lorenzen-Huber et al., 2011), our findings suggest that older adults' knowledge of OIP is the main significantly positive predictor for their behaviors. This further indicates that the lack of knowledge may be the primary cognitive factor leading to older adults' lack of protection behaviors. That is, older adults are concerned about their OIP, but they do not know how to protect it.

Based on our findings, I propose two recommendations for designers and policy makers. First, while developing Internet technologies for older adults, designers should keep in mind that older adults are going to be an increasing user population for Internet technologies, thus there will be many benefits for designing privacy-friendly systems for aging population. In addition, since older adults may have less technological knowledge and are therefore more vulnerable to privacy attacks, it is important to design systems that enables older adults to protect their privacy easily. Furthermore, I think that there is an urgent need to develop an educational program regarding OIP for older adults. Moreover, considering the complexity of OIP and its relevant applications, policy makers need to be creative in delivering complex technological innovations and communicating their related risks through educational materials to older adults.

4.4.3 Limitations and future work

I acknowledge that there are two main limitations in this work. First, our findings are limited to a specific sample because I only recruited U.S. participants. Older adults living outside the U.S. may report different online privacy protection behaviors due to the variety of social contexts and resources. Hence, I suggest future research to recruit international participants and compare the results. Also, our study focused on *what* older adults do to protect their OIP; it still remains unclear *why* older adults prefer taking certain approaches over others. I recommend future research to conduct a qualitative study that may provide more in-depth understanding about older adults' decision-making and their online privacy protection behaviors.

Chapter 5. Older Users' Emotional Impact on Use of Private Browsing Mode

5.1 Introduction

Internet technologies have brought positive influence on people's daily lives around the world. However, the ubiquitous and constant data collection and analyses also pose potential threats to users' online privacy. Also, increasing reports regarding data breaches and hacking have raised public awareness about online privacy and motivate users to seek protection for personal privacy. While many technologies and policies have been proposed and established, we still have limited understanding of inconsistencies in online users' attitudes and behaviors when it comes to privacy. The privacy literature has termed this phenomenon the "privacy paradox" (Barnes, 2006).

The privacy paradox is the phenomenon in which an inconsistency lies between people's attitudes and behaviors regarding online privacy. People often express concerns about their online privacy yet show little regard to privacy in their daily online behaviors (Acquisti et al., 2015). That is to say, people are aware of the potential privacy risks but still make 'irrational' choices. For instance, users still tend to download mobile applications that require access to various types of sensitive information even though they have been informed about such risks (Huang and Bashir, 2017). Many studies have examined people's irrational privacy behaviors from a rational calculus perspective (Culnan and Armstrong, 1999; Dinev and Hart, 2006; Wilson and Valacich, 2012). However, as indicated by Acquisti et al. (2015), privacy-related decision-making is not only affected by people's rational thoughts but also their bounded rationality, social norms, heuristics, and emotions. Studies have also evidenced that emotion plays a fundamental role in our decision-making and behaviors (Vohs et al., 2007; Andrade and Ariely, 2009). Therefore, I postulate that an important, missing piece in the online privacy literature is the role of emotion.

Human emotion is a challenging concept that is difficult to quantify and often debated within the disciplines of psychology, philosophy, and neuropsychiatry (Stark, 2016). In this study, we view emotion as a subjective and conscious experience with various degrees of mental intensity (Ekman and Davidson, 1994; Cabanac, 2002). In addition, previous research has indicated that emotional responses have informational value to people's decisions (Schwarz, 2011). Furthermore, from a HCI perspective, the design of technology can affect users' emotions and further influence their adoption of technology (Norman, 2004). For older users, the emotional factors such as computer anxiety or fear of failure also affect their adoption of technology (Wagner et al., 2010; Wang et al, 2017; Czaja et al., 2006). Following this rationale, I argue that emotion plays a mediator role between users' attitudes and behaviors when it comes to adopting privacy-enhancing features.

Several privacy-enhancing features and technologies has been designed and developed in the last decade. These privacy-enhancing features range from interface design (e.g., Cranor et al., 2006; Kelley et al., 2009) to system development (e.g., Dingledine et al., 2004; Goldberg et al., 1997). However, these features and technologies are still rarely used by people (Hourcade et al., 2014). If we were to examine users' adoption of privacy-enhancing features solely from a rational point of view, we may conclude that users do not adopt or constantly use privacy-enhancing features because they perceive these features to be useless or too difficult to use (Davis, 1985). Nevertheless, as numerous studies have suggested, user behavior not only involves cognition but also emotion. Perhaps users do not use privacy-enhancing features simply because these features make them feel discomfort or displeasure. Although the role of emotion in online privacy has gained more attention in academia (Stark, 2016), it has not been investigated as a principal factor in the adoption of privacy-enhancing features. Hence, the aim of this study is to investigate how users' emotional responses influence their acceptance of privacy-enhancing features.

To study this topic, I propose hypotheses motivated by the theoretical framework of feelings-as-information theory and Technology Acceptance Model. I used private browsing as a case study and designed a survey experiment to investigate how private browsing elicits users' emotions and how these emotions affect their acceptance of private browsing. This work contributes to the usable privacy literatures in several ways. First, I propose an extensive framework of Technology Acceptance Model by considering emotional effects on users' attitudes and behavioral intentions. Second, as far as I know, this is the first study to measure emotion related to the concept of privacy. Third, this study empirically examines how the design of a privacy-enhancing feature can provoke user emotions, which further influence user attitudes and behavioral intentions toward the feature.

5.1.1 Prior literature: emotion, privacy, and interface design

Usable privacy is a field of study that focuses on improving privacy technologies from a Human-Computer Interaction (HCI) perspective. Thus, it is important to examine emotion from an HCI point of view. Emotion has become an important consideration in the field of HCI because more and more scholars and studies evidence its impact on users' experiences with technologies (Norman, 2004; Brave and Nass, 2003; Agarwal and Meyer, 2009). Previous studies in HCI have focused on several emotion-related topics, including measuring emotional dimensions in user experience (Agarwal and Meyer, 2009; Kim et al., 2003), emotional effects on the use of technologies (Agarwal and Karahanna, 2000; Beaudry and Pinsonneault, 2010; Loiacono and Diamasbi, 2010), designing affective user interface (Johnson and Wiles, 2003; Lisetti and Nasoz, 2002), positive emotion-driven design (Finneran and P. Zhang; 2003; Finneran and Zhang, 2005; Ghani, 1995; Koufaris, 2002; Carroll and Thomas, 1988; Hassenzahal, 2007) and the emotional deduction from the artifact (e.g., mouse cursor) (Hibbeln et al., 2017). Although the importance of emotion has been recognized in the HCI literature, its role in the context of privacy has been under-studied (Stark, 2016). In the following sections, we will review the most relevant work on how emotion is associated with interface design, users' technology acceptance, and privacy from an HCI perspective.

5.1.1.1 Emotion and interface design

Interface, as an external appearance of a system, can determine how we feel, perceive, and interact with a system (Demirbilek, 2017). Previous studies have shown that the visual design elements of an interface, such as the shape, color, and texture, can affect users' emotions (Brave and Nass, 2003; Kim et al., 2003; Demirbilek, 2017). For instance, a study by Kim et al. (2003) found that the mixed use of shapes and colors in a menu bar can create a mystic feeling; yet the mixed use of shapes in a background can make users feel confused. In addition, users' emotional responses to design are usually immediate and consistent across time (Tractinsky et al., 2006). While the emotional effect on users' perceptions and behaviors depends on the task and the context (Agarwal, and Venkatesh, 2002; Venkatesh et al., 2003; Venkatesh and Ramesh, 2006), emotion elicited by the design of a system remains a fundamental and influential factor on users' decision-making in technology acceptance.

5.1.1.2 Emotion and technology acceptance

Emotion as a mental state can directly or indirectly influence people's attitudes, decision-making, and behaviors (Russel, 2003; Gratch, and Marsella, 2004; Baumeister et al., 2007). When it comes to the use of technology, studies have shown that positive emotion elicited by system design has positive effects on users' acceptance and use of technology (Venkatesh, 2000; Agarwal and Karahanna, 2000). Conversely, negative emotion elicited by system design results in negative effects on users' perceived ease-of-use (Venkatesh, 2000), and technology adoption (Venkatesh, 2000). Furthermore, users who experience negative emotion will be more likely to spread negative word of mouth (Hibbeln et al., 2017; Gelbrich, 2010), which may further decrease users' acceptance of technology.

5.1.1.3 Emotion in privacy context

The role of emotion in the context of privacy can be discussed from two perspectives: 1) privacy as an emotion (Young, 1978), and 2) emotion as an antecedent of privacy attitudes and behaviors (Sarathy and Xu, 2011).

a) Privacy as emotion

Psychologists have argued that privacy is an emotion that can elicit one's positive feelings and further enhance an individual's autonomy, creativity, and recovery (Young, 1978; Pedersen, 1997). In privacy literature, creepiness is one particular emotional reaction that is often expressed in response to tracking technologies. Creepiness has been described as a combination of fear, uneasiness, strangeness, and disturbance (Tene and Polonetsky, 2013; Ur et al., 2012; Zhang et al., 2016). An interview study by Ur et al. (2012) found that users have creepy feelings about online behavioral tracking technologies even though they consider these technologies to be intelligent. The feeling of creepiness can decrease users' intentions to purchase online (Barnard, 2014).

Furthermore, privacy-enhancing features may elicit feelings of creepiness, which further can trigger users' privacy concerns (Zhang et al., 2016). Zhang et al. (2016) conducted an online experiment to investigate the mediating effects of creepiness between privacy cues (e.g., privacy nudge) on a privacy permission interface and users' privacy attitudes in the setting of a social mobile application. They found that privacy cues may increase users' alertness and elicit creepiness emotions. The creepy feeling further makes users more concerned about their information privacy, perceive less control, and feel less comfortable disclosing personal information. In other words, privacy-enhancing features can trigger negative emotions that may discourage the use of technology.

b) Emotion as a privacy antecedent

Prior research has found that emotion can be a significant predictor for privacy attitudes and behaviors. For example, Li et al. (2011) found that users who rate higher in joyful emotion believe that their privacy is more protected and perceive less privacy risks. On the other hand, users who feel more fears perceive more privacy risks. Another study by Anderson and Agarwal (2011) found that users who have more negative feelings (e.g., sadness, anger, and fear) toward their health condition are more willing to disclose their personal health information. However, the knowledge of emotional effects on privacy attitudes and behaviors is still limited.

Based on previous work, we identified three research gaps in HCI and privacy research, and proposed research questions to address each gap:

- *Type of emotion elicited by privacy-enhancing features remains unidentified*: Although prior studies (Zhang and Xu, 2016; Ur et al., 2012) have pointed out that privacy-enhancing features can provoke an emotion of creepiness, we still have very limited knowledge about how users feel about privacy-enhancing features. Do privacy-enhancing features only elicit users' negative emotions, or do they also evoke positive emotion?

- *Effects of the design of privacy-enhancing features on users' emotions, attitudes, and acceptance remain unclear*: The literature in HCI has indicated that the design of a system can affect users' emotions (Brave and Nass, 2003; Kim et al., 2003; Demirbilek, 2017). Yet, very few studies focus on how the design of privacy-enhancing features affect users' emotions.

- *Emotional effects on the acceptance of privacy-enhancing features remain unknown*: Research (Zhang and Xu, 2016) has pointed out that emotion can affect users' privacy attitudes and use of technology. However, how emotion influences users' attitudes and the acceptance of privacy-enhancing features remains unclear.

My research questions are as follows:

- RQ1: What types of emotion will be elicited in older users by privacy-enhancing features?

- RQ2: How does the interface design of private browsing mode affect older users' emotions?

- RQ3: How does emotion elicited by privacy-enhancing features affect older users' attitudes and use of those features?

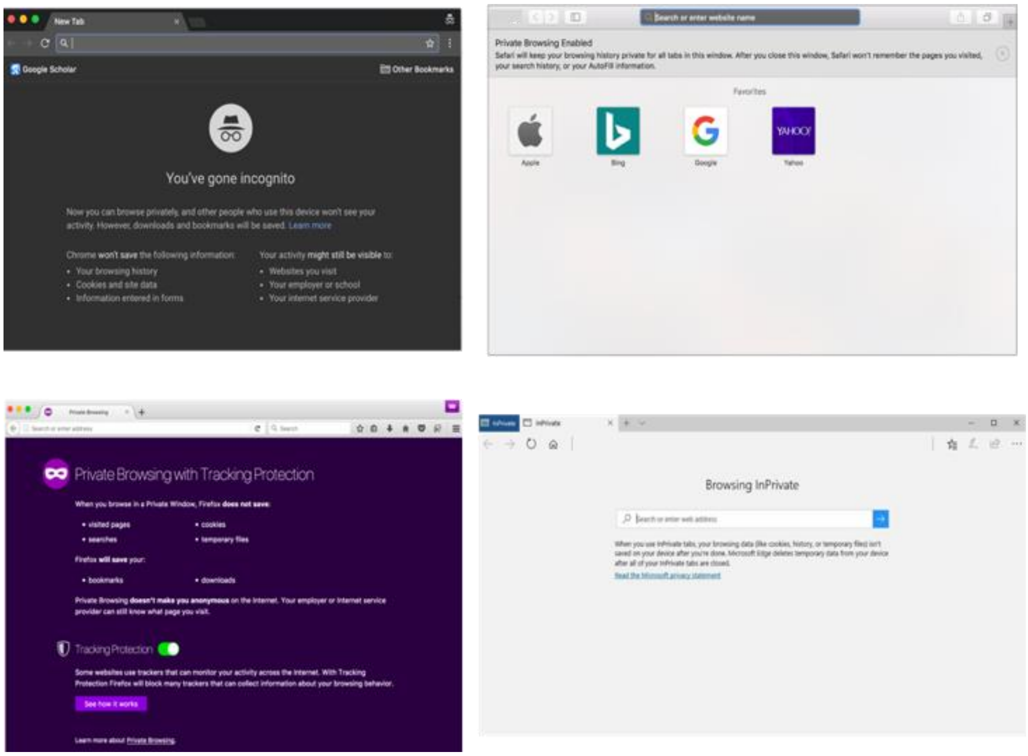
5.1.2 Privacy-enhancing feature: a case study of private browsing mode

An abundant of privacy-enhancing features and functions have been developed as technologies become smarter and more personalized. These privacy-enhancing features include a wider range of applications from interface design (i.e., Cranor et al., 2006; Kelley et al., 2009) to system development (i.e., Dingledine et al., 2004; Goldeberg et al., 1997). One of the popular privacy-enhancing features is private browsing mode. Private browsing mode has been offered as a built-in function in most of today's leading browsers, including Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft Edge/IE. The goal of private browsing mode is to prevent one's browsing history and personal information from being accessed by either local adversaries or tracking sites (Liou et al., 2016). Although most browsers provide similar features in private browsing mode, the design and functionality still vary among browsers. For instance, each browser has different names, indicators, and functions (see Table 5.1).

Also, as shown in Figure 5.1, the interface design for private browsing mode in these four browsers are different from each other. We think that private browsing mode is an appropriate case study for this study for two reasons. First, it is easy to access by users; and second, it encompasses similar functions across browsers but varies in interface design, which is useful for comparing how the design of privacy-enhancing features can elicit emotions that affect users' attitudes and acceptance. We thus select private browsing mode as a research subject in this study. In the next section, we address our hypotheses based on a proposed theoretical framework.

Table 5.1: Overview of private browsing mode on leading browsers

Browser	Chrome 63	Firefox 57	Safari 11	Edge/IE
Name	Incognito window	Private window	Private browsing	InPrivate mode
Indicator	🕵	🎭	Search bar in dark grey	▨ InPrivate
Function	Browsing history, Cookies, Auto-fill info	Browsing history, Cookies, Temporary Internet files	Browsing history, Cookies, Auto-fill info	Browsing history, Cookies, Temporary Internet files



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Private Browsing Enabled

Safari will keep your browsing history private for all tabs in this window. After you close this window, Safari won't remember the pages you visited, your search history, or your AutoFill information.

Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox **does not save**:

- visited pages
- cookies
- searches
- temporary files

Firefox **will save** your:

- bookmarks
- downloads

Private Browsing **doesn't make you anonymous** on the Internet. Your employer or Internet service provider can still know what page you visit.

Tracking Protection

Some websites use trackers that can monitor your activity across the Internet. With Tracking Protection Firefox will block many trackers that can collect information about your browsing behavior.

Learn more about Private Browsing.

Browsing InPrivate

When you use InPrivate tabs, your browsing data (like cookies, history, or temporary files) isn't saved on your device after you're done. Microsoft Edge deletes temporary data from your device after all of your InPrivate tabs are closed.

Read the Microsoft privacy statement

Figure 5.1: Private browsing mode interfaces (up left to right: Google incognito mode, Safari private browsing mode; down left to right: Firefox private window, Edge InPrivate mode)

5.1.3 Theoretical framework and hypotheses

Emotion is a conscious experience that involves mental activity at different levels of intensity and arousal (Ekman and Davidson, 1994; Cabanac, 2002). According to social psychology, emotion is a type of information that affects people's attitudes and behaviors. For instance, according to feelings-as-information theory (Schwarz, 2011), people use emotions as information to guide their evaluations when they determine that their emotional reactions are valuable to their decision-making (Schwarz, 2011). For instance, if an individual believes that her/his emotional responses are reasonable bases for judgment, s/he will use them to form attitudes. On the other hand, if s/he determines that emotional responses are unrelated, then s/he will exclude them from judgement. However, people will depend less on emotions when they have high expertise in the field of judgement (Schwarz, 2011). Applying this concept, emotion is an affective information that can shape people's attitudes and decisions when it comes to an unfamiliar topic or object. Although psychologists have evidenced emotional impact on people's attitudes and decision, emotion seems to be an understudied factor in the premise of Technology Acceptance Model (TAM) (Davis, 1985).

TAM is a well-known and popular model that has been proposed to understand users' acceptance of technology from a cognitive perspective. According to TAM, users' intentions to use a technology is predicted by users' attitudes toward the technology. Due to the focus on the cognitive aspect, the role of emotion in TAM seems to be overlooked or treated as an extension of attitudes, and/or an indirect predictor of behavioral intention (Kulviwat et al., 2007; Bagozzi, 2007). For instance, although Venkatesh (Venkatesh, 2000) included computer anxiety in the TAM model, the anxiety is treated as an antecedent of perceptions instead of a main factor that influences behavioral intention. Therefore, we propose an extensive framework of TAM that considers the effect of emotion on both users' attitudes and behavioral intentions (see Figure 5.2). I next address the hypotheses of this study.

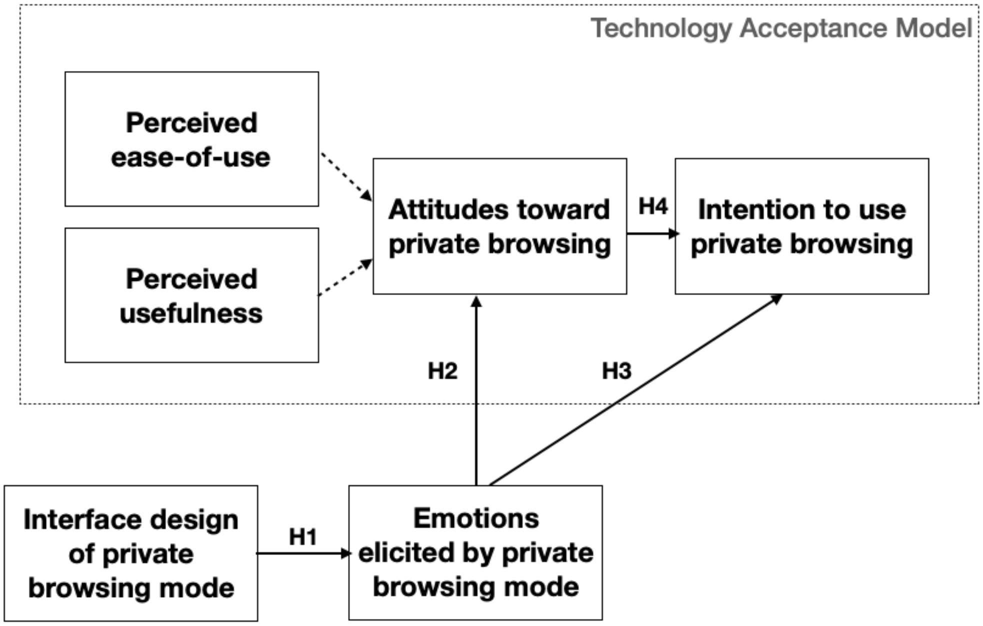

Technology Acceptance Model
Perceived ease-of-use
Perceived usefulness
Attitudes toward private browsing
H4
Intention to use private browsing
H2
H3
Interface design of private browsing mode
H1
Emotions elicited by private browsing mode

Figure 5.2: Theoretical framework and hypotheses

Based on aforementioned models and literature, we think that the design of private browsing mode can provoke users' emotions. For instance, the indicator on private browsing mode may remind users of their private state, which may make them feel that they are 'hiding something'. Thus, our first hypothesis is that private browsing mode will provoke users' negative emotional responses.

> H1: Compared to the normal browsing mode, private browsing mode will provoke more negative emotions in users.

Furthermore, this negative emotion can further affect users' attitudes and their behavioral intention to use private browsing. Consequently, our second and third hypotheses are that users' negative emotion provoked by private browsing mode will impact users' attitudes and behavioral intention toward private browsing.

> H2: Negative emotions provoked by private-browsing mode will adversely influence users' attitudes toward private browsing.

> H3: Negative emotions provoked by private-browsing mode will adversely influence users' intentions to use private browsing.

According to TAM, users' attitudes toward technology have direct effects on their behavioral intentions (Davis, 1985). If users have positive attitudes toward the technology, they will show more intentions to use it; and vice versa. Based on this rational, we hypothesize that users' negative attitudes toward private browsing will have adverse influences on their intentions to use private browsing.

> H4: Users' negative attitudes toward private browsing will adversely influence users' intentions to use private browsing.

5.2 Method

To address the proposed hypotheses, we conducted a mixed-design online survey experiment with one between variable (types of browser) and one within variable (browsing modes: public and private mode). For browser types, we selected four leading browsers as testing subjects, including Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft Edge/IE (W3Schools, 2017).

5.2.1 Survey procedure

Prior to the beginning of the survey, participants were asked to answer four screening questions about what operating system, browser type, and browsing mode they were familiar with and currently use for their online activities. Considering that familiarity with the browser may bias users' emotional response, participants were randomly assigned to assess one of the browser interfaces that they are not currently using or familiar with. In addition, previous research shows that the majority of online browsing takes place in the default or public mode while private mode is only utilized when there is a specific browsing need (Gao et al., 2014). Therefore, based on this inference, we simulated our study design to mimic a real-world scenario where participants were first presented public (default) browsing mode and then private browsing mode. Table 2 exhibits each condition of this survey experiment.

Table 5.2: Design of Survey Experiment

	Public mode	**Private mode**
Condition 1 (n=59)	Chrome	Incognito mode
Condition 2 (n=72)	Firefox	Private window
Condition 3 (n=86)	Safari	Private browsing
Condition 4 (n=88)	Edge	InPrivate mode

The survey includes four sections. In Section 1, participants were first asked about how they felt at the moment. Then they answered questions about their use of the Internet, previous user experience and knowledge of private browsing, as well as a short form about personality traits. In Section 2, participants were firstly presented with the browser interface in normal mode and were asked to rate their emotions about the interface. Then, participants were asked to answer 3 riddle questions to distract their attentions from previous evaluation. Next, participants repeated the same procedure for the interface in private browsing mode. In Section 3, participants were asked to rate their degree of satisfaction with the interface and answered open-ended questions about the interface design. In Section 4, participants' attitudes and behavioral intention toward private browsing mode were measured. At the end of this survey, participants answered demographic questions. This survey experiment was approved by Internal Review Board (IRB). Figure 5.3 exhibits the flow of survey experiment.

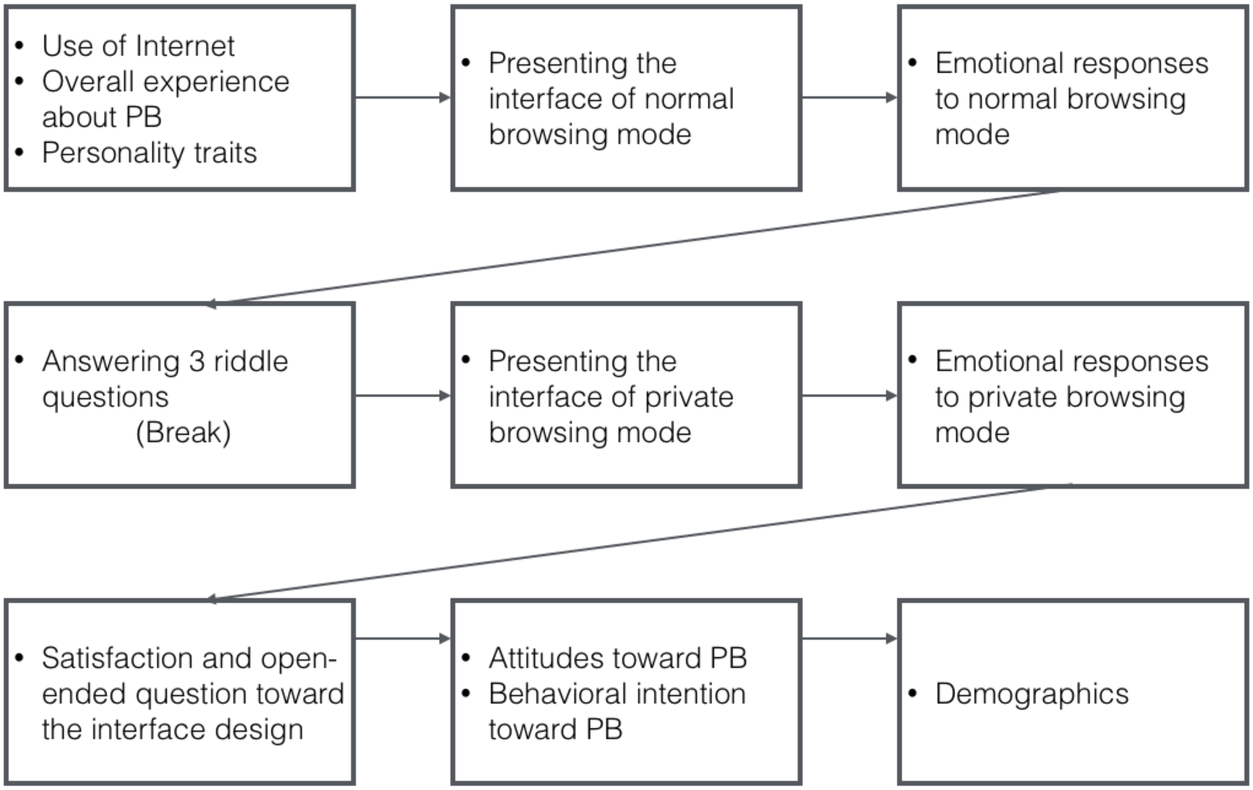

• Use of Internet
• Overall experience about PB
• Personality traits
• Presenting the interface of normal browsing mode
• Emotional responses to normal browsing mode
• Answering 3 riddle questions (Break)
• Presenting the interface of private browsing mode
• Emotional responses to private browsing mode
• Satisfaction and open-ended question toward the interface design
• Attitudes toward PB
• Behavioral intention toward PB
• Demographics

Figure 5.3: Flow of survey experiment

5.2.2 Participants

We recruited 122 older participants aged above 60 years old through Amazon Mechanical Turk, 65 of whom were female. The average age is 66.52 (SD=3.51). For education, 9.8% of participants had a high school degree, 35.7% had completed some college or associate's degrees, 35.7% had earned bachelor's degrees, and 18.9% had earned advanced degrees. All of our participants were from the United States. After completing the study, participants were given $0.85 compensation for their participation.

Table 5.3: Participants' information of the use of browser

Objects	Primary browser for Internet use (n=122)	Browser use for private browsing (n=63)
Chrome	68.0%	65.1%
Firefox	18.0%	22%
Safari	5.7%	4.8%
IE/Edge	7.3%	3.2%
Don't know	1.0%	--
Other	--	4.7%

5.2.3 Measurement

5.2.3.1 Emotions about privacy

To the best of our knowledge, no previous studies have developed measurements to assess people's emotions about privacy. Since emotion is a multifaceted concept, it is very important for us to clarify which aspect of emotion we measured. In this current study, we focused on measuring participants' subjective 'feelings', which are a fundamental part of emotion (Desmet, 2003). Therefore, readers will see the terms of emotions and feelings used interchangeably in following sections.

To generate elicited emotions related to privacy, we conducted a pilot study with 20 online participants who were asked to list up to 10 types of 'feelings' that they would associate with the concept of privacy. A total of 124 words were generated by these participants to describe their emotions about privacy. We first examined these words and selected the words that described basic emotions (Ekman, 1992). The basic emotions addressed by our participants included sadness, anger, fear, and disgust. Then, the words that did not fit into the basic emotion category were labelled as privacy-related emotions. The privacy-related emotions included feeling private, safe, not being watched, not legitimate, and hiding.

We applied the above two categories of emotions (basic emotions and privacy-related emotions) to measure participants' emotions toward private browsing. We adopted self-reported Basic Emotion Assessment (Therapy Aid, 2018) to measure 6 types of basic emotions (happy, sad, angry, fearful, excited, disgusted) using a 6-point unipolar scale. To measure privacy-related emotions, we employed the emotions that were generated by our study participants as mentioned above. A total of 7 items were developed, including: *1) private-public, 2) safe-vulnerable, 3) not being watched-being watched, 4) not censored, censored, 5) feeling like a legitimate citizen-feeling like a criminal, 6) ordinary-feeling unique, 7) having nothing to hide-having something to hide*. Participants were asked to rate on 5-point bipolar scale. To test the internal consistency of the scale, the Cronbach's alpha is measured, which is 0.79.

5.2.3.2 Attitudes toward private browsing

To measure participants' attitudes toward private browsing, we adopted and developed 5 items based on the framework of TAM (Davis, 1985; Venkatesh, 2000). These items included: Private browsing is *1) useful, 2) effective, 3) easy-to-use, 4) an appropriate way, 5) a secure way* to protect my online privacy (Cronbach's alpha =.91). Participants were asked to rate their attitudes on a 7-point Likert scale.

5.2.3.3 Intention to use private browsing mode

We developed 5 items to measure participants' intentions to use private browsing mode using a 7-point Likert scale. These items were: I intend to: *1) use private browsing mode to protect my online privacy, 2) use private browsing mode to secure my personal information online, 3) use private browsing mode more often than before, 4) use the private browsing as* *the default on my browser, 5) recommend others to use private browsing mode* (Cronbach's alpha =.88).

5.3 Results

5.3.1 Older adult's use of private browsing: an overview

The majority of our participants had home internet and password for their Wi-Fi. Most participants use either desktop or laptop computer for their online activities. The average amount of daily Internet use reported by participants was 5.17 hours (SD=3.18). As shown in Table 5.4, 68% of participants used Chrome as their primary browser for Internet use, followed by Firefox, IE/Edge, and Safari. For private browsing, 51.6% (n=63) of people had experience with private browsing mode; 27.1% (n=33) reported no experience; and 21.3% (n=26) did not know what private browsing mode is. Over half of participants reported to use Chrome for private browsing, which is followed by Firefox, Safari, and IE/Edge (see Table 5.4). The average daily use of private browsing is 2.53 (SD=3.55) hours. Table 1 exhibits more detailed information about participants' use of Internet and private browsing.

5.3.1.1 Why do older adults use private browsing?

Prior research has explored the reason what do people use private browsing mode for, including not wanting browsing history and cookies saved, protecting personal information, visiting dating or porn websites, online shopping, entertaining online on work computers, using for curiosity (Gao et al., 2014). Yet, 95.5% of their participants were younger adults. In this study, I am interested if older adults have different needs for using private browsing mode.

The results show that over 80% of participants used private mode because they want to avoid online tracking; and about 50% want to avoid personalized ads. In addition, 30% of participants use private mode to visit websites that are taboo or stigmatized, and approximately 20.6% use it because they do not want family members to know what they browse online. 7.9% of participants did not want employer to know what they do online. Four participants selected other reasons and 4.8% of them used private browsing to secure their financial information, and 1.6% used it to disable caching on browser.

Table 5.4: Overview of older participants' use of Internet and private browsing

Variable	**%**
Home Internet (n=122)	
Yes	98.4%
No	0.6%
Wi-fi password for home Internet	
Yes	91.0%
No	5.7%
Don't know	3.3%
Device used primarily for online activities (n=122)	
Desktop computer	43.4%
Laptop computer	49.2%
Smartphone	6.6%
Tablet	0.8%
Shared device used primarily for online activities (n=122)	
Yes	19.7%
No	80.3%
Primary browser for Internet use (n=122)	
Chrome	68.0%
Firefox	18.0%
Safari	5.7%
IE/Edge	7.3%
Don't know	1.0%
Use of private browsing mode (n=122)	
Have used	51.6%
Don't use	27.1%
Don't know	21.3%
Browser use for private browsing (n=63)	
Chrome	65.1%
Firefox	22%
Safari	4.8%
IE/Edge	3.2%
Other	4.7%

Table 5.5: Reasons for using private browsing mode.

Reason	% (n)
Don't want online services to track me	81.0% (n=51)
Don't want to see personalized ads	50.8% (n=32)
Visit websites that are taboo or stigmatized	30.2% (n=19)
Don't want family members to know what I do online	20.6% (n=13)
Don't want employer to know what you do online	7.9% (n=5)
Other: to increase security for visiting financial websites	4.8% (n=3)
Other: to disable caching on browser	1.6% (n=1)

5.3.1.2 Why do older adults not use private browsing?

I also explored why older adults they do not use private browsing mode. There are two main reasons: 1) have no need to use; and 2) have no knowledge or information about private browsing mode.

When I look into details about why participants thought that there is no need to use it, there are several reasons. First, many participants simply do not 'feel' the needs without specific explanation. Second, participants have their own way to protect their online privacy and they hence do not have the need to use private browsing. In addition, some participants reported that they have nothing to hide. For example, a participant pointed out that s/he never go to the sites that s/he is ashamed of so that there is no need for using private browsing. This further suggests that user may think that private browsing is only for people who have something to hide. Furthermore, two participants reported that they do not care about privacy. More specifically, they do not care if other people know what they do online. Several participants also emphasized that they do not share their computer with others, indicating that they may think the purpose of using private browsing is only for preventing offline people from knowing their online activities. Another specific reason addressed by participant is that private browsing is not safer since her/his computer can still get infected by virus.

Another main reason why older users do not use private browsing is because they do not have knowledge or information about it. Most participants reported that they did not know what private browsing mode is or means, and how to use it. For some participants who do not know about private browsing, they also reported that they have no needs for it. Conversely, other participants expressed the interests in learning more about private browsing mode.

Table 5.6: Reasons for not using private browsing

Category	Reason	Example of Participants' Response	No.
No need to use private browsing	Don't feel needs to use private browsing mode	*"Never felt the need"* *"I don't have any need to."* *"I don't feel I need it."*	13
	Have their own way to protect privacy	*"I know, what private mode is, but I don't have a reason to use it. Once in a while, I clean my cache, cookies and history myself."* *"I use secure mode with the use of AVG Internet Security Suite."*	2
	Have Nothing to hide	*"I don't need to. I have nothing to hide."* *"I have no need to, I do not visit sites that I would wish to hide my browsing history of…"* *"I never go to sites that I'm ashamed of."*	5
	Don't care about privacy	*"I just never feel the need. I don't really care who knows I am on line."* *"I do not care who knows what i do on the web."*	2

Table 5.6 (cont.)

Category	Reason	Example of Participants' Response	No.
No need to use private browsing	Don't share the computer	*"Since I don't share a computer with anyone...I don't see any need to keep my browsing private."* *"I live alone, and others rarely use my computer."*	4
	Private mode is not safer	*"I have no need for privacy mode. I understand they ignore cookies. Cookies need to be enabled on my computer as I do online marketing and it is a necessity...In my opinion It's not safer as I can just as easily be infected with a virus from an installation."*	1
No knowledge & information about private browsing	Don't know what private browsing is	*"I've never heard of private mode and have no idea what it is."* *"I don't know anything about private mode or that other one I have run across occasionally, don't know what the differences are between the different modes and haven' researched them "*	8
	Don't know the concept of private browsing	*"not sure what you mean perhaps you are referring to a VPN? which I do use at times"*	6
	Don't know how to do private browsing	*"I don't know how to use it."* *"...I don't know how to get to it or turn it on or what it does."*	5
	Don't know what it is but will try	*"I am not sure how to use the private mode. If it is more safe to use the private mode, I will, if someone teaches me how to do so."*	1

Table 5.6 (cont.)

Category	Reason	Example of Participants' Response	No.
No knowledge & information about private browsing	Don't know what it is but curious about it	*"I am not sure what private mode is and how to install it...But I will look into it."* *"I did not know you could use a private setting, I may try it..."*	2
	Don't know about it and don't have needs	*"Never heard anything about it and why I would use it."* *"I don't know anything about it and don't know how to do it or why I should"*	2
	Not sure if they have used it before	*"I don't know what private mode is. I mean, I may be using it without knowing I'm using it."*	2
	Just don't use it	*"I know it's there I just don't use it although I know I should to protect my privacy"*	1

5.3.2 Emotion provoked by private browsing

Our first hypothesis is that the design of private browsing mode will provoke users' negative emotions (H1). The nonparametric Wilcoxon signed-rank test was conducted to test participants' self-reported emotions in normal and private browsing mode.

For basic emotions, we found that participants rated significantly higher in fearful feeling toward private mode than normal mode (V=131, p=.002). However, there are no significant differences in other basic emotions (Figure 5.4 a).

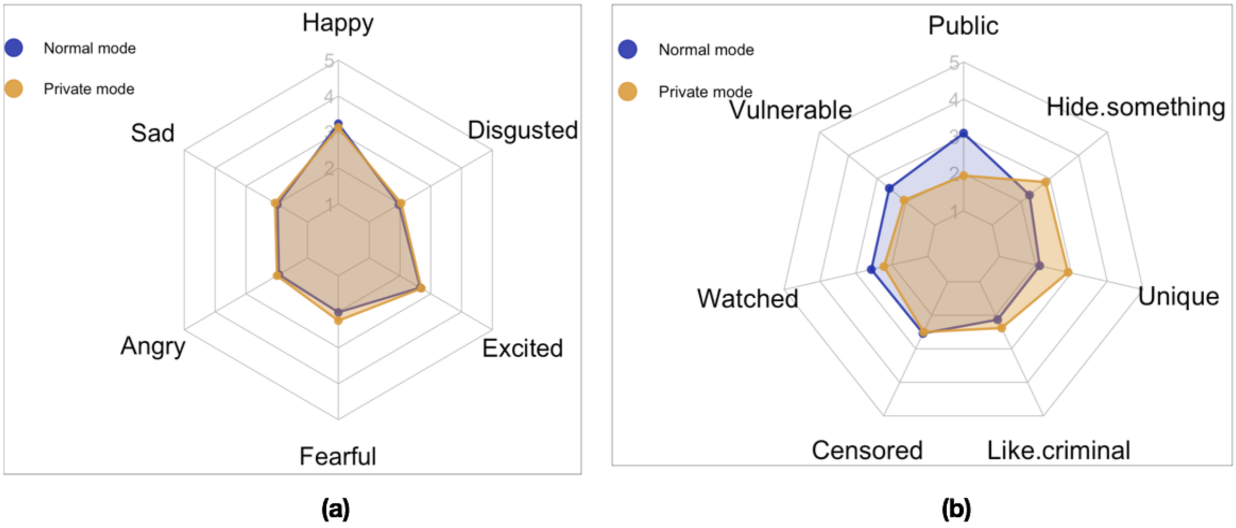


Figure 5.4: Basic emotions (a) and privacy-related emotions (b) elicited by normal and private browsing modes

For privacy-related emotions, participants reported feeling less public (V=22056, p<.0001), vulnerable (V=11858, p<.0001), and being watched (V=12790 p<.0001) in private mode than normal mode. In other words, private browsing mode provoked emotions of feeling private, safer, and not being watched. Nevertheless, private browsing mode also significantly elicited more emotions such as feelings like a criminal (V=448.5, p=.0002), feeling unique (V=2468, p<.0001), and feeling hiding something (V=711, p<.0001) when compared to normal mode (Figure 5.4b). We found no significant difference in feeling censored. These results suggest that private browsing mode interfaces did provoke certain negative emotions in participants. Accordingly, H1 is supported.

5.3.3 Browsers' interface design and its effect on users' emotions

We were also interested in how users feel distinctively toward different private browsing mode interfaces in the leading browsers. Considering the non-normalized distribution of our data, we used the Kruskal-Wallis H test to determine if the medians of emotion, attitudes, and intention to use toward private browsing mode are equal across these four browsers. When the Kruskal-Wallis H test was significant, we further conducted a post-hoc analysis by using Dunn's test with Bonferroni correction to determine which browser has significant differences from other browsers while comparing users' emotions, attitudes, and behavioral intentions.

In terms of basic emotions toward private browsing, we found that four browsers showed significant differences in three basic emotions, including happiness (X^2= 11.3, df = 3, p=.012), fear (X^2= 16.61, df = 3, p= .0008), and excitement (X^2= 10.97, df = 3, p=.012). Our post-hoc analyses reveal that Firefox's Private window (p=.007) and Safari's private browsing (p=.025) evoked more feelings of happiness than Edge's InPrivate mode (see Figure 5.5). Moreover, Chrome's Incognito mode provoked more fearful feelings in participants than Edge's InPrivate mode (p=.038) and Safari's Private browsing (p=.016). On the other hand, Firefox's Private window provokes more excited feelings in older participants than Edge's InPrivate mode (p=.009).

For privacy-related emotions, the results only found significant difference in feeling of being censored (X^2= 12.37, df = 3, p=.006). As shown in Figure 5.5, Chrome's Incognito mode provoked more emotions of being censored than all other browsers (Firefox's Private window, p=.037; Edge's InPrivate mode, p=.024; Safari's Private browsing, p=.002). Furthermore, our result shows a significant difference in participants' attitudes toward private browsing (X^2= 12.37, df = 3, p=.006). Participants reported lower level of negative attitudes toward Firefox's Private window than Chrome's Incognito mode (p=.028). Yet there is no significant difference in intentions to use private browsing mode.

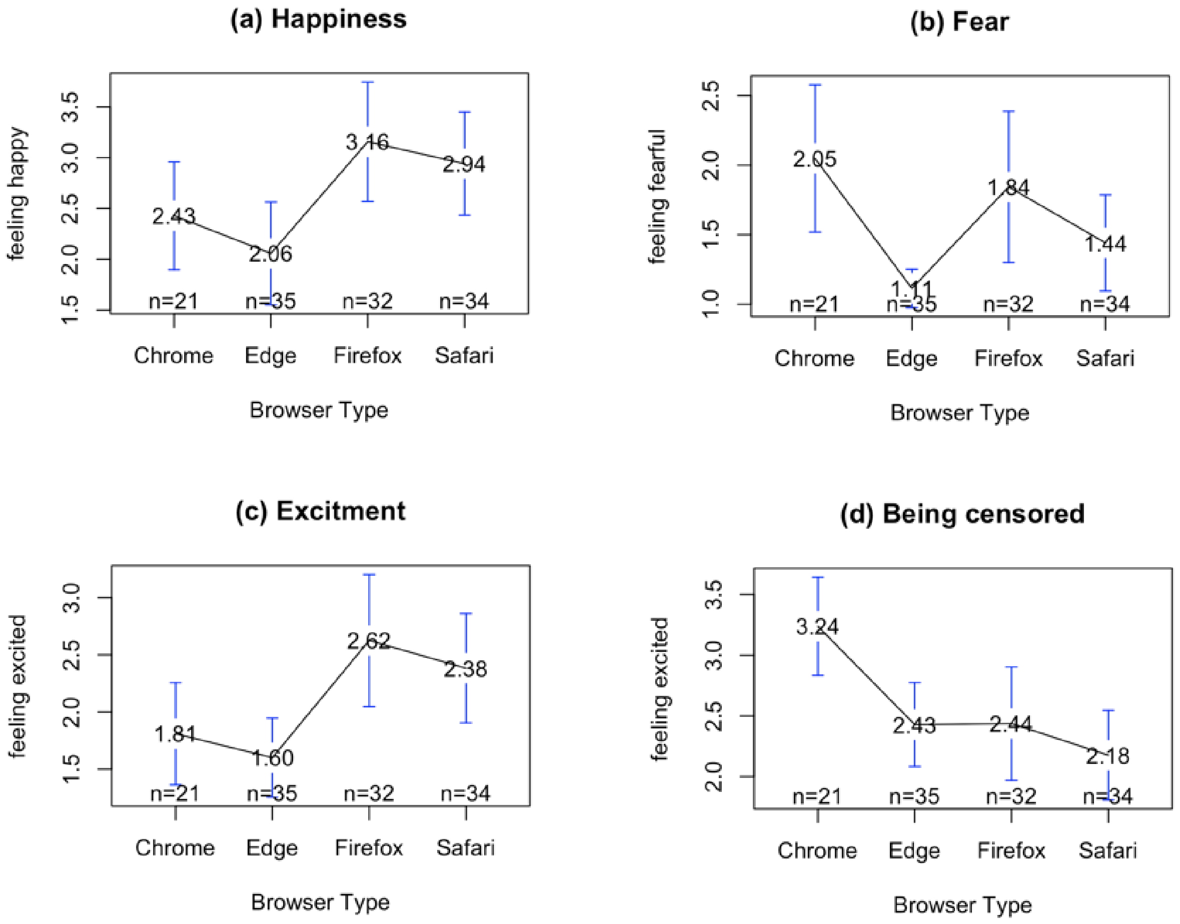


Figure 5.5: Mean of basic emotions by browsers

5.3.4 Emotional effect on attitudes toward private browsing

To examine emotional effects on users' attitudes toward and intentions to use private browsing mode, we conducted linear regression analysis by employing Generalized Linear Model (GLM) in R. Considering that our variables are not normally distributed, GLM model is particularly useful because it can transform the response variable by defining the link function. The 'identity' link function is adopted in the model due to the continuous nature of our variables.

The GLM model for attitudes includes 6 predictors of basic emotions and 7 predictors of privacy-related emotions by controlling browser types, age, gender, and users' prior experience with private browsing. As shown in Table 5.7, I found no significant effects of negative emotions on users' attitudes toward private browsing. Hence, the second hypothesis that negative emotions provoked by private browsing mode will adversely influence users' attitudes toward private browsing (H2) is rejected. In addition, the result also reveals that older participants who are younger and have used private browsing mode showed more positive attitudes toward it.

5.3.5 Emotional effect on behavioral intention to use private browsing

The third hypothesis is that negative emotions provoked by private-browsing mode will adversely influence users' intentions to use private browsing (H3). To test this hypothesis, the second GLM model is conducted to examine emotional effects on older users' behavioral intention toward using private browsing. The second model is similar to the first one except for adding users' attitudes toward private browsing.

The results show that the feelings of 'excitement' are the only significant positive predictor of participants' intention of use. That is, participants who felt more excited toward the interface would be more inclined to use it. However, the negative emotions do not have significant impacts on participants' behavioral intention. Hence, H3 is rejected.

5.3.6 Attitudinal effect on behavioral intention to use private browsing

Our fourth hypothesis is that users' negative attitudes toward private browsing will adversely influence users' intentions to use private browsing (H4). The regression analysis indicates that participants who showed more negative attitudes toward private browsing mode would also indicate less intention to use it. Thus, H4 is supported.

Table 5.7: GLM models of emotional impacts on attitudes toward and behavioral intention to use private browsing mode

	Model 1: Attitudes		**Model 2: Intention to use**	
	Beta	**t-value (*p*)**	**Beta**	**t-value (*p*)**
Intercept	10.12	4.53 (p<.0001)	4.46	1.57 (*p*=.120)
Basic emotions				
Happy	.137	1.46 (*p*=.148)	.144	1.30 (*p*=.196)
Sad	-.023	-0.07 (*p*=.947)	-.162	-0.41 (*p*=.680)
Fearful	.045	-0.21 (*p*=.834)	.058	0.03 (*p*=.974)
Angry	-.127	-0.36 (*p*=.718)	-.085	-0.21 (*p*=.836)
Disgusted	-.138	-1.13 (*p*=.260)	.396	1.34 (*p*=.182)
Excited	-.121	-0.55 (*p*=.587)	.330	2.66 (*p*=.009)
Privacy-related emotions				
Feeling hiding something	-.133	-1.12 (*p*=.267)	-.199	-1.43 (*p*=.156)
Feeling watched	.018	0.12 (*p*=.906)	-.173	-0.99 (*p*=.326)
Feeling like a criminal	-.229	-1.45 (*p*=.151)	-.037	-0.20 (*p*=.844)
Feeling unique	-.080	0.77 (*p*=.444)	-.118	-0.97 (*p*=.335)
Feeling public	-.276	-1.92 (*p*=.057)	.180	1.06 (*p*=.291)
Feeling vulnerable	-.171	-1.02 (*p*=.312)	-.173	-0.88 (*p*=.379)
Feeling censored	.105	0.85 (*p*=.396)	.069	0.48 (*p*=.630)
Browser type (ref.: Chrome)				
Edge	.465	1.30 (*p*=.198)	-.539	-1.28 (*p*=.202)
Firefox	.164	0.44 (*p*=.664)	-.447	-1.02 (*p*=.310)
Safari	-.049	-0.13 (*p*=.894)	-.466	-1.09 (*p*=.280)
Demographics				
Age	-.085	-2.69 (*p*=.009)	-.026	-0.69 (*p*=.490)
Gender (Male)	-.172	-0.78 (*p*=.437)	-.293	-1.14 (*p*=.257)

Table 5.7 (cont.)

	Model 1: Attitudes		Model 2: Intention to use	
	Beta	**t-value (*p*)**	**Beta**	**t-value (*p*)**
Experience with private mode (ref.: Don't know)				
Use private mode	.655	2.22 (*p*=.029)	-.069	-0.20 (*p*=.846)
Don't use private mode	.169	0.52 (*p*=.608)	-.562	-1.47 (*p*=.144)
Attitudes toward PB	--	--	.435	4.77 (*p*=.0003)
F-value	F (20,101) = 2.16, p=.007		F (21,100) = 4.87, p<.0001	
R^2	.299		.505	

5.4 Discussion

Emotion is an essential consideration in the use of privacy-enhancing features since it not only has immediate but also consistent influences across time (Tractinsky et al., 2006). Accordingly, studying emotional impacts on the acceptance of privacy-enhancing features is important to usable privacy literature. In this study, I used private browsing mode as a case study and examined whether private browsing mode would elicit uses' emotions, which further affect their use of private browsing mode by conducting an online survey experiment. Next, I discuss the findings and applications to the design of privacy-enhancing features for older users.

5.4.1 Users' emotions provoked by private browsing

Private browsing not only provokes positive but also negative emotions in users. When compared to public browsing mode, our findings show that users feel more private, safer, unique, and less being watched in private browsing mode. However, users also feel more fearful, like a criminal, and hiding something while using private browsing mode, which supports our hypothesis (H1). These findings further indicate that private browsing mode provokes two conflicting feelings in users. On the one hand, private mode elicits feelings of privacy and safety; on the other hand, it elicits users' emotions of feeling fearful, like a criminal, and having something to hide. We think that these conflicting emotions result from the interface design of private browsing mode, which provokes both negative and positive emotions in users. Another possible explanation is that the use of private browsing mode may already have negative association, and therefore influencing users' emotions. Meaning, the request to use private browsing mode itself may be perceived to be a negative behavior and thus influencing their emotions in a negative manner prior to even evaluating the private mode. Therefore, their subsequent emotional response may be elevated after the actual evaluation due to this initial bias. While this explanation needs further investigation and validation, future studies are needed.

5.4.2 Interface design and emotions

Interface design is users' first and most direct interaction with a system, which can determine users' emotions toward the system (Demirbilek, 2017). In this study, we analyzed users' emotions in response to four browsers (Chrome, Firefox, Safar, and Edge), which represent different design styles. One of the main differences between the interface designs of private browsing modes across these browsers lies in their color hues and tones, which range from darker shades to brighter shades. As displayed in Figure 5.6, Chrome's incognito design is the darkest; both Safari and Edge's interface designs use lighter colors. Since the colors used in interface design have critical influences on human emotions (Brave and Nass, 2003), a possible explanation for why Chrome's incognito mode provokes more negative emotions (e.g., feeling fearful, feeling more like a criminal) than other browsers may be because of its use of darker color tone for its interface. On the other hand, when compared to other browsers, Firefox's design elicits more positive emotions (e.g., happiness, excitement) in users although it also uses the darker color tone. This may be due to the use of color purple, which has been evidenced that it can elicit feelings of pleasure (e.g., happiness) and arousal (e.g., excitement) (Valdez and Mehrabian, 1994).

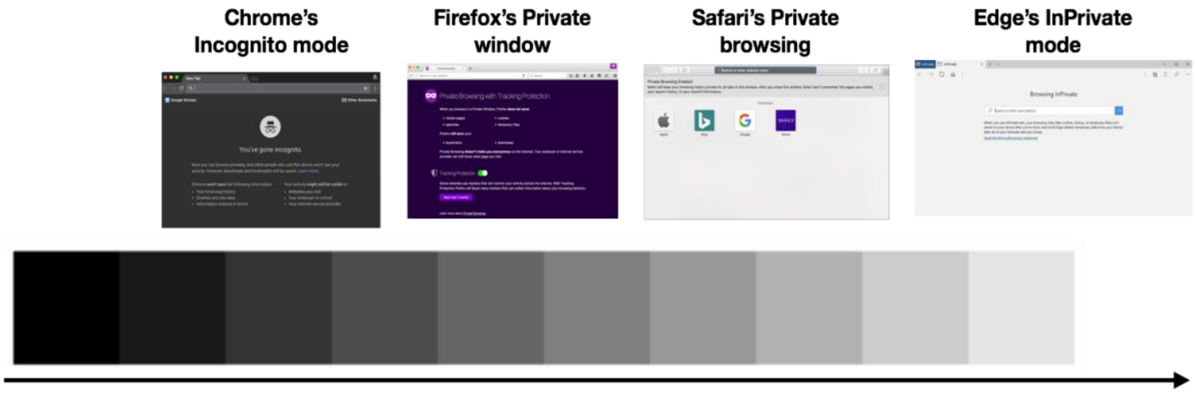


Figure 5.6: Spectrum of color tones for each browser's private browsing mode (dark to bright)

Overall, our results corroborate prior studies' findings that interface design can provoke users' emotions (Brave and Nass, 2003; Kim et al., 2003; Demirbilek, 2017). That is, the use of color or icons embedded in interface design may bear symbolic meanings and may imbue a system with positive or negative associations (Brave and Nass, 2003; Demirbilek, 2017), which may further influence users' acceptance of technologies.

5.4.3 Positive emotions enhance users' acceptance of private browsing

I further investigated how emotions provoked by private browsing mode affect users' acceptance of it. I hypothesized that negative emotions provoked by private browsing mode would adversely affect users' attitudes and their intention to use. Interestingly, our hypothesis for attitudes (H2) is rejected by the results. The findings show that negative emotions do not have significant influences on users' attitudes. Also, positive emotions toward interface show no significant influence neither. These results further suggest that older users' attitudes toward private browsing are not associated with their emotions toward it.

For older users' intention to use private browsing mode, I found that a positive emotion, excitement, is a significant predictor. Older users who feel more excited toward the interface of private browsing are more inclined to use it in the future. In another word, the elicited emotion of excitement may lead older users to their actual use of private browsing mode. This further suggest that positive emotions toward a privacy-enhancing feature may motivate users to adopt it, which corresponds to the idea that design works better when it can elicit positive emotions (Norman, 2004).

5.4.4 Implication of findings

Based on our findings, when a privacy-enhancing feature elicit more positive emotions in older users, they are more likely to adopt it. On the other hand, the negative emotions elicited by the interface design do not necessarily deter older users' behavioral intention. Also, older users who show more positive attitudes toward private browsing will be more inclined to use it. Therefore, if the goal of the design is to enhance older users' use of a privacy-enhancing feature, then designers should consider eliciting positive emotions and attitudes in older users.

Furthermore, although negative emotions have no significant prediction on older users' behavioral intentions, the findings do reveal that certain interface design styles of private browsing mode can elicit certain negative feelings in users, which may come from the negative social connotations for private browsing. Thus, the design of privacy-enhancing features may encounter an inherent challenge because privacy-seeking behavior may have prior, negative connotations in a given cultural context (Solove, 2008). I suggest that privacy-enhancing features should adopt positive interface design to allow older users to be aware of being in private state while not elicit their negative emotions.

5.4.5 Limitations and future research

I acknowledge there are some limitations in this work. First, our findings may only apply to the specific sample group and cultural context because we only recruited U.S. participants via an online crowdsourcing platform. For example, people with different cultural backgrounds may perceive interface design elements (e.g., meaning of color tones) in alternative ways. I suggest that future studies can replicate this current study in different cultural contexts and further compare the results. In addition, the generalizability of the results to other privacy-enhancing features may be limited since I only focused on private browsing in this study. I recommend future research to adopt a similar approach to investigate other types of privacy-enhancing technologies, such as anonymous browsers, privacy notifications, or search engines.

Chapter 6. Usability Study of Tor Browser from Older Users' Perspective

6.1 Introduction

When designing Privacy-Enhancing Technologies (PETs) for older adults, it is important to consider the usability aspect of the technology due to the natural decline in older users' physical and cognitive capabilities. However, existing PETs usually require the application of certain computer knowledge or skills, which can be too difficult or complicated for older users. In addition, the complicated design of PETs may lead users to engage in high privacy-risk behaviors due to the users having a false sense of security, as well as a lack of understanding of the tool (Gao et al., 2014). Therefore, it is important to understand the usability challenges and problems that hinder older users' adoption of PETs. In this study, we select one of the popular online privacy-enhancing browsing tools, Tor Browser, as our case study.

Tor Browser is a browsing tool that is supported by Tor network, which is a free and open global network that provides routing services to Internet users around the world. According to Tor Metrics (Tor Project, 2018), around 2 million users utilize Tor for online browsing every day. As mentioned in Chapter 2, Tor network provides users online anonymity by routing traffic through three volunteer-run nodes, including guard, middle, and exit nodes. Each node only knows the identities of the previous sender and the next receiver. Thus, no node knows the source (who sent it), the subject (what was sent), and the destination (where it was sent) of a message. When the traffic reaches the exit (last) node, the plain text of the message is delivered to the final destination.

For instance, when Alice sends an online message to Bob, her information will not be directly sent to him; instead, it will travel through three different relay nodes. Since

Alice's message is embedded in multiple encryption layers, each node can only peel one layer and move her message along to the next node. In this way, Alice and Bob can exchange or browse information anonymously (Figure 6.1). Also, a proxy server and a client can connect with each other without knowing each other's IP addresses via Tor. With the support of Tor network, Tor Browser provides the highest level of online anonymity and privacy compared to the built-in private browsing mode offered by other browsers (Table 6.1).

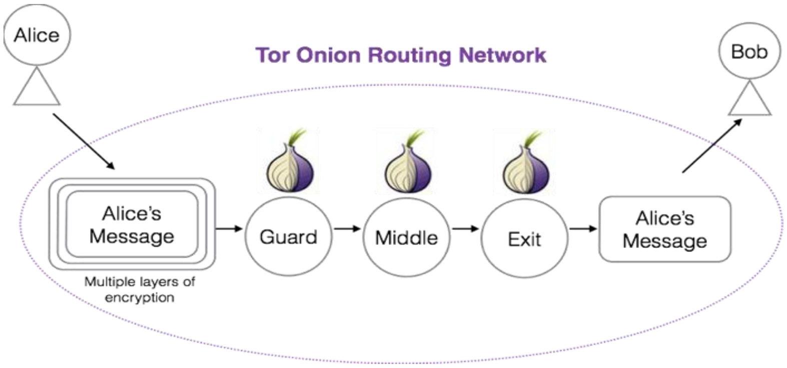


Figure 6.1: Sending Alice's message to Bob via Tor network

In Tor Browser, users can use a component called Tor Launcher to select whether or not to configure a proxy and bridge before connecting to Tor at the beginning. Furthermore, users' can see and control their routing bath via Tor button extension for each web page. In order to protect users from potential eavesdropping by malicious exit nodes, Tor Browser automatically includes the HTTPS Everywhere to encrypt users' traffic. The add-on function NoScript is also included in Tor Browser to prevent Cross-Site Scripting (XSS) attacks, which allow an attacker to steal users' authentication credentials by adding malicious code from one site onto a different site. Table 6.2 exhibits an overview of components on Tor Browser, which is summarized from a design document by Perry et al. (2018).

Table 6.1: Privacy functions of anonymous browsers and private browsing mode

Privacy features	Tor Browser	Typical private browsing mode
No browsing history	Yes	Yes
No auto-filled form for search or login information	Yes	Yes
No passwords are stored	Yes	Yes
No cookies are stored	Yes	Yes
No cache files are stored	Yes	Yes
No list for downloaded files	Yes	Yes
Hidden IP address	Yes	No
No browser extension	Yes	Depends on the browser
Level of network anonymity	High	Low

Table 6.2: Overview of components on Tor Browser

Components	Function
Tor Launcher	Provides graphic user interface for users to configure and control the underlying operation process of Tor network.
Torbutton	An extension to augment users' browsing behavior and provide an overview to users about the routing path for each web page.
HTTPS Everywhere	Encrypts users' traffic and protects users from eavesdropping attacks by potential malicious Tor exit nodes.
NoScript	Protects users from potential Cross-Site Script attacks
Pluggable	Provides censorship circumvention in areas in which the Tor network is blocked by IP addresses or by protocol fingerprinting.

However, like any other PETs, Tor Browser requires that users have a certain level of computer knowledge or understanding. Also, previous user studies have identified several usability challenges and problems with Tor Browser (Lee et al., 2017; Norcie et al., 2012; Gallagher et al., 2018). When adopting a new technology, older users may encounter even more difficulties and confusion than their younger peers because of natural changes in cognition and vision entailed in the aging process (Fisk et al., 2009; Hawthorn, 2000; Arch, 2009). Yet, as far as we know, there is no user study focusing on older users' adoption of Tor Browser. Thus, in this study, we will examine the usability of Tor Browser from the perspective of older users. The study aims to answer the following research questions:

- RQ1: what types of usability challenges and problems might older users encounter while using Tor Browser?
- RQ2: what are older users' behavioral responses when they experience usability challenges and problems on Tor Browser?

Based on our findings, we will further provide solutions for each usability consideration. Next, we will review the most related work on the usability of Tor Browser. Then, we will describe our research method and present the findings. Subsequently, we will discuss the results and the potential usability solutions.

6.1.1 Prior literature in usability of Tor browser

A great number of studies have investigated Tor from a technical perspective. However, there has been little research when it comes to user experience of Tor. In the following subsections, we will first review previous works related to the usability of Tor. Then, we will exhibit the findings regarding how users utilize Tor based on prior research.

6.1.1.1 Usability of Tor Browser

The user studies of Tor can be categorized into two types: those dealing with the network level, and those dealing with the interface level. For the network level, one of the usability issues is the latency of request (Brecht et al., 2011). Due to the design of the network, users may experience slowness while requesting access to the web page. Fabian et al. (2010) found that the added latency causes users to become frustrated and cancel requests and prevents user adoption of Tor. Given the negative impact of latency on user experience, improving the latency within the Tor network has been a significant concern of Tor developers (Dingledin and Murdoch, 2009). In addition, Khattak et al. (2016) investigated the quality of web browsing via Tor network. They found that 1.3 million IPv4 addresses and around 3.67% of the Alexa top 1,000 websites either blocked Tor users or offered them degraded services. The inaccessibility of web pages via Tor network may reduce the quality of user experience and further discourage its usage.

In terms of the user interface of Tor, one of the very first studies was conducted by Clark et al. (2007). The study examined four configurations of Tor software (e.g., Vidalia, Privoxy, Torbutton, and FoxyProxy) by performing a cognitive walk-through. Their results showed that none of the tools had satisfactory usability. They thus proposed changing the user interface to improve the configuration of Tor software. However, since Tor has utilized the Tor Browser as the user interface for the Tor network, these improved configuration tools are no longer applicable.

For the Tor Browser, Norcie et al. (2012) investigated issues experienced by individuals installing and using the browser by conducting a laboratory user study. They interviewed 25 undergraduate students and discovered that 64% of the participants encountered various problems while installing and using the Tor Browser. The usability problems of Tor Browser revealed in their study include difficulties in installation, difficulty distinguishing between Tor browser and Firefox, and browsing delay. In their follow-up study, Norcie et al. (2014) evaluated the effectiveness of their proposed interface solutions and found statistically significant usability improvement for most issues. Another study by Lee et al. (2017) examined the usability of the Tor Launcher that configures Tor Browser's connections. They found that users had difficulty understanding the technical terms on the Tor Launcher, as it did not provide appropriate feedback, thus resulting in users' frustration and errors. They further presented interface changes for the Tor Launcher that would effectively address these challenges. A recent user study of Tor Browser conducted by Gallagher et al. (2018) examined user experience of the Tor Browser in a naturalistic setting for routine online tasks by conducting a one-week diary study with 19 undergraduate students. Their results corroborate prior research that the browsing delay, differential treatment, and inaccessibility of webpages frustrate use of the browser. Furthermore, they also discovered several new usability challenges that led users to abandon the use of the Tor Browser, such as restricted access due to geolocation of the relay, confusion toward the web search engine, and missing common features on the browser. Table 6.3 exhibits an overview of the usability issues identified in previous studies.

Table 6.3: Overview of usability issues on Tor

Aspect of Tor	Identified Usability Issue	Identified by Research
Network	Latency of network[5]	Dingledin & Murdoch, 2009; Brecht et al. 2011; Fabian et al., 2010
Installation / Configuration (Tor Launcher)	Overall difficulties in installation	Norcie et al., 2012
	Unfamiliar technical terms	Lee et al., 2017
	Missing information and too many choices for configuration (proxy and bridge)	Lee et al., 2017
	Bad recovery from failed connection	Lee et al., 2017

[5] Please see further explanation of network latency in Appendix D.

Table 6.3 (cont.)

Aspect of Tor	Identified Usability Issue	Identified by Research
Browsing quality (Tor Browser)	Browsing delay / latency	Norcie et al., 2012; Gallagher et al., 2018
	Differential treatment	Khattak et al., 2016; Gallagher et al., 2018
	Inaccessibility of web pages	Khattak et al., 2016; Gallagher et al., 2018
	A lack of support for specific operations (e.g., stream contents)	Gallagher et al., 2018
	Missing common features (e.g., bookmarks, password saving capabilities)	Gallagher et al., 2018
	Restricted access or customization by geolocation	Gallagher et al., 2018
	Confusing web search engine (Duckduckgo)	Gallagher et al., 2018
Other	Confusion in distinguishing between Tor Browser and Firefox	Norcie et al., 2012
	Confusing operation message	Gallagher et al., 2018

6.1.1.2 User of Tor Browser

As indicated by prior research (Gallagher et al., 2018), an understanding of users' characteristics, attitudes, and needs is beneficial to improving user experience of Tor Browser. The first effort contributing to this aspect was performed by McCoy et al. (2008). Their study examined the traffic from an entry guard and an exit node and found that users sent a large amount of sensitive information via the Tor network in plaintext.

Another interview study conducted by Forte et al. (2017) discovered that some contributors of open collaboration projects (e.g., Wikipedia) utilized Tor to protect themselves from certain risks, such as surveillance, harassment, potential violence, and reputation loss. In addition, Gallagher et al. (2017) examined users' mental models of Tor Browser by performing an interview study with 17 participants. They found that expert and non-expert users not only utilize Tor in distinct ways but also exhibit differences in understanding of Tor operation and threat model. They also pointed out that the misunderstandings of non-expert users may endanger personal anonymity because of a false sense of security. Similarly, Winter et al. (2018) conducted a survey study to understand users' mental models of onion services. Their findings reveal that users have difficulty understanding onion services and encounter issues in determining the authenticity of onion services. On another note, a survey study by Huang and Bashir (2016) uncovered the intrinsic and extrinsic motivations of Tor volunteers and further indicated the difficulties faced by the global volunteers.

6.1.2 Research gap in current user study of Tor browser

In the past decade, prior user studies have contributed to identifying several usability challenges and problems with Tor at both the network and interface level. Nevertheless, to the best of our knowledge, there is no user study focusing on older users' adoption of Tor Browser. Since older users' needs for technology are distinguishably different from those of their younger counterparts, in this study, we examine two aspects of older users' use of Tor: 1) what types of usability challenges and problems older users may encounter while using Tor Browser; and 2) what older users' behavioral responses are when they face usability challenges and problems on Tor Browser.

6.2 Method

This study aims to evaluate the usability of Tor Browser with older adults by conducting an in-lab user study, which has been approved by the University of Illinois' Institutional

Review Board (IRB). In the following subsections, we describe the rationale of our study design and procedure, details of participant recruitment, and approaches used for data analyses, respectively.

6.2.1 Study design

Users' adoption of privacy-enhancing browsers is usually driven by the specific needs or motives (Gao et al., 2014). In order to simulate older users' use of Tor Browser in the real world, we designed a public library scenario in which users are using a computer in a public library and a librarian whom they have known for a while will come and introduce them to Tor Browser. This scenario was particularly designed to provide older users with a motivation to use Tor Browser. In addition, considering that older users are more likely to adopt a new tool if it is introduced by a trusted person, we specifically emphasized that the browser was introduced by a librarian that the older users knew. To help participants engage more fully with the scenario, we designed a short conversation and had a user-librarian role-playing with participants.

6.2.2 Study procedure and instrument

To evaluate the usability of the Tor Browser, we designed a 3-phase user study, which included a pre-testing survey, a usability test, and a post-testing interview. In the pre-testing session, participants received an email 24 hours prior to the usability session, which asked them to answer a short survey questionnaire regarding their general use of the Internet, prior experience with online privacy, computer proficiency, general health, and demographics. After an introductory scenario, participants were instructed to perform five tasks to test Tor Browser, including: 1) installing Tor, 2) logging to an email account, 3) getting online news, 4) searching for a flight ticket, and 5) checking their browsing history before leaving. Then, we conducted a post-testing interview in which participants were given a short questionnaire to evaluate the overall usability of the browser, and then the researcher conducted a semi-structured interview to probe into participants' perceptions and behavioral intentions toward Tor Browser. At the end of the session, researcher explained the operation and functionality to participants and answered their questions if they had any. Each usability session took approximately 60 minutes. We next describe the details of each task.

- Task 1: Installation of Tor browser

Participants were given instructions about the installation of the browser. If participants encountered difficulties installing the browser, they could ask for help from researchers. Researchers would offer participants help if they did not complete the installation in 15 minutes but otherwise did not actively offer assistance. After installation, participants were asked open-ended questions to evaluate the usability of the browser.

- Tasks 2-4: Logging into email, getting online news, searching for flight tickets

To test the usability of the browser, participants were asked to perform three common online activities on the browser, including logging into an email account, getting online news, and searching for a flight ticket (Purcell, 2011). For the email login task, participants were asked to log into an email account provided by the researcher instead of their own email account. After each activity, participants were asked open-ended questions to evaluate the usability of the browser.

- Task 5: Checking browsing history before leaving

Subsequently, participants were given a scenario in which they had finished their online activities in the library and were about to leave. We asked participants to describe their strategies for checking if their browsing history is cleared. If participants clearly stated that they did not know what to do, the researcher would give participants hints so that they could continue with the task. Additionally, the researcher asked participants several open-ended questions to assess the usability of the browser.

6.2.3 Participants

In this study, I recruited participants who had no prior experience with Tor Browser but have used the Internet at a regular basis. A total of 24 participants were recruited via flyers from senior centers, local chapters, and assisted living. Participants who were interested in the study contacted the researcher via email. Then that researcher sent out a confirmation email to schedule a time to meet with participants. All usability testing session were conducted in two labs; one located at Midwest University and the other located in a retirement community collaborating with Midwest University. Each participant was given $20 cash in compensation after completing the study.

For demographics, the average age of participants is 76 years old and 66.7% (n=16) of participants are female. 87.5% (n=21) of participants are Caucasian. For education, 8.3% (n=2) have some college; 12.5% (n=3) have a bachelor's degree; 58.3% (n=14) of participants have a graduate or professional degree; and 16.7% (n=4) have a doctoral degree. As for living status, 41.7% (n=10) of participants reported that they currently live with a significant other; 33.3% (n=8) reported that they live alone; 12.5% (n=3) live with family members; 8.3% (n=2) live in a retirement community; and 4.2% (n=1) live with non-family members. Their average daily use of the Internet is 2.58 hours per day. Detailed information on each participant is exhibited in Table 6.4.

Table 6.4: Detailed demographics of each participant

Participant	Age	Gender	Ethnicity	Education	Living Status
PT001	85	F	white	Graduate or Professional degree	living in a retirement community
PT002	83	F	white	Bachelor's degree	living alone
PT003	75	M	white	Graduate or Professional degree	living alone
PT004	90.7	M	white	Graduate or Professional degree	living with significant other
PT005	72	F	white	Graduate or Professional degree	living with significant other
PT006	91.5	F	Asian / Pacific Islander	Graduate or Professional degree	living in a retirement community
PT007	81	F	white	Graduate or Professional degree	living alone
PT008	77	F	white	Graduate or Professional degree	living alone
PT009	69	F	white	Some college	living with significant other
PT010	81	M	white	Doctoral degree	living with significant other
PT011	58	F	white	Graduate or Professional degree	living with non-family members
PT012	67	F	white	Graduate or Professional degree	living with significant other

Table 6.4 (cont.)

Participant	Age	Gender	Ethnicity	Education	Living Status
PT013	75	M	white	Graduate or Professional degree	living with family members
PT014	83	F	white	Graduate or Professional degree	living alone
PT015	66	F	white	Associate degree	living with significant other
PT016	69	M	white	Some college	living with significant other
PT017	79	F	white	Bachelor's degree	living alone
PT018	66	F	white	Bachelor's degree	living alone
PT019	79	F	Asian / Pacific Islander	Graduate or Professional degree	living with significant other
PT020	81	M	Asian / Pacific Islander	Doctoral degree	living with family members
PT021	78	M	white	Doctoral degree	living with significant other
PT022	76	M	white	Graduate or Professional degree	living with family members
PT023	71	F	white	Graduate or Professional degree	living with significant others
PT024	71	F	white	Graduate or Professional degree	living alone

6.2.4 Data analysis

Qualitative data collected via interviews was analyzed with thematic coding techniques based on Grounded Theory approaches (Glaser and Strauss, 2017). The researcher began coding the qualitative data after completing the data collection. The coding process includes two stages: open and axial. During open coding, the researcher coded the data sentence-by-sentence and generated codes without an initial hypothesis. Subsequently, the researcher grouped codes with similar connotations or connections into overarching categories via axial coding. These categories were utilized to provide insight pertaining to usability problems encountered by our participants. The software Dedoose was used for implementing the qualitative analyses.

6.3 Results

In this study, we designed a public library scenario and asked participants to complete 5 tasks to test Tor Browser, including installation of the program, logging into an email account, getting online news, searching for a flight ticket, and checking their browsing history. Table 6.5 displays the completion rate for each task.

Table 6.5: Completion rate for each task tested on Tor Browser

ID	Task	Completion rate (n=24)
1	Installation of Tor Browser	79.2% (n=19)
2	Logging into email account	58.3% (n=14)
3	Going to news websites	66.7% (n=16)
4	Searching for flight ticket	41.7% (n=10)
5	Checking browser history	20.8% (n=5)

The results show that the task with the highest completion rate is the installation of Tor Browser, followed by going onto a news website, logging into an email account, and searching for a flight ticket. Only one fifth of participants knew where to check their browser history. In the following sections, I will present the usability challenges and problems identified by older participants.

6.3.1 Connect or configure?—confusion during installation

The current version of Tor Browser provides an installation wizard to walk users through the process. Over half of participants (n=16) reported that it was easy for them to install. However, there are 9 participants who stated that they were somewhat confused by the interface. The most common thing that caused confusion was that participants did not know about private networks and proxy servers. They were not sure if their network was private or not. A participant expressed his confusion about the choices between connect or configure.

> *"I'm trying to decide if this particular browser is set up that requires a connect or whether I should go to configure… It is clear what we need to connect for, up to a point, such as the country, but it's not so clear about the private network that requires a proxy… because I'm not familiar here, I'm not sure which one to go with at this stage."* (PT003, M, 75)

Another participant who chose to configure the network was not sure what proxy was. When she chose to use proxy to connect to the network, she thought that she should put in her personal email information in order to connect to the network (Figure 6.2).

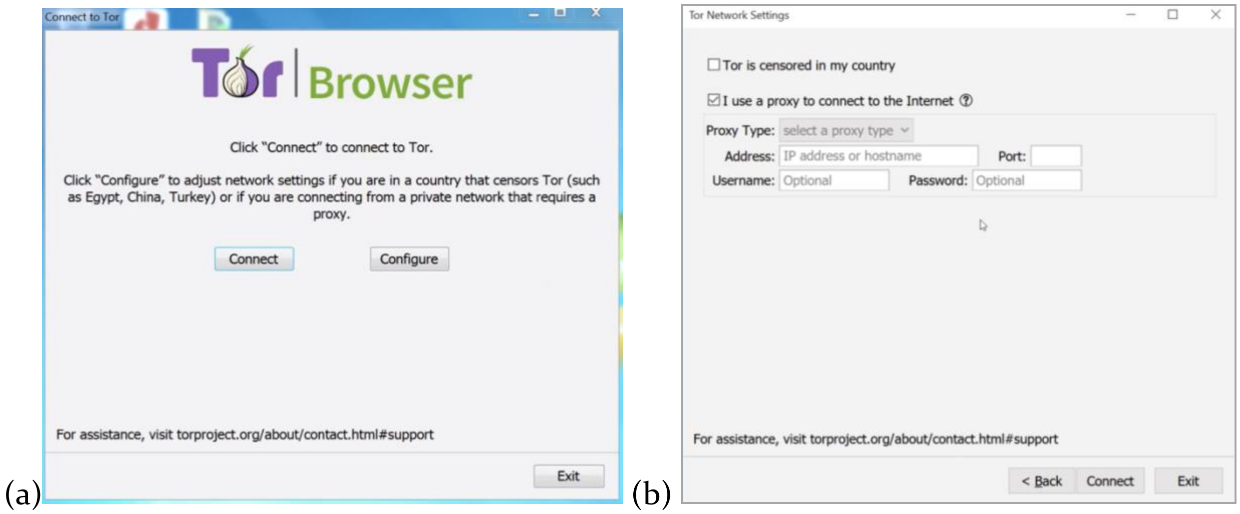
> *"I'm not sure what proxy means at this point… in order to get to the browser there has… like an email address, name and the password. Trying to figure out how to… get into the library system."* (PT019, F, 79)

When asked what the most difficult aspect of using the browser was, she pointed out that both the instructions for the proxy and the term 'configure' are confusing.

> "*All those instructions about the proxy and the proxy name and then…the vocabulary configure and connect because I think a person who is not familiar with the…language might not know what configure means… That proxy part… wasn't quite clear and again, without somebody to explain at the beginning how to use it might be a little difficult…especially for seniors."* (PT019, F, 79).

When participants didn't know the concepts of private networks and proxy, most decided where to 'connect' based on the first condition mentioned, i.e., that of the country in which they were located. For instance, a participant was asked about the decision in installation and she answered: "I'm not in a country that says I can't do it. And I can't remember what the other one was really about…" (PT014, F, 83). The participant did not recall the private network condition, which further suggests that the participant only made the decision based on the one condition that she could understand.

These findings further suggest that technical terminologies such as private network and proxy are confusing and difficult to understand for older users. This could also lead older users to make an erroneous decision on Tor network setting, which may expose older users and further put them in danger. Therefore, it is important to help older users understand and decide whether they are in a private network to prevent erroneous decisions.



Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit torproject.org/about/contact.html#support

□ Tor is censored in my country

☑ I use a proxy to connect to the Internet

Proxy Type: select a proxy type

Address: IP address or hostname Port:

Username: Optional Password: Optional

For assistance, visit torproject.org/about/contact.html#support

Figure 6.2: Tor Browser installation wizard. (a) the dialogue that allows users to choose to connect or configure; (b) the network setting if the user decided to use proxy

6.3.2 Frustration caused by warning messages

Since Tor Browser has more security measures (in the form of built-in features and add-ons) to protect users' privacy, it also generates more warning messages to ask for users' confirmation.

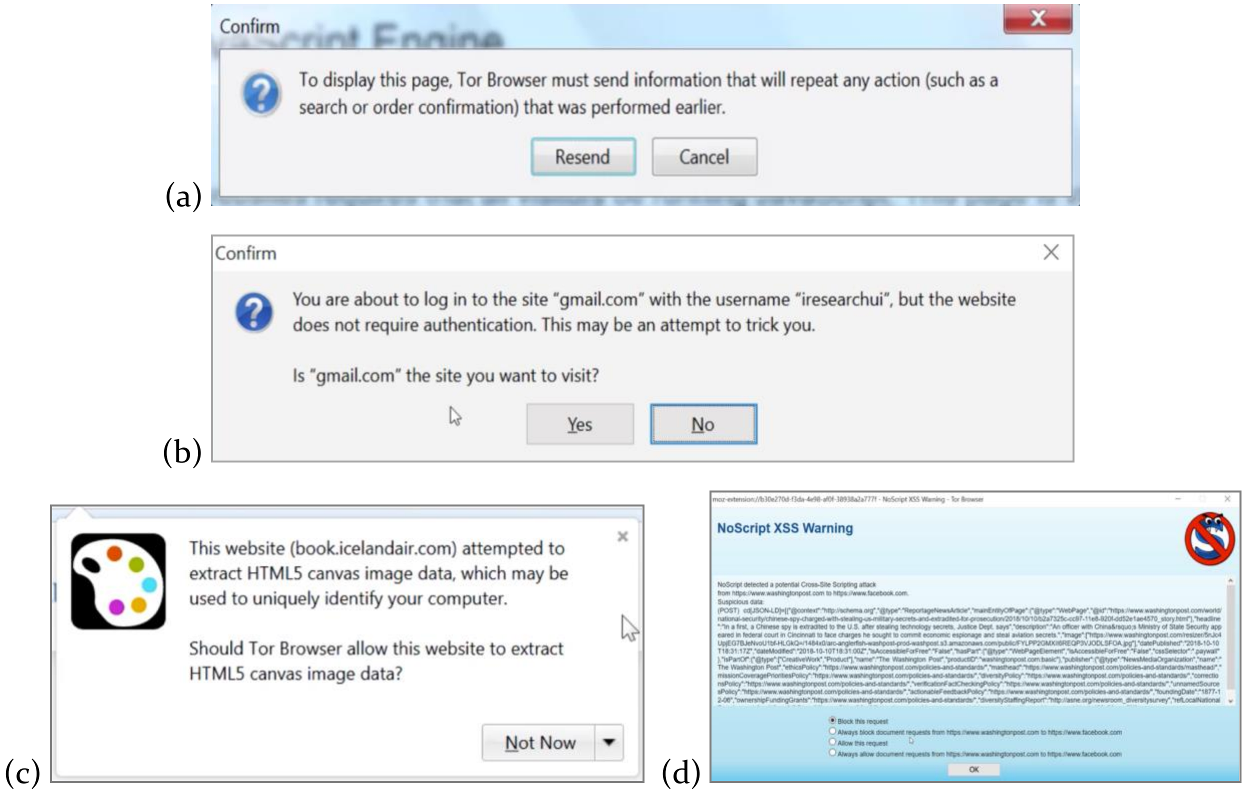
As shown in Table 6.6 and Figure 6.3, participants were likely to encounter 3 types of warning messages, including Confirmation dialogue, HTML5 Canvas Image Data Extraction[6], and NoScript Cross-site attack[7]. While these messages were meant to inform users about the situation, our data shows that older users often found these messages confusing and difficult to understand. Next, I discuss in detail the usability issues caused by warning messages.

[6] Please see further explanation of HTML5 Canvas Image Data in Appendix D.

[7] Please see further explanation of NoScript Cross-site attack in Appendix D.

Table 6.6: Warning messages of Tor Browser shown in this study

Warnings / Confirmation	Pop-up situation	N (n=24)
Confirmation Dialogue	Type 1-participants put their full email account into the search bar. Type 2- search for flight ticket	9 (37.5%)
HTML 5 Canvas Image Data Extraction	Go to news or airline sites	11 (45.8%)
NoScript--XSS Attack	Go to news or airline sites	9 (37.5%)


(a)

Confirm

To display this page, Tor Browser must send information that will repeat any action (such as a search or order confirmation) that was performed earlier.

(b)

Confirm

You are about to log in to the site "gmail.com" with the username "iresearchui", but the website does not require authentication. This may be an attempt to trick you.

Is "gmail.com" the site you want to visit?

(c)

This website (book.icelandair.com) attempted to extract HTML5 canvas image data, which may be used to uniquely identify your computer.

Should Tor Browser allow this website to extract HTML5 canvas image data?

(d)

moz-extension://b30e270d-f3da-4e98-af0f-38938a2a777f - NoScript XSS Warning - Tor Browser

NoScript XSS Warning

NoScript detected a potential Cross-Site Scripting attack
from https://www.washingtonpost.com to https://www.facebook.com.
Suspicious data:

```
(POST) cd[JSON-LD]=[{"@context":"http://schema.org","@type":"ReportageNewsArticle","mainEntityOfPage":{"@type":"WebPage","@id":"https://www.washingtonpost.com/world/
national-security/chinese-spy-charged-with-stealing-us-military-secrets-and-extradited-for-prosecution/2018/10/10/b2a7325c-cc97-11e8-920f-dd52e1ae4570_story.html"},"headline
":"In a first, a Chinese spy is extradited to the U.S. after stealing technology secrets, Justice Dept. says","description":"An officer with China&rsquo;s Ministry of State Security app
eared in federal court in Cincinnati to face charges he sought to commit economic espionage and steal aviation secrets.","image":["https://www.washingtonpost.com/resizer/5nJo4
UpjEG7BJeNvoU1bf-HLGkQ=/1484x0/arc-anglerfish-washpost-prod-washpost.s3.amazonaws.com/public/FYLPP2GMXII6REQP3VJODLSFOA.jpg"],"datePublished":"2018-10-10
T18:31:17Z","dateModified":"2018-10-10T18:31:00Z","isAccessibleForFree":"False","hasPart":{"@type":"WebPageElement","isAccessibleForFree":"False","cssSelector":".paywall"
},"isPartOf":{"@type":["CreativeWork","Product"],"name":"The Washington Post","productID":"washingtonpost.com:basic"},"publisher":{"@type":"NewsMediaOrganization","name":"
The Washington Post","ethicsPolicy":"https://www.washingtonpost.com/policies-and-standards/","masthead":"https://www.washingtonpost.com/policies-and-standards/masthead/","
missionCoveragePrioritiesPolicy":"https://www.washingtonpost.com/policies-and-standards/","diversityPolicy":"https://www.washingtonpost.com/policies-and-standards/","correctio
nsPolicy":"https://www.washingtonpost.com/policies-and-standards/","verificationFactCheckingPolicy":"https://www.washingtonpost.com/policies-and-standards/","unnamedSource
sPolicy":"https://www.washingtonpost.com/policies-and-standards/","actionableFeedbackPolicy":"https://www.washingtonpost.com/policies-and-standards/","foundingDate":"1877-1
2-06","ownershipFundingGrants":"https://www.washingtonpost.com/policies-and-standards/","diversityStaffingReport":"http://asne.org/newsroom_diversitysurvey","refLocalNational
```

● Block this request
○ Always block document requests from https://www.washingtonpost.com to https://www.facebook.com
○ Allow this request
○ Always allow document requests from https://www.washingtonpost.com to https://www.facebook.com

Figure 6.3: Warning messages that came up during the tasks. (a) & (b) are confirmation dialogues; (c) is the HTML5 canvas image data warning; (d) is the NoScript XSS warning attack

6.3.2.1 Technical terminologies are difficult to understand

Our results show that over half of the participants did not understand the messages for HTML5 Canvas Image DATA, NoScript XSS Attack, and Access Denied (See Table 6.6). Participants expressed that they did not understand technical terms such as 'HTML5 Canvas Data', and 'Cross-site attack'.

> *"I have no idea what they are (HTML5 Canvas Data message) talking about…"* (PT023, F, 71)

> "*I don't think…it's clear. I'm in a potential cross site scripting attack. Well, I know what attack means, but I have no idea what a cross site scripting attack (NoScript XSS Attack) is…*" (PT014, F, 83)

These technical terms cause participants to feel anxious, confused, and frustrated, especially when participants encounter these messages repeatedly. For instance, a participant got repeated cross-site attack warning messages while trying to search on Tor Browser. She started feeling nervous and was not sure what went wrong with her computer.

> *"Well, it's, um, script again. I don't know, once again, it's telling me there's a problem of some kind and um, again, I'm not really sure. I don't know what the cross-site scripting attack from whatever [website]… Well, It makes me nervous. I mean something's going on that uh, I'm not sure if it's telling me…that my laptop or my browser is being attacked or if uh, this particular account is under attack… There's a problem with the website…*" (PT018, F, 66)

Another participant also felt frustrated about the warning and expressed that he could not understand the message. He suggested using plain language to explain things to users.

> "*Why gave me this thing (NoScript XSS warning)? Listen, …this is your internal note that the user does not understand what this is. Just tell us what it is…… What does that mean? I knew nothing about this. I just …don't know anything about the reason. So tell me why. So…you got the problem that you want (users) to respond to the problem and you need to explain to the user what happened. Don't use too many technology terms here…we don't understand.*" (PT020, M, 81)

Based on our data, older users have difficulty understanding the technical terms, which can result in increased anxiety and frustration. As a result, it is important to make the warning messages as simple as possible for older users.

6.3.2.2 Behavioral strategies toward warning messages

When the technical terms hindered participants' understanding of the messages, we observed that participants used different behavioral strategies to respond to the situation. As shown in Table 6.7, the first strategy most taken is following the default suggestion. Participants would follow the default suggestion because they did not understand what the warning messages meant. A participant expressed that "*In this case it wants me to block it, so… We'll block it, and I come back (to the page)…I don't know what it blocked…*" (PT017, HTML5 Canvas Data). Another participant reported having the same thought: "*Follow what they recommend, I guess… like I said, I don't really understand exactly what (*NoScript XSS Attack*) that is.*" (PT018, F, 66). This finding further indicates that older users who follow the default suggestions do not attempt to understand the warnings.

In addition, our results found that some participants would try to make decisions based on their own reasoning when encountering warning messages. For instance, a participant decided to allow HTML5 Canvas Data Extraction because she thought that it must be something she needed to make the website work. Although she did not know what the warning meant, she still developed her own understanding of the message and made the decision based on her own reasoning instead of following the default suggestion.

> *"I'm usually, um, very hesitant to give anybody any access, so I don't understand. I don't know what HTML5 (Canvas Data) I don't know what it is, but it must be something that I need, so I probably will go ahead and allow. That would be my inclination."* (PT010, M, 81)

Table 6.7: Older users' reactions and behavioral strategies to warning messages

	First reactions	**Behavioral Strategies**		
Warning message	**Don't understand / Don't know**	**Following the suggestion**	**Deciding based on own reasoning**	**Not responding by Closing**
Confirmation Dialogue (n=9)	2 (22.2%)	0	9	--
HTML 5 Canvas Image Data Extraction (n=11)	7 (63.6%)	1	5	--
NoScript--XSS Attack (n=9)	13 (69%)	3	3	3

We also found that some participants decided to block the request because they did not want the website to have access to their data. For example, a participant with prior hacking experience made the decision based on his distrust toward the online entities.

> *"I don't even know what HTML5 Canvas Image data...I couldn't count them because it got me in trouble. It's not necessary for me to do what I want to do because I can get the news someplace else. I'm not going to go someplace where they want to...access and use the data that I enter on the computer. It's not necessary."* (PT022, M, 76)

When participants experienced repeated warning messages, some of them altered their decision based on their own inferences. One participant decided to allow the third party to collect data after encountering repeated NoScript's XSS attack warnings. When researcher asked if there was any particular reason why she changed her decision, she explained: "*Because if I say always block them, I wouldn't get this (page). If I said always allow them, then I might get stuff I didn't want, and I really only want one (only for this website)... Well, it's a request from New York Times. That sounds good. I think I would say allow this request*" (PT014, F, 83). In this case, the participant's decision to allow this request was based on both her trust of the site and her need for access.

The third strategy used by participants was to close the window. A participant reported that she was inclined to close all the pop-ups when she was online: "*It came fast that I'm routinely hitting keys that are run in closing other things all the time. Often close the whole thing by myself*" (PT023, F, 71).

6.3.3 Inaccessibility of websites

While searching news and flight tickets on Tor Browser, 18 out of the 24 participants had their access denied by the websites. Participants felt frustrated and anxious because of this unexpected issue, especially when they tried to access a site that they had used frequently in other browsers. Frustration towards inaccessibility on Tor Browser decreases its usability.

> "*The fact that you can't access travelocity.com, does that have to do with the browser? Okay. Well I mean that's ridiculous... I use (it) regularly. I didn't know if that had to do with your browser, if that just had to do with how you've got everything set up, but then not being able to access certain websites like Orbitz or Travelocity... is like a total disadvantage.*" (PT005, F, 72)

> *"It was easy enough to use, but then you keep getting these 'denied'. So then it's not really easy to use because you can't really use it… If I was using it in a public setting I'd be kind of surprised. Why am I getting all these denied [messages]. And I guess if it's supposed to be for security than it's just saying nothing's secure… So then that just creates anxiety in, oh, I can't search for anything, you know, because it's not secure." (PT012, F, 66)*

One participant further expressed that receiving 'access denied' messages had her wondering if she was using unsecure websites and putting herself at risk.

> *"Because this is keeping…saying that's not a safe site, that's not a safe site…but those seem like pretty common sites and not to be safe. And I've also booked flights before on [the website] or whatever. So this is saying, oh, you know, somebody lurking in the background there. Then I'm thinking, oh, so I've already put myself at risk?" (PT012, F, 66)*

We also found that participants have a strong need to know why access was denied.

> "*What the heck am I supposed to do to fix it by telling me that access is denied? [The message] Doesn't tell me anything. It's like you can't get in there, but I'm not going to tell you why you can't get in there."* (PT015, F, 72)

> *"Oh it is denied… Why are you denying? Why it is denied. What's the reason for deny?"* (PT006, F, 91)

> "*I'm wondering why… Why is it blocked on this server? The Expedia.com as far as I know it was open to everyone so I'm not sure what the reason is…*" (PT018, F, 66)

6.3.3.1 Behavioral strategies toward access denied messages

After experiencing access denied messages, participants were asked about what they would do as a next step. According to the data, five behavioral strategies were adopted by participants (see Table 6.8). Nine of 18 participants tried to use other websites to see if they worked. This was the most adopted strategy by our participants. Participants would not only try other similar sites but would also use search engines that they were familiar with.

> "*Well, when it [access denied message] comes up, what I would do is try something very simple like going back to Google and saying Kayak and see if it gives me anything.*" (PT004, M, 90.7)

> "*I'm thinking it's not letting me indirectly, but maybe if I go through by way of a google search... Now let me try something different. Let me go to google.com to try and search for Expedia...*" (PT011, F, 58)

Table 6.8: Behavioral strategies for access denied messages

Behaviors toward access denied	N (=18)
Try other websites	9 (50%)
Try the search again	5 (27.8%)
Seek help	3 (16.7%)
Leave and use other browsers	3 (16.7%)
Search for the content of the message	2 (11.1%)

Furthermore, five participants, instead of trying different sites, would try the same search again. For instance, a participant indicated that she would try to search again later instead of looking for support.

> *"I would probably say I'll close this, come back to it in an hour, or ten minutes, go get a cup of coffee or something. And then I'd come back and start again. Support, I usually don't use, because my own experience with support has not been particularly good. And nothing is important enough to deal with the confusing messages you get."* (PT002, F, 83)

Additionally, 3 participants mentioned that they would seek others' help to solve the problem. Another 3 participants stated that they would leave and go use other browsers. Only 2 participants tried to find the answer to the problem by searching for the content of the message online.

6.3.4 Unexpected language barrier caused by geolocation

Language barrier is another usability issue that came up during the test. Nine participants (37.5%) reported that they experienced difficulties continuing the task on Tor Browser due to language. Since Tor network is distributed worldwide and the exit node can be in any country, the display of the web page could be in a language other than English. One participant described her experience encountering a different language when trying to log into her email account.

> *"It's fairly simple except that the different language threw me off... It just a surprise that had come up in a different language because you're not expecting it. If you're doing it in English, you just expect straight English, right? You don't expect a different language and there were two different languages in there."* (PT019, F)

6.3.4.1 Behavioral strategies toward the language barrier

When participants faced the unexpected language barrier, their first reaction was to question whether they had done something wrong. For instance, PT009 was wondering if she had mistyped something. After checking the spelling, she was confused and did not know what to do.

> *"I would check that I've not mistyped something. Misspelled it or something... That's in Spanish. I definitely don't want that. Or it's in some other language. I don't know what this is... Now I'm confused. That's not what I want."* (PT009, F, 69)

A participant who was familiar with the interface of her Google email account used the guessing strategy and typed in the information based on her memory of the interface.

> *"In French... I don't know how to change [it]... So I would guess. Let's see how you do it... Well, I guess... (typing) this email address... Okay."* (PT014, F, 83)

Four participants looked for the feature that could change the language on the browser. And 2 participants had no idea what to do with different languages.

Based on these findings, older users feel confused by the unexpected language barrier and are likely to spend a lot of time attempting to change the language, which decreases Tor Browser's ease of use.

6.3.5 Confused by empty browsing history

In the last task, participants were asked to check if their browsing histories were clear on the browser before they left. 62.5% (n=15) of participants did not know how and where to check their browsing history. After given a hint and landing on the menu for browsing history, participants' first reaction was to click on 'clear recent history', yet the item is unclickable. Thus, the next reaction of participants was to click on 'View History Sidebar'. However, as shown in Figure 6.4, there was no browsing history on the sidebar. Participants at this point did not understand why there was no browsing history and were not sure if their browsing history was clear.

> *"I didn't understand why when I checked for flights, it didn't show it as part of my history, so I couldn't get rid of it. That's what I don't understand. Did the browser get rid of it?"* (PT001, F, 85)

> *"Clear recent history... View history... Okay. That might do. Let's see what that is. It doesn't look like that's right. There's nothing here... I don't know."* (PT007, F, 81)

Most participants did not have experience in checking or clearing their browsing history on their own browsers. When checking browsing history, participants expected to see the history and clear it. However, the browsing history shown on Tor Browser was empty, which confused participants. Based on this finding, the current design makes it unclear to older users as to whether or not the history is clear on the browser. Older users need direct confirmation or feedback on the status of their browsing history.

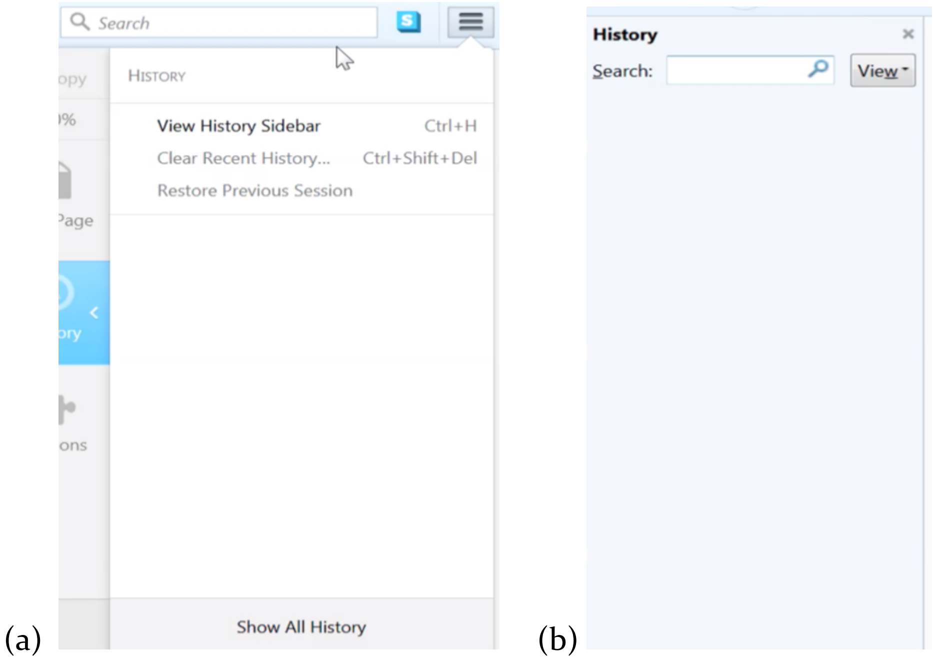


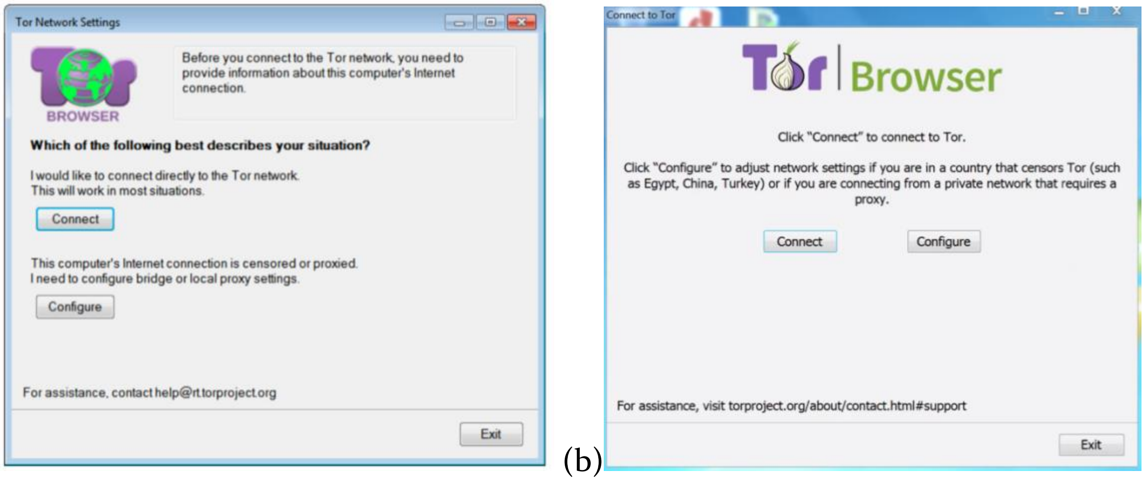
Figure 6.4: Menu for browsing history on Tor Browser

6.4 Discussion

This in-lab scenario-based user study reveals several usability challenges and problems with Tor Browser for older adults that were not addressed in previous studies. Next, we discuss the most prominent usability insights derived from the findings and provide design solutions to solve the corresponding issues and improve the usability of Tor Browser for older users.

6.4.1 Confusion during installation

The installation of Tor Browser is configured via the interface of Tor Launcher. A prior usability study of Tor Launcher (Lee et al., 2017) has pointed out that users usually have difficulties in installing the browser due to being given too many choices, and the use of unfamiliar technical terminologies. Thus, they recommend avoiding technical concepts and leveraging users' existing knowledge (e.g., current country of residence) to guide users through the installation process. After their study, the interface and flow of Tor Launcher has been modified and improved (see Figure 6.5). However, we found that older users are still confused by the terminologies in the latest version of Tor Launcher, such as 'proxy', and 'configure', which corroborates previous findings (Lee et al., 2017). In addition, our results also indicated that older users have difficulty defining private networks. They were uncertain as to whether or not the Wi-Fi of the university or a retirement community is considered a private network, which results in difficulty deciding between connect and configure. The unfamiliarity with the concept of private networks also has older users only relying on the knowledge of country-based conditions to make the installation decision. Basing their choice on one factor may lead to older users making an erroneous decision.



(a)

Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

I would like to connect directly to the Tor network.
This will work in most situations.

This computer's Internet connection is censored or proxied.
I need to configure bridge or local proxy settings.

For assistance, contact help@rt.torproject.org

(b)

Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit torproject.org/about/contact.html#support

Figure 6.5: The interface of Tor Launcher is redesigned. (a) older version; (b) latest version

Usability solution: Assist users in deciding what to choose by asking basic questions. For older users, technical information is useless when it is too difficult to understand. The technical concepts, as mentioned above, should be explained in plain language to older users. In terms of the concept of private networks, one approach is to guide older users to figure out if their Internet connection is on a private network by asking basic questions, such as ‘does your Internet network require passwords’ and ‘is your Internet network monitored by an entity (e.g., a corporate or governmental organization)?’.

6.4.2 Confusing warning messages

Three main types of warning messages showed up during the testing, including Confirmation dialogue, HTML5 Canvas Image Data Extraction, and NoScript Cross-site attack. Our findings indicate that older users find these repeated warning messages difficult to understand, which becomes one of Tor Browser’s main usability issues. According to our findings, older users’ first reaction to the warning messages is confusion. Then they want to know ‘why’ these messages show up, and they try to find out by reading the messages. However, these warning messages do not explain why, but contain many technical terms that confuse older users and make them feel even more frustrated.

Although older users do not understand the messages, we found that they still attempt to tackle the problem in different ways, such as following the default suggestions, deciding what to do based on their own reasoning, and not responding to the message. Yet, when warning messages keep showing up, older users start feeling helpless and do not know what to do.

Usability solution: Provide explanations and reasoning for warning messages. With natural aging, older adults' memory and cognitive capabilities start to decline. Therefore, it is important to make the messages as simple as possible, so older users understand them. When asked how to improve warning messages, the majority (n=14) of participants who experienced warning messages suggested providing more information on why they got the messages and how they can solve the issue. Since older users often have lower confidence (Dunlosky and Hertzog, 1998) or self-efficacy (Wagner et al., 2010) in learning or using unfamiliar technologies, they may think that they have done something wrong with the computer when they encounter warning messages. Therefore, one of the solutions is to provide effective information to explain to older users 'why' the warning messages come up instead of using technical jargon. The instructive information would not only reduce older users' anxiety but may also help them form cognitive schemas of warning messages, which can further enhance their learning and experience of Tor Browser.

6.4.3 Inaccessibility of websites

The inaccessibility of websites has been a notable usability issue of Tor Browser (Khattak et al., 2016; Gallagher et al., 2018). Correspondingly, our findings also suggest that older users are confused and frustrated by the unexpected inaccessibility. In order to complete the tasks, one of the most adopted strategies by older users was to try using different websites. As pointed out by Gallagher et al. (2018), the inaccessibility of Tor Browser is not a technical issue but a political one, because there is no standard way to know who blocks Tor network, which makes this issue more difficult to tackle. Previous studies have suggested several solutions to this issue, such as working with website operators and vendors to make exceptions for Tor, crowdsourcing the list of inaccessible websites, and providing access to sites via archive or cache Internet content (Singh et al., 2017; Gallagher et al., 2018). Yet, from the perspective of older users, these approaches may not reduce their anxiety or frustration when access is denied by the website. Therefore, we propose a different approach that focuses on easing older users' negative emotions and supporting them in completing tasks on Tor Browser.

Usability solution: Explain why the website is inaccessible. In our study, we found that older users often have a strong need to know 'why' their access is blocked by a website. Accordingly, we suggest that Tor Browser provide clear and simple explanations to ease older users' minds when they encounter a website to which access is denied.

Usability solution: Recommend alternative accessible websites. As revealed above, older users are inclined to seek alternative websites to which they can gain access. Therefore, another approach is to recommend other accessible websites based on users' requests on Tor Browser.

6.4.4 Unexpected language barrier caused by geolocation

The practice of tailoring content based on users' IP addresses has been widely adopted by global websites. Thus, with Tor Browser, the delivered content could be displayed in a different language if the user's traffic is routed via an exit node in a country other than where the user is located. Similarly, to a previous finding (Gallagher et al., 2018), older users typically find this unexpected barrier annoying and not user-friendly. In our study, participants ended up spending lots of time figuring out how to change the language setting on the browser or the website. Although Tor Browser enables users to specify the desired country for exit nodes, this change of the default setting requires users to modify the Tor run-time configuration file (torrc), which is complicated and difficult to do, especially for novice users (Gallagher et al., 2018).

Usability Solution: Automatically set the preferred exit node location based on the use of the language. In the study by Gallagher et al. (2018), their proposed solution to geolocation issues is allowing users to easily switch to a preferred exit node location within the set of settings. However, this approach brings up two other issues. First, the level of anonymity and security will decrease due to the reduced number of potential circuits. In other words, users' privacy and security may be compromised to a certain degree. Second, it requires extra effort for older users to know where and how to change the settings. Therefore, we propose that the preferred exit node location be set automatically based on the users' preferred language, which will be specified at the beginning of installation. This way, the number of potential circuits increases, which can minimalize the negative consequences on the levels of anonymity and security. Also, older users do not need to acquire any additional knowledge to change the settings.

6.4.5 Confusion caused by an empty browsing history

Since Tor Browser's default setting is private mode, the browser does not record users' browsing histories. Therefore, the browsing history is empty. However, we found that this default design confuses older users because of a lack of understanding of the operation of Tor Browser.

Usability solution: Showing a clear message to let users know the browsing history has been cleared. While checking their browsing history, older users expect to see the history and clear it manually, just like they do with other browsers. That is, older users need direct confirmation or feedback to know that the history has been cleared. So, instead of just showing the empty history box, the browser should show a message to confirm that the history has been cleared.

Overall, the usability challenges revealed in this study can be categorized into two types, the general and specific challenges. The general challenges are the usability issues that have been identified in prior studies, including technical terminology (Lee et al., 2017), inaccessibility of website (Khattak et al., 2016; Gallagher et al., 2018), and inconveniently customized contents by geolocation (Gallagher et al., 2018). The specific challenges are newly discovered in this study, such as warning messages and confusing interface for reviewing browsing history. However, it is important to note that these specific challenges may not be only limited to older users. Younger users may also encounter similar usability challenges. Consequently, further investigation and comparative studies are needed to confirm whether these issues are age-related.

6.4.6 Limitations and future work

It is important to note a few limitations of this study while applying the generalizability of the findings. First, the usability testing was conducted in a laboratory setting with a designed scenario, and participants only used the browser for a short period of time. Although our scenario simulated potential use cases in the real world, the laboratory setting may still have impacted older users' behaviors (Franz et al., 2015). Therefore, we recommend future studies observe older users' usage of Tor Browser in a natural setting for a longer period of time in order to get first-handed neutralized data.

In addition, the sample was rather small and homogenous in terms of gender, education, and ethnicity. Since the study was performed in the U.S., older users in the U.S. may have had more exposure to new technologies than others living outside the US. Additional studies are needed to research the usability aspects in other populations.

Chapter 7. Conclusion

7.1 Summary of findings

This thesis research investigates online privacy-enhancing browsing experience from older adults’ perspective. As shown in Figure 7.1, the findings of the thesis show the importance of three elements on older users' online privacy-enhancing behaviors, including knowledge, psychological state, and usability of the technology. Overall, the findings indicate that older users' knowledge plays a significant role in older users' actual online privacy protection behavior in their daily life (Chapter 4). In addition, the findings also reveal the phenomenon of ‘Privacy Divide' among older adults (Chapter 4).

Regarding the psychological state, certain types of negative emotions can be elicited by the interface design of private browsing mode in older users (Chapter 5). However, the elicited emotions are not significant predictors for older users' attitudes toward private browsing mode (Chapter 5). When it comes to the behavioral intention for private browsing mode, the result shows that older users who exhibit more positive emotions toward private browsing mode are more likely to adopt it (Chapter 5). Also, older users who display more excited emotion elicited by private browsing mode will be inclined to use it more often in the future.

I further examined the usability aspect of the Tor Browser, a privacy-enhancing browsing tool, from older users' perspective (Chapter 6). The findings point out several usability issues for older users, such as the unfathomable technical terminologies in warning messages, the inaccessibility of websites, and the confusing communication of browsing history. Based on these findings, I propose applicable usability considerations (Chapter 6). Next, I will review how these findings answer my three main research questions and the design application for privacy-enhancing browsing experience for older users.

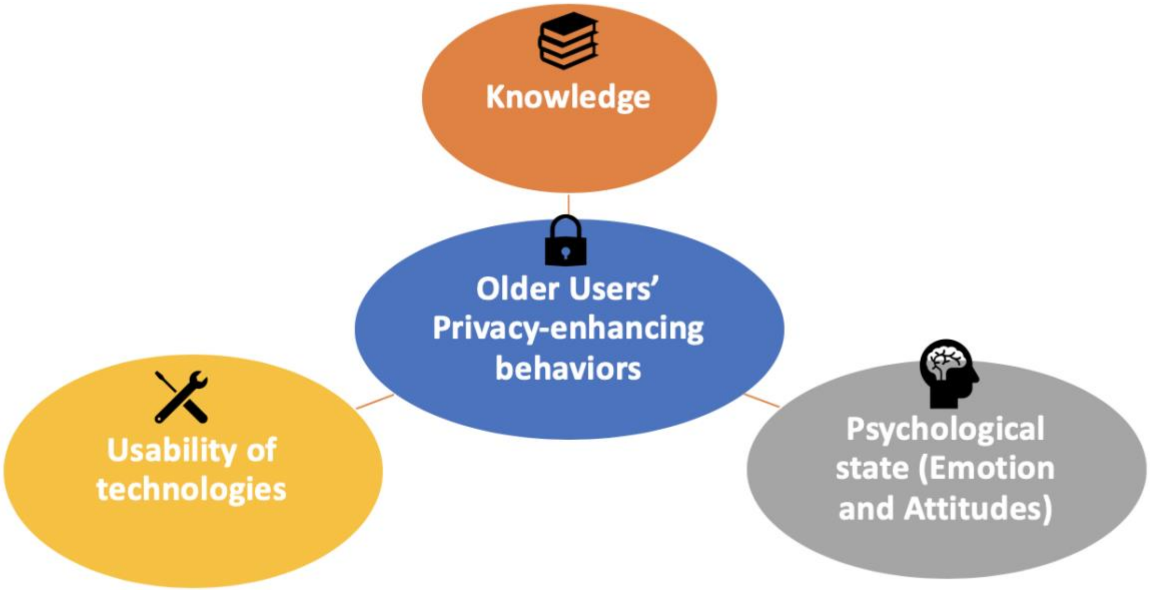

Knowledge
Older Users' Privacy-enhancing behaviors
Usability of technologies
Psychological state (Emotion and Attitudes)

Figure 7.1: Three elements on older users' online privacy-enhancing experience

7.1.1 What do older users know and behave toward online privacy?

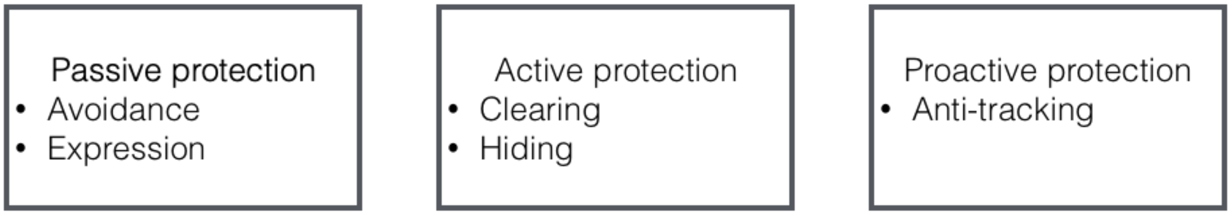
My first research question is to understand older users' knowledge and their actual behaviors toward online privacy in daily life. The findings reveal three phenomena that are as follows:

1) Older users' online privacy protection behaviors are diverse;
2) Privacy knowledge is a missing puzzle for older users' contradictory attitudes and actual behaviors;
3) Privacy divide exists among older users.

In the following subsections, I will elaborate and explain more details on these findings and conclusions.

7.1.1.1 Older users' online privacy protection behaviors

Users' actual online privacy behaviors have been difficult to measure or observe in privacy studies. Therefore, many studies have focused on intended behaviors instead of actual behaviors. However, privacy behavioral intentions do not necessarily lead to actual privacy protection behaviors (Kokolakis, 2017). To the best of my knowledge, no study investigates older adults' actual online privacy behaviors. To fill this research gap, I specifically focus on older adults' actual privacy protection behaviors. As exhibited in Figure 7.2, older users have three main behavioral strategies, including passive, active, and proactive approaches. For each strategy, there are underlying protective mechanisms. For instance, older users will avoid using online websites if they have privacy concerns or they may express their concerns directly to the website or authorities. Nevertheless, the results show that very few older users use the expression strategy to protect their online privacy. A possible explanation is that older users may think that it is too many efforts to directly express their concerns to the website. For active approach, I found that the majority of older users reported that they have experiences in clearing their browsing history, cookies, or unwanted emails on their computer. Yet, very few older users have experience in using a virtual private network to hide their IP addresses. Similarly, the majority of older users do not adopt the proactive strategy.



Passive protection

- Avoidance
- Expression

Active protection

- Clearing
- Hiding

Proactive protection

- Anti-tracking

Figure 7.2: Overview of older users' behavioral strategies

In a nutshell, I found that there is a discrepancy in older users' actual online privacy protection behaviors. Some older users take more advanced approaches than others. When I further conducted the regression analysis to examine the cognitive impacts on older users' behaviors, the results show that knowledge of privacy and security is the only significant cognitive factor, instead of privacy concerns and perceived risks. Next, I explain how knowledge is one of the main factors impacting older users' knowledge.

7.1.1.2 Impacts of older users' knowledge

Prior research has indicated that older adults are concerned about their online privacy while connected to the Internet. A survey study (Walters, AARP, 2017) conducted in the U.S. shows that approximately 75% of older people expressed online privacy concerns and 86% were concerned about their data being breached. Nevertheless, older adults seem to take less online protections than their younger counterparts even though they express similar concern about online privacy (Miltgen and Peyrat-Guillard, 2014; Blank et al., 2014; Van den Broeck, et al., 2015). Based on previous literature (Garg et al., 2011), I hypothesized that in addition to privacy concerns, the lack of knowledge in online privacy can be one of the main factors resulting in the contradiction in older users' privacy attitudes and their actual behaviors. In the study, the results show that knowledge is the only significant factor that can be used to predict older users' actual online privacy protection behaviors, which supports my hypothesis.

As indicated in Chapter 4, I found that interestingly, older users, in general, are knowledgeable about online security. However, the majority of them are lack of knowledge in online privacy-enhancing tools and data practices employed by online companies. For instance, the findings suggest that over half of participants did not know private browsing mode, anonymous browser, a virtual private network, and two-factor authentication. When it comes to online data practices, the findings show that over half of participants have the misconception in whether online companies can exchange their information with third parties; also, over half of them thought that the privacy policy could protect them from third parties sharing. That is, older users may not know how to protect their online privacy because they do not know what kind of tools or mechanisms that can be used. Also, older users may not think there is a necessity to take actions to protect their online privacy due to the misconception of online data practices. The lack of knowledge of privacy tools and online data practices is a missing puzzle for contradictory attitudes and actual behaviors.

7.1.1.3 Privacy divide existing among older users

Another exciting and significant finding is the phenomena of ‘privacy divide.' Based on the results, I found that younger and online older users are more likely to use active and proactive approaches to protect their online privacy compared to their older and offline peers. The identified privacy divide is similar to the concept of the digital divide (Choi and DiNitto, 2013), which indicates the divide in use of technology and digital literacy between a low and high socioeconomic older adult group. Different from the digital divide, one of the main reasons for privacy divide is the knowledge. I think that older users who are younger and more engaged in online activities are more likely to gain knowledge or information regarding online privacy, which further lead to their actual behaviors.

7.1.2 How do older users’ psychological state (e.g., emotions, attitudes) affect their behavioral intention to use a privacy-enhancing browsing tool?

In privacy literature, very few empirical studies investigated the effect of users' psychological state on their adoption of technology. Typically, users are more likely to adopt the technology if they have positive emotions or attitudes toward it. However, it remains unclear whether the current design of privacy-enhancing technologies elicits positive or negative emotions in users. In chapter 5, I selected private browsing mode as a case study and examined the effect of older users' emotions and attitudes on their behavioral intention toward using private browsing mode. The findings indicate two main phenomena:

1) Private browsing mode elicits conflict emotion in older users;

2) Positive emotions and attitudes will enhance older users’ future use of private browsing mode.

Next, I will elaborate more details on these two findings.

7.1.2.1 Elicited emotions by private browsing mode

The results reveal that private browsing mode built-in current leading browsers elicit both positive and negative emotions in older users. For instance, older users feel more private, safer and less being watched in private mode than the public mode. Yet, at the same time, they also feel more fearful, more like a criminal, and more like they are hiding something while using private browsing mode. Suggesting that the interface of private browsing mode provokes two conflicting feelings in users. This type of conflicting emotions may be also associated with the negative association of using private browsing. As discussed in Chapter 6, older users may already have negative perceptions regarding using private browsing mode, which further biasing their emotional response. Therefore, I postulate that negative emotions toward private browsing mode are the consequence of dual effects from the design of the interface and the negative association of the privacy-seeking behavior. However, in this study, it is difficult to evaluate which factor have more impacts on older users' emotions. Further investigation of this topic is needed.

7.1.2.2 Emotional and attitudinal impacts on behavioral intentional toward private browsing mode

In chapter 5, the regression analyses further evidence that older users display a higher level of behavioral intention toward private browsing when they feel more excited and have more positive attitudes toward it. Interestingly, negative emotions have no significant impacts on their behavioral intention. Meaning that negative emotions do not necessarily deter older users' future use of private browsing; on the other hand, positive emotions will drive their future use.

7.1.3 What are usability challenges of a privacy-enhancing browsing tool for older users?

In Chapter 6, I focused on older users' use of a popular privacy-enhancing browsing tool, called Tor Browser. Previous studies have identified several usability challenges and problems of Tor Browser from younger users' point of view, such as latency of the network, difficulty in installation, and inaccessibleness of web pages (see Table 6.2 in Chapter 6). Nevertheless, as far as I know, no empirical study has investigated older users' adoption of Tor Browser. It remains unclear if older users would encounter generic or specific usability issues while using the Tor Browser. Thus, in this study, I examined the usability of Tor Browser from older users' perspective.

According to the findings, usability issues can be further categorized into generic and specific challenges, which is addressed as follow:

1) The generic challenges have been identified in prior research, including the confusion during installation (Lee et al., 2017), inaccessibility of websites (Khattak et al., 2016; Gallagher et al., 2018), and language barriers caused by geolocation (Gallagher et al., 2018);

2) The specific challenges are uniquely identified in this study, which are troubling warning messages and the confusion of empty history box.

I subsequently articulate more details in these two main findings.

7.1.3.1 Generic usability challenges in Tor Browser

As stated above, there are three main generic usability challenges also encountered by older users. The first usability challenge is that older users are confused by the technical terminologies and concepts, such as ‘proxy’, ‘private network’, and ‘configure’. I further found that older users only rely on the knowledge of country-based condition to make the installation, which may mislead older users making an erroneous decision. This further suggests that the complexity of privacy-enhancing tools can, in fact, discount its degree of privacy and security due to end-users' errors.

The second generic usability challenge is the inaccessibility of websites. I found that older users are confused and frustrated by the unexpected inaccessibility. Although previous studies have suggested several solutions to this issue, such as working with websites operators and vendors to make exceptions for Tor, crowdsourcing the list of inaccessible websites, and providing access via archive or cache Internet content (Singh et al., 2017; Gallagher et al., 2018), from older users' perspective, these approaches are far reached and not helpful to reduce their immediate anxiety or frustration with browser. Therefore, I propose a different usability approach to solve this problem for older users. Since older users are frustrated and confused, it is essential to explain why for them to understand and further recommend the alternative choice of websites for them.

The third generic usability challenge is language barrier caused by geolocation of the Tor exit node. Similarly, older users feel annoyed and frustrated by this issue. In order to reduce older users' cognitive load, I suggest to automatically set the preferred exit node location based on the use of the language that is detected during installation for older users. There two benefits by using this approach. First, the number of potential circuits increase that can minimalize the negative consequence on the level of anonymity and security. Furthermore, older users do not need to spend other efforts in learning how to change the setting.

7.1.3.2 Specific usability challenges of Tor Browser

The findings indicate two specific usability challenges uniquely identified by older users. The first challenge is the unfathomable warning messages. Since Tor Browser has built-in addon functions to prevent users from malicious attacks, users sometimes can get the warning messages. The findings suggest that older users find these repeated warning messages difficult to understand and confusing. While older users usually feel frustrated and confused by the warning messages, they also show strong need to understand ‘why' these messages show up. Nevertheless, the design of these warning messages does not provide explanations but only display technical terminologies that cause further frustration in older users. Also, the findings further indicate that older users will have their strategies to tackle the warning message, such as following default suggestion, deciding based on own reasoning, and not responding to the message by closing. Yet, older users begin to feel helpless when the warning message is recurring. Since that older users have strong cognitive needs in knowing the reasoning of a warning message, it is important to provide older users with a simple and useful explanation of warning messages. With the reasoning, it cannot only help older users to make a better decision but also further decrease older users' frustration and anxiety while receiving the warning message.

The other specific usability challenge is the confusion by empty browsing history box. I observed that the majority of older participants do not know how to clear browsing history. When instructed to check browsing history, older users are confused and surprised that there is no history. The reason why older users are confused because it is unexpected and different from their understanding of browsing history. Their expectation is usually to see the browsing history so that they can clear it. Yet, there is no feedback for the status of browsing history on Tor Browser. Older users are hence confused. A proposed consideration for this problem is to have feedback to inform older users the status of browsing history.

7.2 Recommendations

7.2.1 Enhancing older users’ knowledge of online privacy

Overall, Chapter 4 identified that knowledge is the main cognitive factor that can lead older users to their actual privacy protection. Also, the privacy divide exists among older users, which should be noticed and tackled. Therefore, I recommend setting up an educational program to raise older users' awareness and enhance their knowledge of online privacy. While online privacy knowledge can be complicated, it is critical to provide an easy-to-learn and understandable program for older users due to their potential declines in cognitive capacity (Fisk et al., 2009).

7.2.2 Applying positive interface design

Based on the case study of Chapter 5, I conclude that positive psychological state elicited in older users by an interface can motivate older users' adoption of a privacy-enhancing tool. Thus, I suggest using positive design in privacy-enhancing technologies to encourage older users' adoption. Moreover, a positive design may mitigate the negative association of a privacy-enhancing tool, such as private browsing, and further reduce older users' negative feelings.

7.2.3 Utilizing interactive design for privacy-enhancing technologies

When it comes to using a privacy-enhancing tool like Tor Browser, older users may take longer time or need more training and support than their younger counterparts (Fisk et al., 2009). Accordingly, it is important to provide sufficient information and training for older users. In terms of learning strategies for new technology, Barnard et al. (2013) identified three common styles adopted by older users, including 1) having someone guiding them step-by-step, 2) trial and error, and 3) reading a manual or instructions. However, these learning styles are insufficient for the dynamic activities (e.g., surfing on the Internet, using a word processor) (Banard et al., 2013). In the case of Tor Browser, I propose to apply interaction interface design to guide and assist older users throughout the browsing sessions.

Since older users' working memory may decline due to the natural aging process (Fisk et al., 2009; Karbach and Verhaeghen, 2014), it may be difficult for older users to remember how to respond to the unpredictable usability challenges, such as inaccessibility of websites, warning messages, or language barrier caused by geolocation. By providing interactive interface design, older users can gain immediate support whenever they encounter usability difficulties, instead of guessing, memorizing, or putting extra efforts on looking for solutions. More importantly, interactive interface design can also decrease older users' feelings of anxiety, frustration, or helplessness by delivering immediate feedback and instructional solutions for usability issues. In this way, it cannot only enhance the usability of Tor Browser but also increase older users' adoption of Tor Browser.

7.3 Contributions

7.3.1 Contributions of Study 1 (Chapter 4)

The advent of intelligent and Internet technologies will support healthy aging and enhance autonomy and independence for older adults. However, the deep interconnectedness of the Internet also increases risks for information privacy and security breaches, which can put older adults in danger. Therefore, how we empower older adults to protect their information privacy becomes an urgent and challenging question. In summary, the exploratory study found that older adults use different strategies to protect their online information privacy, and reveals that knowledge actually plays a critical role in older adults' protective behaviors. This work contributes in two ways. First, to the best of our knowledge, this is the first study revealing and categorizing older adults' online privacy protection behavioral strategies. Second, this study confirms a phenomenon of *Privacy Divide* among older adults. Therefore, I advocate for designing privacy-friendly systems and educational programs for older populations. While there is still a long road ahead of us to build an aging-friendly and comprehensive privacy-enhancing environment for older adults, this study offers insights for addressing online privacy challenges for an aging population.

7.3.2 Contributions of Study 2 (Chapter 5)

Emotion has been an understudied factor in the usable privacy literature. To fill this gap, the second study investigated the role of emotion in the acceptance of privacy-enhancing features by conducting an online survey experiment on private browsing. The results suggest that the interface design of private browsing may elicit both positive and negative emotions in users. These elicited emotions further affect users' attitudes and behavioral intentions toward it. Generally speaking, positive emotions seem to encourage the use of privacy-enhancing features. However, it also raises an ethical challenge whether privacy-enhancing features should be designed to elicit emotions in users. Another design challenge in privacy-enhancing features is that online privacy-seeking behavior may provoke negative emotions regardless of interface design, because it may already have certain negative connotations in a given cultural context. While there is still much to be done in order to gain a comprehensive understanding of emotional impacts on the use of privacy-enhancing features, this work reveals interesting phenomena and provides insights in the design of privacy-enhancing features. This work will help inform better approaches for future research in usable privacy.

7.3.3 Contributions of Study 3 (Chapter 6)

With the increasing online tracking and data breach, it is critical to empowering older users with the accessible and usable privacy-enhancing tool for online browsing. The third study examines the usability of Tor Browser, a prominent privacy-enhancing technology, from older users' perspective by conducting an in-lab user study. The findings reveal several usability issues identified by older users. According to the findings, we further propose a design solution to each of usability issues from older users' point of view. This study contributes in two significant ways. To the best of my knowledge, this is the first study to examine older users' adoption of privacy-enhancing technology. Since there has been a noticeable digital divide between the younger and older generation, it is critical to making PETs also easy to use and access for older users. Hence, one of the significant contributions of this study is to provide insights on improving one of PETs. Moreover, this study investigates novice users of Tor Browser who constitute the majority of the population. The findings provide understandings on novice users and non-experts' usage of Tor Browser, which may further increase the adoption of Tor Browser.

With the increasing aging population, Internet technologies have not only become essential support for healthy aging but also provided autonomy and independence for older adults in their daily activities from healthcare to banking. Nevertheless, the constant and pervasive connection of the Internet also exposes older adults to the danger of information privacy and security breach. Hence, empowering older users with a useful and usable online privacy-enhancing tools becomes a critical challenge. Nevertheless, there has been a lack of research focusing on older users' privacy-enhancing experience. To fill this gap of knowledge, this thesis examines older users' online privacy-enhancing experience from an interdisciplinary human-computer interaction approach. As the world's aging population continues to grow and advances in Internet technologies happen more rapidly, the design of future technology, from smart homes to self-driving cars, has to adopt the user-centered approach and consider end-users' needs from all age groups. While this research provides certain insights into privacy design for an aging population, additional studies are still urgently needed for the design of human-centered Internet technologies that incorporates and respects users' information privacy and security.

References

1. Abdi, H., & Valentin, D. (2007). Multiple correspondence analysis. *Encyclopedia of measurement and statistics*, 651-657.
2. Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014, November). The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 674-689). ACM.
3. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.
4. Andrade, E. B., & Ariely, D. (2009). The enduring impact of transient emotions on decision making. *Organizational Behavior and Human Decision Processes*, *109*(1), 1-8.
5. Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*(3), 469-490.
6. Angulo, J., & Ortlieb, M. (2015, July). "WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations. In *Symposium on Usable Privacy and Security (SOUPS)*.
7. Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly*, 665-694.
8. Agarwal, R., & Venkatesh, V. (2002). Assessing a firm's web presence: a heuristic evaluation procedure for the measurement of usability. *Information Systems Research*, *13*(2), 168-186.
9. Agarwal, A., & Meyer, A. (2009, April). Beyond usability: evaluating emotional response as an integral part of the user experience. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems* (pp. 2919-2930). ACM.
10. Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010, August). An analysis of private browsing modes in modern browsers. In *Proceedings of the 19th USENIX conference on Security* (pp. 6-6). USENIX Association.
11. Arch, A. (2009, April). Web accessibility for older users: successes and opportunities (keynote). In *Proceedings of the 2009 International Cross-Disciplinary Conference on Web*

Accessibililty (W4A) (pp. 1-6). ACM.

12. Bagozzi, Richard P. "The legacy of the technology acceptance model and a proposal for a paradigm shift." *Journal of the association for information systems* 8, no. 4 (2007): 3.
13. Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9).
14. Barnard, L. (2014). *The cost of creepiness: How online behavioral advertising affects consumer purchase intention*(Doctoral dissertation, The University of North Carolina at Chapel Hill).
15. Basic Emotion Assessment. Therapy aid. Available on February 5th, 2018 at: https://www.therapistaid.com/therapy-worksheet/basic-emotion-assessment
16. Baumeister, R. F., Vohs, K. D., Nathan DeWall, C., & Zhang, L. (2007). How emotion shapes behavior: Feedback, anticipation, and reflection, rather than direct causation. *Personality and Social Psychology Review*, *11*(2), 167-203.
17. Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, *9*(2), 18-26.
18. Brave, S., & Nass, C. (2003). Emotion in human-computer interaction. *The human-computer interaction handbook: fundamentals, evolving technologies and emerging applications*, 81-96.
19. Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. *MIS quarterly*, 689-710.
20. Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419-426.
21. Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites (SSRN).
22. Boise, L., Wild, K., Mattek, N., Ruhl, M., Dodge, H. H., & Kaye, J. (2013). Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. *Gerontechnology: international journal on the fundamental aspects of technology to serve the ageing society*, *11*(3), 428.
23. Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of

online privacy concern and protection for use on the Internet. *Journal of the Association for Information Science and Technology*, *58*(2), 157-165.

24. Bures, R. M. (1997). Migration and the life course: is there a retirement transition?. International Journal of Population Geography, 3(2), 109-119.
25. Brecht, F., Fabian, B., Kunz, S., & Mueller, S. (2011, June). Are you willing to wait longer for internet privacy?. In *ECIS*.
26. Brown, R. T., Diaz-Ramirez, L. G., Boscardin, W. J., Lee, S. J., & Steinman, M. A. (2017). Functional impairment and decline in middle age: a cohort study. Annals of internal medicine, 167(11), 761-768.
27. Cabanac, M. (2002). What is emotion?. *Behavioural processes*, *60*(2), 69-83.
28. Caine, K. E., Fisk, A. D., & Rogers, W. A. (2006, October). Benefits and privacy concerns of a home equipped with a visual sensing system: A perspective from older adults. In *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 50, No. 2, pp. 180-184). Sage CA: Los Angeles, CA: Sage Publications.
29. Caine, K., Šabanovic, S., & Carter, M. (2012, March). The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults. In *Proceedings of the seventh annual ACM/IEEE international conference on Human-Robot Interaction* (pp. 343-350). ACM.
30. Carroll, J. M., & Thomas, J. C. (1988). Fun. *ACM SIGCHI Bulletin*, *19*(3), 21-24.
31. Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948-956.
32. Chiasson, S., van Oorschot, P. C., & Biddle, R. (2006, August). A Usability Study and Critique of Two Password Managers. In *USENIX Security Symposium* (pp. 1-16).
33. Choi, N. G., & DiNitto, D. M. (2013). Internet use among older adults: association with health needs, psychological capital, and social capital. Journal of medical Internet research, 15(5), e97.
34. Clausen, S. E. (1998). Applied correspondence analysis: An introduction (Vol. 121). Sage.
35. Clark, J., Van Oorschot, P. C., & Adams, C. (2007, July). Usability of anonymous web browsing: an examination of tor interfaces and deployability. In *Proceedings of the 3rd*

symposium on Usable privacy and security (pp. 41-51). ACM.

36. Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., & Reagle, J. (2002). The platform for privacy preferences 1.0 (P3P1. 0) specification. *W3C recommendation*, *16*.
37. Cranor, L. F., Guduru, P., & Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *13*(2), 135-178.
38. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.
39. Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE).
40. Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology).
41. Demiris, G., Oliver, D. P., Giger, J., Skubic, M., & Rantz, M. (2009). Older adults' privacy considerations for vision-based recognition methods of eldercare applications. *Technology and Health Care*, *17*(1), 41-48.
42. Desmet, P. M., Porcelijn, R., & Van Dijk, M. B. (2007). Emotional design; application of a research-based design approach. *Knowledge, Technology & Policy*, *20*(3), 141.
43. Demirbilek, O. (2017). Evolution of Emotion Driven Design. In *Emotions and Affect in Human Factors and Human-Computer Interaction* (pp. 341-357).
44. Dickinson, A., Arnott, J., & Prior, S. (2007). Methods for human–computer interaction research with older people. *Behaviour & Information Technology*, *26*(4), 343-352.
45. Dingledine, R., & Murdoch, S. J. (2009). Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it. *Online: http://www. torproject.org/press/presskit/2009-03-11-performance. pdf*.
46. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.
47. Dunlosky, J., & Hertzog, C. (1998). Training programs to improve learning in later adulthood: Helping older adults educate themselves. *Metacognition in educational theory and practice*, *249*, 276.

48. Eckersley, P. (2010, July). How unique is your web browser?. In *Privacy Enhancing Technologies* (Vol. 6205, pp. 1-18).

49. Ekman, P. (1992). An argument for basic emotions. *Cognition & emotion*, *6*(3-4), 169-200.

50. Ekman, P. E., & Davidson, R. J. (1994). *The nature of emotion: Fundamental questions*. Oxford University Press.

51. Fabian, B., Goertz, F., Kunz, S., Müller, S., & Nitzsche, M. (2010). Privately waiting–a usability analysis of the tor anonymity network. In *Sustainable e-Business Management* (pp. 63-75). Springer Berlin Heidelberg.

52. Federal Bureau of Investigation (2013-17). Internet Crime Report. Available at: https://www.ic3.gov/media/annualreports.aspx

53. Finneran, C. M., & Zhang, P. (2003). A person–artefact–task (PAT) model of flow antecedents in computer-mediated environments. *International Journal of Human-Computer Studies*, *59*(4), 475-496.

54. Finneran, C. M., & Zhang, P. (2005). Flow in computer-mediated environments: promises and challenges. *Communications of the association for information systems*, *15*(1), 4.

55. Fisk, A. D., Rogers, W. A., Charness, N., Czaja, S. J., & Sharit, J. (2009). Designing for older adults: Principles and creative human factors approaches. CRC press.

56. Fisher, G. G., Chacon, M., & Chaffee, D. S. (2019). Theories of Cognitive Aging and Work. In Work Across the Lifespan (pp. 17-45). Academic Press.

57. Forte, A., Andalibi, N., & Greenstadt, R. (2017, February). Privacy, anonymity, and perceived risk in open collaboration: A study of Tor users and Wikipedians. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (pp. 1800-1811). ACM.

58. Friemel, T. N. (2016). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, *18*(2), 313-331.

59. Franz, R. L., Munteanu, C., Neves, B. B., & Baecker, R. (2015, August). Time to retire old methodologies? Reflecting on conducting usability evaluations with older adults. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct* (pp. 912-915). ACM.

60. Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002, April). Users' conceptions of web security: a comparative study. In *CHI'02 extended abstracts on Human factors in computing systems* (pp. 746-747). ACM.

61. Gallagher, K., Patil, S., Dolan-Gavitt, B., McCoy, D., & Memon, N. (2018, October). Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1290-1305). ACM.

62. Gallagher, K., Patil, S., & Memon, N. (2017, July). New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (pp. 385-398). USENIX} Association}.

63. Gao, X., Yang, Y., Fu, H., Lindqvist, J., & Wang, Y. (2014, November). Private browsing: An inquiry on usability and privacy protection. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (pp. 97-106). ACM.

64. Garg, V., Camp, L. J., Mae, L., & Connelly, K. (2011, July). Designing risk communication for older adults. In Symposium on Usable Privacy and Security (SOUPS).

65. Gelbrich, K. (2010). Anger, frustration, and helplessness after service failure: coping strategies and effective informational support. *Journal of the Academy of Marketing Science*, *38*(5), 567-585.

66. Ghani, J. A. (1995). Flow in human computer interactions: Test of a model. *Human factors in information systems: Emerging theoretical bases*, 291-311.

67. Glaser, B. G., & Strauss, A. L. (2017). Discovery of grounded theory: Strategies for qualitative research. Routledge.

68. Goldberg, I., Wagner, D., & Brewer, E. (1997, February). Privacy-enhancing technologies for the Internet. In Compcon'97. Proceedings, IEEE (pp. 103-109). IEEE.

69. Gratch, J., & Marsella, S. (2004). A domain-independent framework for modeling emotion. *Cognitive Systems Research*, *5*(4), 269-306.

70. Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology*, *36*(3), 173-192.

71. Ha, V., Inkpen, K., Al Shaar, F., & Hdeib, L. (2006, April). An examination of user perception and misconception of internet cookies. In *CHI'06 extended abstracts on*

Human factors in computing systems (pp. 833-838). ACM.

72. Hassenzahl, M. (2007). The hedonic/pragmatic model of user experience. *Towards a UX manifesto*, *10*.
73. Hawthorn, D. (2000). Possible implications of aging for interface designers. *Interacting with computers*, *12*(5), 507-528.
74. Henry, A. (2014). Which browser is better for privacy?. Lifehacker. Available on May 15th, 2018 at: https://lifehacker.com/which-browser-is-better-for-privacy-1525895782
75. Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? SSRN.
76. Hourcade, J. P., Cavoukian, A., Deibert, R., Cranor, L. F., & Goldberg, I. (2014, April). Electronic privacy and surveillance. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems* (pp. 1075-1080). ACM.
77. Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., & Weinmann, M. (2017). How is your user feeling? Inferring emotion through human–computer interaction devices. *Group*, *1000*, 248.
78. Huang, H. Y., & Bashir, M. (2017, July). Android App Permission and Users' Adoption: A Case Study of Mental Health Application. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 110-122). Springer, Cham.
79. Huang, H. Y., & Bashir, M. (2016, October). The onion router: Understanding a privacy enhancing technology community. In Proceedings of the 79th ASIS&T Annual Meeting: Creating Knowledge, Enhancing Lives through Information & Technology (p. 34). American Society for Information Science.
80. Huang, H. Y., & Bashir, M. (2018). Surfing safely: Examining older adults' online privacy protection behaviors. Proceedings of the Association for Information Science and Technology, 55(1), 188-197.
81. Jackson, C., Bortz, A., Boneh, D., & Mitchell, J. C. (2006, May). Protecting browser state from web privacy attacks. In *Proceedings of the 15th international conference on World Wide Web* (pp. 737-744). ACM.
82. Johnson, D., & Wiles, J. (2003). Effective affective user interface design in games. *Ergonomics*, *46*(13-14), 1332-1345.

83. Kahn, P.H., Ishiguro, H., Friedman, B., Kanda, T., Freier, N.G., Severson, R.L. and Miller, J. 2007. What is a human? Toward psychological benchmarks in the field of humanrobot interaction. *Interaction Studies*, *8* (3), 363-390.
84. Karbach, J., & Verhaeghen, P. (2014). Making working memory work: a meta-analysis of executive-control and working memory training in older adults. *Psychological science*, *25*(11), 2027-2037.
85. Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009, July). A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 4). ACM.
86. Khattak, S., Fifield, D., Afroz, S., Javed, M., Sundaresan, S., McCoy, D., ... & Murdoch, S. J. (2016, February). Do You See What I See? Differential Treatment of Anonymous Users. In *NDSS*.
87. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.
88. Koufaris, M. (2002). Applying the technology acceptance model and flow theory to online consumer behavior. *Information systems research*, *13*(2), 205-223.
89. Koelen, M., Eriksson, M., & Cattan, M. (2017). Older People, Sense of Coherence and Community. In *The Handbook of Salutogenesis* (pp. 137-149). Springer International Publishing.
90. Kisekka, V., Chakraborty, R., Bagchi-Sen, S., & Rao, H. R. (2015). Investigating Factors Influencing Web-Browsing Safety Efficacy (WSE) Among Older Adults. *Journal of Information Privacy and Security*, *11*(3), 158-173.
91. Kim, J., Lee, J., & Choi, D. (2003). Designing emotionally evocative homepages: an empirical study of the quantitative relations between design factors and emotional dimensions. *International Journal of Human-Computer Studies*, *59*(6), 899-940.
92. Kim, S., Gajos, K. Z., Muller, M., & Grosz, B. J. (2016, September). Acceptance of mobile technology by older adults: a preliminary study. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services* (pp. 147-157). ACM.
93. Krishnamurthy, B., Naryshkin, K., & Wills, C. (2011, May). Privacy leakage vs. protection measures: the growing disconnect. In *Proceedings of the Web*(Vol. 2, pp. 1-10).
94. Kulviwat, S., Bruner II, G. C., Kumar, A., Nasco, S. A., & Clark, T. (2007). Toward a unified

theory of consumer acceptance technology. *Psychology & Marketing*, *24*(12), 1059-1084.

95. Kwasny, M., Caine, K., Rogers, W. A., & Fisk, A. D. (2008, April). Privacy and technology: folk definitions and perspectives. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems* (pp. 3291-3296). ACM.
96. Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing* (pp. 273-291). Springer Berlin/Heidelberg.
97. Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., & Wagner, D. (2017). A Usability Evaluation of Tor Launcher. *Proceedings on Privacy Enhancing Technologies*, *3*, 87-106.
98. Lorenzen-Huber, L., Boutain, M., Camp, L. J., Shankar, K., & Connelly, K. H. (2011). Privacy, technology, and aging: A proposed framework. *Ageing International*, *36*(2), 232-252.
99. Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., & Cranor, L. (2012, May). Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 589-598). ACM.
100. Lerner, B. S., Elberty, L., Poole, N., & Krishnamurthi, S. (2013, September). Verifying web browser extensions' compliance with private-browsing mode. In *European Symposium on Research in Computer Security* (pp. 57-74). Springer, Berlin, Heidelberg.
101. Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.
102. Li, J., Theng, Y. L., & Foo, S. (2016). Exergames for older adults with subthreshold depression: does higher playfulness lead to better improvement in depression?. Games for health journal, 5(3), 175-182.
103. Lindsay, S., Jackson, D., Schofield, G., & Olivier, P. (2012, May). Engaging older people using participatory design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1199-1208). ACM.
104. Liou, J. C., Logapriyan, M., Lai, T. W., Pareja, D., & Sewell, S. (2016, August). A Study of the Internet Privacy in Private Browsing Mode. In *Proceedings of the The 3rd Multidisciplinary International Social Networks Conference on SocialInformatics 2016,*

Data Science 2016 (p. 3). ACM.

105. Loiacono, E., & Djamasbi, S. (2010). Moods and their relevance to systems usage models within organizations: an extended framework. *AIS Transactions on Human-Computer Interaction*, *2*(2), 55-72.

106. Lisetti, C. L., & Nasoz, F. (2002, December). MAUI: a multimodal affective user interface. In *Proceedings of the tenth ACM international conference on Multimedia* (pp. 161-170). ACM.

107. Mayer, J. R., & Mitchell, J. C. (2012, May). Third-party web tracking: Policy and technology. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 413-427). IEEE.

108. McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008, July). Shining light in dark places: Understanding the Tor network. In International symposium on privacy enhancing technologies symposium (pp. 63-76). Springer, Berlin, Heidelberg.

109. McNeill, A., Briggs, P., Pywell, J., & Coventry, L. (2017, June). Functional privacy concerns of older adults about pervasive health-monitoring systems. In *Proceedings of the 10th International Conference on Pervasive Technologies Related to Assistive Environments* (pp. 96-102). ACM.

110. Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103-125.

111. Narayanan, A. (2011). An adversarial analysis of the reidentifiability of the heritage health prize dataset. *Unpublished manuscript*.

112. Narayanan, A., & Shmatikov, V. (2008, May). Robust de-anonymization of large sparse datasets. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on* (pp. 111-125). IEEE.

113. Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

114. Norman, D. A. (2004). *Emotional design: Why we love (or hate) everyday things*. Basic Civitas Books.

115. Norcie, G., Caine, K., & Camp, L. J. (2012, July). Eliminating stop-points in the installation and use of anonymity systems: a usability evaluation of the tor browser bundle. In *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS)*.

116. Norcie, G., Blythe, J., Caine, K., & Camp, L. J. (2014, February). Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. In *Proceedings 2014 Workshop on Usable Security*.

117. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

118. Ohana, D. J., & Shashidhar, N. (2013). 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.

119. Oh, H., Rizo, C., Enkin, M., & Jadad, A. (2005). What is eHealth (3): a systematic review of published definitions. *Journal of medical Internet research*, *7*(1).

120. Park, S., Fisk, A. D., & Rogers, W. A. (2010). Human factors consideration for the design of collaborative machine assistants. *Handbook of ambient intelligence and smart environments*, 961-984.

121. Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019-1027.

122. Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215-236.

123. Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology*, *17*(2), 147-156.

124. Perry, M., Clark, E., Murdoch, S., Koppen, G. (2018). The design and implementation of the Tor Browser. Available at: https://www.torproject.org/projects/torbrowser/design/#privacy

125. Pew Research Center, (December, 2010). Generations 2010. Available at: http://www.pewinternet.org/2010/12/16/generations-2010/

126. Pew Research Center, (May, 2017). Technology use among seniors. Available at: http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/

127. Pew Research Center (February, 2018). Internet/Broadband Fact Sheet. Available at: http://www.pewinternet.org/fact-sheet/internet-broadband/

128. Purcell, K. (2011). Search and email still top the list of most popular online

activities. *Pew Internet & American Life Project*, *9*, 1-15.

129. Renaud, K., & Van Biljon, J. (2008, October). Predicting technology acceptance and adoption by the elderly: a qualitative study. In *Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology* (pp. 210-219). ACM.

130. Rogers, W. A., & Fisk, A. D. (2010). Toward a psychological science of advanced technology design for older adults. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, *65*(6), 645-653.

131. Russell, J. A. (2003). Core affect and the psychological construction of emotion. *Psychological review*, *110*(1), 145.

132. Said, H., Al Mutawa, N., Al Awadhi, I., & Guimaraes, M. (2011, April). Forensic analysis of private browsing artifacts. In *Innovations in information technology (IIT), 2011 International conference on* (pp. 197-202). IEEE. 638-646.

133. Satvat, K., Forshaw, M., Hao, F., & Toreini, E. (2014). On the privacy of private browsing–a forensic approach. In *Data Privacy Management and Autonomous Spontaneous Security* (pp. 380-389). Springer, Berlin, Heidelberg.

134. Schwarz, N. (2011). Feelings-as-information theory. *Handbook of theories of social psychology*, *1*, 289-308.

135. Singh, R., Nithyanand, R., Afroz, S., Pearce, P., Tschantz, M. C., Gill, P., & Paxson, V. (2017, August). Characterizing the nature and dynamics of Tor exit blocking. In *26th USENIX Security Symposium (USENIX Security). USENIX Association, Vancouver, BC* (pp. 325-341).

136. Soghoian, C. (2011). Why private browsing modes do not deliver real privacy. *Center for Applied Cyber security Research, Bloomington*.

137. Solove, D. (2008). Understanding privacy.

138. Sourial, N., Wolfson, C., Zhu, B., Quail, J., Fletcher, J., Karunananthan, S., ... & Bergman, H. (2010). Correspondence analysis is a useful tool to uncover the relationships among categorical variables. *Journal of clinical epidemiology*, *63*(6),

139. Stark, L. (2016). The emotional context of information privacy. *The Information Society*, *32*(1), 14-27.

140. Syverson, P., Dingledine, R., & Mathewson, N. (2004). Tor: The secondgeneration onion router. In *Usenix Security*.

141. Taddicken, M. (2014). The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248-273.

142. Tene, O., & Polonetsky, J. (2013). A theory of creepy: technology, privacy and shifting social norms. *Yale JL & Tech.*, *16*, 59.

143. Thomas, J. C., & Kellogg, W. A. (1989). Minimizing ecological gaps in interface design. *ieee Software*, *6*(1), 78-86.

144. Tor Project (2018). Tor Metrics. Available at: https://metrics.torproject.org/

145. Tractinsky, N., Cokhavi, A., Kirschenbaum, M., & Sharfi, T. (2006). Evaluating the consistency of immediate aesthetic perceptions of web pages. *International journal of human-computer studies*, *64*(11), 1071-1083.

146. Turkle, S. (1997). Life on the screen: Identity in the age of the internet. *Literature and history*, *6*, 117-118.

147. United Nation (2017). World Population Ageing. Available at: http://www.un.org/en/development/desa/population/publications/pdf/ageing/WPA2017_Highlights.pdf

148. Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012, July). Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *proceedings of the eighth symposium on usable privacy and security* (p. 4). ACM.

149. Valdez, P., & Mehrabian, A. (1994). Effects of color on emotions. *Journal of experimental psychology: General*, *123*(4), 394.

150. Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media+ Society*, *1*(2), 2056305115616149.

151. Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research*, *11*(4), 342-365.

152. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

153. Venkatesh, V., & Ramesh, V. (2006). Web and wireless site usability: Understanding differences and modeling use. *MIS quarterly*, 181-206.

154. Vohs, K. D., Baumeister, R. F., & Loewenstein, G. (Eds.). (2007). *Do Emotions Help or Hurt Decisionmaking?: A Hedgefoxian Perspective*. Russell Sage Foundation.

155. Vuori, S., & Holmlund-Rytkönen, M. (2005). 55+ people as internet users. *Marketing Intelligence & Planning*, *23*(1), 58-76.

156. Wang, Y. (2009). Privacy-enhancing technologies. In Handbook of research on social and organizational liabilities in information security (pp. 203-227). IGI Global.

157. Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multi-disciplinary review. Computers in human behavior, 26(5), 870-882.

158. Walters, N. (2017). Maintaining privacy and security while connected to the Internet. AARP Public Policy Institute.

159. Wash, R. (2010, July). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 11). ACM.

160. Wild, K., Boise, L., Lundell, J., & Foucek, A. (2008). Unobtrusive in-home monitoring of cognitive and physical health: Reactions and perceptions of older adults. *Journal of applied gerontology*, *27*(2), 181-200.

161. Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus.

162. Winkielman, P., Berridge, K. C., & Wilbarger, J. L. (2005). Unconscious affective reactions to masked happy versus angry faces influence consumption behavior and judgments of value. *Personality and Social Psychology Bulletin*, *31*(1), 121-135.

163. Winter, P., Edmundson, A., Roberts, L. M., Dutkowska-Żuk, A., Chetty, M., & Feamster, N. (2018). How do tor users interact with onion services? In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 411-428).

164. World Health Organization. Definition of an Older or Elderly Person. 2012. Available at: http://www.who.int/healthinfo/survey/ageingdefnolder/en.

165. W3schools. Browser statistics (2017). Available at: https://www.w3schools.com/browsers/default.asp.

166. Young, J. B. (1978). Introduction: A Look at Privacy, in PRIVACY (John B. Young ed.)

167. Zhang, B., & Xu, H. (2016, February). Privacy nudges for mobile applications: Effects

on the creepiness emotion and privacy attitudes. In *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing* (pp. 1676-1690). ACM.

168. Zukowski, T., & Brown, I. (2007, October). Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 197-204). ACM.

Appendix A. Survey Questionnaire (Chapter 4)

Section 1: In this section, we are interested in **your general use of the Internet.** Please read and answer the following questions carefully.

Q1: Do you happen to own any of the following devices? Please select all that apply.

❑A desktop computer

❑A laptop computer

❑A smartphone

❑A tablet

❑A wearable device (e.g., smart watch)

❑Other, please specify: ____________________

Q2: Which of the following devices do you use primarily for online activities? Please select all that apply.

❑A desktop computer

❑A laptop computer

❑A smartphone

❑A tablet

❑Others, please specify: ____________________

Q3: Which operating system is on the device that you used for online activities?

❍Microsoft Windows

❍Mac OS X

❍Linux

❍Other, please specify ____________________

❍Don't know

Q4: Do you have an Internet connection at your home?

❍ Yes

❍ No

Q5: How often do you use the Internet?

❍ Several times a day

❍ About once a day

❍ A few times a week

❍ About once a week

❍ About once a month

❍ Just a few times a year

Q6: On average, how many hours do you usually spend on the Internet every day?

Hours / per day____________________

Q7: When browsing on the Internet, which browser do you usually use?

❍ Google Chrome

❍ Mozilla Firefox

❍ Safari

❍ Internet Explorer

❍ Other, please specify: ____________________

❍ Don’t know

Q8: Do you have anti-virus software installed on your computer device?

❍ Yes

❍ No

❍ Don't know

Q9: Online social media sites have provided us opportunities to connect with others. Do you use any of the social media sites, like Facebook, Youtube, LinkedIn, etc.?

❍ Yes, please specify which sites you currently use:

____

❍ No

Q10: In general, would you say your health is: (Please **circle** the answer)

1	2	3	4	5
Poor	Fair	Good	Very Good	Excellent

Section 2: Risk Perceptions

Q11: In your opinion, **how risky the following online activities are**? Please **circle** your opinion below.

Not risky at all = 1-------2-------3-------4-------5 = Extremely risky

1. Send or read email
2. Watch a video clip or listen to an audio clip
3. Look up a phone number or address
4. Take a virtual tour of a location
5. Use online financial services like banking, investing, paying bills
6. Upload photos to a website so you can share them with others
7. Log on to the Internet using a public wireless device
8. Pay to access or download digital content

9. Share files from your computer with others
10. Chat in a chat room or discussion forum
11. Using a webcam to communicate with someone remotely
12. Sell something online
13. Visit an adult website
14. Send or receive an invitation to a meeting or party using an invitation service
15. Download files (e.g., computer games, music, videos) to your computer
16. Use a map service
17. Use a social networking site
18. Use a search engine
19. Makes travel reservations
20. Shop online
21. Search for health information
22. Take a class or participate in job training online
23. Make a doctor's appointment online
24. Use an online prescription service

Section 3: Information sharing practices

Q12: In our daily online activities, we exchange many different types of information. In this section, we would like to know more about **your online information sharing preferences.**

- Please **circle** which types of information you would like to share with **Health sites (e.g., WebMD, Yahoo! Health)**.
- Please **circle** which types of information you would like to share with **Banking/Financial sites (e.g., Chase, Paypal)**
- Please **circle** which types of information you would like to share with **Search engine sites (e.g., Google, Bing)**

- Please **circle** which types of information you would like to share with **E-commerce sites (e.g., Amazon, Zappos)**
- Please **circle** which types of information you would like to share with **Social media sites (e.g., Facebook, twitter)**

List of information:

1. Credit card number
2. Hobbies
3. Legal records
4. Place of birth
5. Credit score
6. Income bracket
7. Email address
8. Marital status
9. Ethnicity
10. Online purchasing history
11. Political donations
12. Phone number
13. Online browsing history
14. Legal name
15. List of friends
16. Charitable donations
17. Phone contact
18. Age
19. Social security number
20. List of partners
21. Religious views
22. Home address
23. Gender

24. Sexual orientation
25. Medical history
26. Political views
27. Text / Message
28. Education
29. Occupation
30. Mental health information
31. Family history
32. Photos/Video files
33. Date of birth
34. Location
35. Emotional state

Section 4: Experience with online privacy practices

Q13: When browsing on the Internet, we may be exposed to some risks. Based on your past experience, **have you ever taken the following actions** because you were **concerned about personal privacy and wanted to protect it**? Please **circle** your response.

If you have **NOT** done it before, please select the box 'Want to learn' if you are **interested in** how to do it.

Yes, I have-------------------No, I have not □ Want to learn

- Stopped visiting particular websites
- Given a false or inaccurate email address or fake name to websites
- Decided not to make an online purchase
- Chosen not to register on a website
- Complained to a consumer or government agency about marketing practices of particular websites

- Asked a website to remove your name and address from their lists/database
- Asked a website not to share your personal information with other companies
- Used an email address that is not your main address
- Cleared your web browser history
- Used filters to block or manage unwanted email
- Erased some or all of the cookies on your computer
- Used software that hides your computer's identity from websites you visit

Q14: Did you use any **other strategy** when you were concerned about your **personal online privacy**? Please describe your strategy or experience.

Section 5: we would like to know your opinions toward the **use of online information by online services.**

Q16: Please rate how much you **agree or disagree** with the following statements.

Strongly disagree = 1-------2-------3-------4-------5 = Strongly agree

1. I want an online service to tell me how my personal information will be used.
2. I am concerned about unauthorized entities getting access to my personal information.
3. I mind when an online service monitors my purchasing patterns.
4. I mind when an online service collects information about my browsing patterns.
5. I mind when my personal information is shared or sold to third parties.
6. I mind when Internet Service Providers (e.g., Comcast, AT&T, Verizon) use and share my information without my consent.

Q17: While using the Internet, certain unexpected situations may occur. Please **circle** how '**worried**' you are about the following situations on the scale.

Not worried at all = 1-------2-------3-------4-------5 = Extremely worried

1. Someone looking at the contents of my mobile device.

2. Strangers looking at the things I post on the Internet.
3. Someone obtaining or intercepting my credit card number after I make an online purchase
4. Online services not being who they claim they are
5. People online not being who they say they are
6. Advertisers using information about me to advertise to me
7. Companies sharing my personal information without my permission
8. No encryption of my data when I submit it to an Internet service
9. Large amounts of information about me being available online
10. In general, how worried are you about your privacy while you are using the Internet?

Section 6: we would like to know more about your awareness of **online activities and services.**

Q18: Please indicate whether you think each statement is true or false. Select "I'm not sure" if you don't know the answer.

True--------------------False--------------------Not sure

1. Public Wi-Fi is as secure as private Wi-Fi.
2. Internet Protocol addresses can always uniquely identify your computer.
3. When you visit a website, the site can store a cookie so it can recognize your device in the future.
4. Phishing scams are usually fraudulent email messages appearing to come from a legitimate entity (e.g., charity, bank, government).
5. Malware/Virus can cause your device to crash and can be used to monitor and control your online activity.
6. Most browsers provide private browsing mode, which can prevent websites from collecting your information.
7. ToR is software that enables you to send anonymous requests to online services.

8. A Virtual Private Network cannot allow you to access the Internet privately.
9. A website with a HTTPS address is less secure than a website with a HTTP website.
10. Encryption can protect your email or device from snooping.
11. When Two-Factor Authentication (TFA) is applied, it requires not only something you know (e.g., your password or username), but also something you have (e.g., your phone).
12. Companies today have the ability to place an online advertisement that targets you based on information collected about your web-browsing behavior
13. A company can tell if you have opened an email even if you do not respond
14. When you go to a website, it can collect information about you even if you do not register.
15. Online business sites may exchange your personal information with law enforcement and credit bureaus without your awareness
16. If a website has a privacy policy, it means the site will not share your information with other websites or companies
17. Social networking sites can collect your web browsing information even if you are not logged into the service.

Section 7: we would like to know more about **your online protection behavior.**

Q19: Are you currently using any of the following online tools? Please **circle** your response. If you have **NOT** used it before, please select the box 'Want to learn more' if you are interested in **learning more information** about any of following online tools.

Yes, I am. ---------------- No, I am not. □ Interested in learning more

1. Anonymous web browser (e.g., ToR browser)
2. Ad-blocking plugin on your web browser (e.g., Adblock, Beef Taco)
3. Third party blocking plugin (e.g., Disconnect, Privacy Badger)

4. Browser plugin to make sure that you only access websites with a HTTPS header (e.g., HTTPS everywhere)
5. Anonymous web search engine (e.g., DuckDuckGo)
6. Cookies/Cache/Online history cleaner (e.g., BetterPrivacy, CCleaner)
7. Password management (e.g., 1 password, Lastpass)
8. Online tracker management (e.g., Ghostery, Blur)
9. Email encryption (e.g., Mailvelope, Enigmail)
10. Instant messaging encryption (e.g., Cyrptocat, TorChat, Signal)
11. Disconnect social media tracking (e.g., Facebook Disconnect)

Section 8: Use of Password

Q20: Have you ever shared a password to one of your online accounts with a friend or family member?

❍ Yes

❍ No

Q21: Do you use two-factor or two-step authentication for any of your online accounts?

Note: Two-factor authentication is a feature where you are sent a one-time code via email or text message that you would enter after first entering your username and password, and only works for a single login and for a limited amount of time.

❍ Yes

❍ No

Q22: Considering different ways you keep track of your online passwords, **do you use any of the following strategies**? Please **circle** the answer.

Memorizing them in your head	Yes	No
Writing them down on a piece of paper	Yes	No
Saving them in a note or document on your computer or mobile device	Yes	No
Using a password management program such as Dashlane, Lastpass, or Apple Keychain.	Yes	No
Saving them in your internet browser	Yes	No

Section 9: Background information

Q23: What is your age? ______________

Q24: What is your gender?

❍ Male

❍ Female

❍ Other

Q25: Are you currently…?

❍ Retired

❍ Working

❍ Retired but still working

❍ Other, please specify: ____________________

Q26: What is the highest education level you've achieved?

❍ Some high school

❍ High school

❍ Some college

❍ Associate's degree

❍ Bachelor's degree

❍ Graduate or Professional degree

❍ Doctoral degree

❍ Prefer not to answer

Q27: Generally speaking, how would you indicate your political point of view?

❍ Republican

❍ Democrat

❍ Independent

❍ Other, please specify: ____________________

Q28: What is your living status?

❍ living alone

❍ living with significant others

❍ living with family members

❍ living with non-family members

❍ Other, please specify: ____________________

Q29: What is your ethnicity?

❍ White

❍ Hispanic or Latino

❍ Black or African American

❍ Native American or American Indian

❍ Asian / Pacific Islander

❍ Other, please specify: ____________________

Appendix B. Questionnaire of Survey Experiment (Chapter 5)

Section 1: In this section, we are interested in your ability to perform a number of tasks on a computer. Please answer each question by selecting a choice that is most appropriate for you.

Q1: If you have not tried to perform the task below or do not know what it is, please mark "NEVER TRIED", regardless of whether or not you think you may be able to perform the task.

Please select a choice for each row.

- Never tried (1)
- Not at all (2)
- Not very easily (3)
- 4 -Somewhat easily (4)
- Very easily (5)

I can:

- Use a computer keyboard to type (1)
- Use a mouse (2)
- Replace the ink cartridge of printer (3)
- Open emails (4)
- Send emails (5)
- Find information about local community resources on the Internet (6)
- Find information about my hobbies and interests on the Internet (7)
- Use a computer to enter events and appointments into a calendar (8)
- Check the date and time of upcoming and prior appointments (9)
- Use a computer to watch movies and videos (10)
- Use a computer to listen to music (11)

- Fix the printer when paper jams (12)

Section 2 : Now, we are interested in your computer use and Internet experience. Please read each question carefully and provide a response to each one of them.

Q2: How familiar would you say you are using the computer to access the Internet?

Not familiar at all=1 --2 --3 --4 --5=Extremely familiar

Q3: Do you own any of the following devices? Please select all that apply.

- A desktop computer (1)
- A laptop computer (2)
- A smartphone (3)
- A tablet (4)
- Other, please specify: (5)

Q4: Which of the following devices do you use primarily for online activities?

- A desktop computer (1)
- A laptop computer (2)
- A smartphone (3)
- A tablet (4)
- Other, please specify: (5)

Q5: Do you share your primary computer device with others?

- Yes (1)
- No (2)

Q6: Which operating system do you use for online activities?

- Microsoft Windows (1)
- Mac OS X (2)
- Linux (3)

- Others, please specify: (4)
- Don't know (5)

Q7: Do you have an Internet connection at your home?

- Yes (1)
- No (2)

Q8: Does your home Internet / Wi-Fi require passwords to access?

- Yes (1)
- No (2)
- Don't know (3)

Q9: How often do you use the Internet?

- Several times a day (1)
- About once a day (2)
- A few times a week (3)
- About once a week (4)
- About once a month (5)
- Just a few times a year (6)

Q10: On average, how many hours do you usually spend on the Internet everyday?

____

Q11: When browsing on the Internet, which browser do you <u>usually</u> use?

- Internet Explorer / Edge (1)
- Mozilla Firefox (2)
- Safari (3)
- Google Chrome (4)
- Other, please specify: (5)

  - Don't know (6)

Q12: Have you ever used private mode on a browser?

- Yes (1)
- No (2)
- Don't know what private mode is (3)

Q13: Which browser do you usually use for private browsing?

- Incognito mode on chrome (1)
- InPrivate browsing on IE / Edge (2)
- Private window on Firefox (3)
- Private browsing on Safari (4)
- Other, please specify: (5)

Q14: Which kind of device(s) do you usually use when using private browsing? Please select all that apply.

- Desktop (1)
- Laptop (2)
- Tablets (3)
- Mobile phone (4)
- Other, please specify: (5)

Q15: On average, how many hours per week do you spend on using private mode?

Q16: How often do you use private browsing mode for online activities?

- Several times a day (6)
- About once a day (5)
- A few times a week (4)
- About once a week (3)

- About once a month (2)
- Just a few times a year (1)

Q17: We all want to use private browsing for a variety of reasons. We are interested in learning what motivates you for using private browsing mode. Please select all that apply.

- Don't want family members to know what you do online (1)
- Don't want online services to track you (2)
- Don't want to see personalized ads (3)
- Don't want employer to know what you do online (4)
- Visit websites that are taboo or stigmatized (5)
- Other, please elaborate: (6)

Section 3: Privacy knowledge

Q18: In this section, we would like to know more about your understanding of private browsing. Please read the following statements and indicate whether you think each statement is true or false. Please select "*Don't know*", if you are not sure about the answer.

True---False---Don't know

- In private browsing mode, the pages I visit will not be added to my browsing history list. (1)
- In private browsing mode, things I enter into search bar will be saved for autocompleted form. (2)
- In private browsing mode, my passwords will not be saved (3)
- In private browsing mode, the files I download will be listed in the list of downloads after I turn off private browsing. (4)
- In general, cookies will either not be stored or be cleared after I close the private browser. (5)
- Internet Service Providers cannot access my browsing history if I used private browsing mode. (6)

Section 4: Personality traits and view on people using privacy browsing mode

Q19: Here are a number of personality attributes that may or may not apply to you. Please indicate the extent to which you agree or disagree with each statement below.

- Disagree strongly (1)
- Disagree moderately (2)
- Disagree a little (3)
- Neither agree nor disagree (4)
- Agree a little (5)
- Agree moderately (6)
- Agree strongly (7)

I see myself as…

- Extraverted, enthusiastic (1)
- Critical, quarrelsome (2)
- Dependable, self-disciplined (3)
- Anxious, easily upset (4)
- Open to new experiences, complex (5)
- Reserved, quiet (6)
- Sympathetic, warm (7)
- Disorganized, careless (8)
- Calm, emotionally stable (9)
- Conventional uncreative (10)

Q20: What kind of characteristics would you associate with people who use private browsing?

Please indicate your rating on the following scale.

People who use private browsing are…

Trustworthy	1	2	3	4	5	Untrustworthy
Decent	1	2	3	4	5	Mischievous
Liberal	1	2	3	4	5	Conservative
Religious	1	2	3	4	5	Not religious
Open	1	2	3	4	5	Secretive
Straightforward	1	2	3	4	5	Mysterious
Careless	1	2	3	4	5	Cautious
Independent	1	2	3	4	5	Dependent
Having nothing to hide	1	2	3	4	5	Having something to hide
Lawful	1	2	3	4	5	Criminal

Section 5: Interface evaluation

Q21: In this section, we are interested in your overall feelings about interface. We are going to present you an interface and would like to have your feedback regarding how this interface makes you feel. In general, how does this interface make you feel?

[Insert public or private browsing mode interface]

Please rate your feelings on the following scale.

none 0 -- 1 – 2 -- 3 -- 4 – 5 very

- Happy (1)
- Sad (2)
- Angry (3)
- Fearful (4)
- Excited (5)
- Disgusted (6)

Q22: Again, please focus on the interface below. What are some <u>other feelings</u> this interface brings to you? Please rate your feelings on the following scale.

[Insert public or private browsing mode interface]

This interface makes me feel…

Private	1	2	3	4	5	Public
Safe	1	2	3	4	5	Vulnerable
Like not being watched	1	2	3	4	5	Like being watched
Not censored	1	2	3	4	5	Censored
Like a legitimate citizen	1	2	3	4	5	Like a criminal
Ordinary	1	2	3	4	5	Unique
Having nothing to hide	1	2	3	4	5	Having something to hide

Section 6: Interface evaluation

Q23: Now, we're interested in your opinions about <u>the design</u> of the interface below. Please look at this interface and answer the questions below. Overall, how easy is it for you to understand the functions on this interface?

[Insert private browsing mode interface]

1-Not easy at all – 2—3—4—5—6—7 Extremely easy

Section 7: Interface evaluation

Q24: The interface below is a website presented in private mode on a browser. Now, please focus on this interface and see if you can find (by clicking on it) the icon (or sign), which indicates that you're using private mode.

[Insert private browsing mode interface]

1-Not easy at all – 2—3—4—5—6—7 Extremely easy

Section 8: In this section, we are interested in your opinion about the design of the icon below.

Q25: In general, how do you feel about this icon below? Please rate your feeling on the following scale.

[Insert the icon of private browsing mode]

Private	1	2	3	4	5	Public
Safe	1	2	3	4	5	Vulnerable
Like not being watched	1	2	3	4	5	Like being watched
Not censored	1	2	3	4	5	Censored
Like a legitimate citizen	1	2	3	4	5	Like a criminal
Ordinary	1	2	3	4	5	Unique
Having nothing to hide	1	2	3	4	5	Having something to hide

Q26: Overall, how much do you like this icon?

1-Not like it at all –2—3—4—5—6—7 Extremely like it

Section 9: Now, for the very last time, we are interested in your opinion about the entire interface presented below.

Q27: Overall, how satisfied are you with this interface?

Not satisfied at all=1—2—3—4—5—6—7 =Extremely satisfied

Q28: If you could change this interface, what would it be? Please provide suggestions for how this interface can be improved.

Section 10: Please indicate your opinion on the following statements.

Q29: Overall, I think private browsing is ____________ to protect my online privacy.

Strongly disagree=1 --2 --3 --4 –5 --6 --7=Strongly agree (7)

- Useful (1)
- Effective (2)
- Easy-to-use (3)
- An appropriate way (4)
- A secure way (5)

Q30: Please indicate your opinion on the following statements.
I intend to use private browsing mode…

Strongly disagree=1 --2 --3 --4 –5 --6 --7=Strongly agree (7)

- To protect my online privacy (1)
- To secure my personal information online (2)
- More often than I have done in the past (3)
- As the default on my browser (4)
- And recommend it to others (5)

Section 11: In this final section, we would like to learn more about you.

Q31: What is your age?_______

Q32: What is your gender?

- Male (1)
- Female (2)
- Other (3)

Q33: Please specify your current status for your occupation.

- Working (1)
- Retired (2)
- Retired but still working (3)
- Other, please specify: (4)

Q34: What is your current living status?

- living alone (1)
- living with significant others (2)
- living with family members (3)
- living with non-family members (4)
- others (5)

Q35: What is the highest education level you've achieved?

- Some high school (1)
- High school (2)
- Some college (3)
- Associate's degree (4)
- Bachelor's degree (5)
- Graduate or Professional Degree (6)

Q36: Please specify your ethnicity.

- White (1)
- Hispanic or Latino (2)
- Black or African American (3)
- Native American or American Indian (4)
- Asian / Pacific Islander (5)
- Other, please specify: (6)

Q37: Generally speaking, do you usually think of yourself as a Republican, a Democrat, or an Independent?

- Republican (1)
- Democrat (2)
- Independent (3)
- Other, please specify: (4)

Appendix C. Interview Materials of User Study (Chapter 6)

Part 1: Post Task Interview Script

(Ask after each task)

Q1: If 1 is not easy at all and 10 is extremely easy, how easy is it for you to do this task?

Q2: While doing the task, did you encounter any difficulty or obstacle? Please describe your experience.

Q3: Did you find something on the interface that confused you? Please describe your experience.

Q4: If user see any warning message on the interface:

- What did you think of the warning message?

Part 2: Private browsing post-interview / Questionnaire

Please read each statement and select a response by using tick or X.

Strongly Disagree =1—2—3—4--Strongly Agree=5

a. I think that I would like to use this tool frequently.

b. I found the tool unnecessarily complex.

c. I thought the tool was easy to use.

d. I think that I would need the support of a technical person to be able to use this tool.

e. I found the various functions in this tool were well integrated.

f. I thought there was too much inconsistency in this tool.

g. I would imagine that most people would learn to use this tool very quickly.

h. I found the tool very cumbersome to use

i. I felt very confident using the tool.

j. I needed to learn a lot of things before I could get going with this tool.

Q2: Feelings of security and privacy about private browser

I am going to ask you some questions about your feelings toward the browser.

- If one is not secure at all and ten is very secure, in general, how secure do you feel about the browser? Please elaborate your answer.

  Not secure at all=1 2 3 4 5 6 7 8 9 10=Extremely secure

- If one is not private at all and ten is very private, in general, how private do you feel about the browser do you feel? Please elaborate your answer.

  Not private at all=1 2 3 4 5 6 7 8 9 10=Extremely private

Q3: Like and dislike feature of private browser

- In general, what feature do you like the most on this browser? Please elaborate your answer.
- In general, what feature do you dislike the most on this browser? Please elaborate your answer.

Q4: Difficulties to use private browser

- While using TOR, what was the most difficult part for you to use? Please explain your answer.
- Was there anything on TOR confusing you? Please elaborate your answer.
- If you could make the tool better, what would you do?
- Is there any additional function or privacy-related information you would like to know while using the tool?

Q5: Intentions to use private browser

- Would you recommend this tool to your friend?
- Would you intend to use this type of private browser in the near future? Please elaborate your answer.

Part 3: Post-Interview about privacy and technology

Confirm with RPT: Is there any things you want to tell me about the tool?

Now, I'm going to ask some questions about your opinions toward privacy and technology:

Q1: In your opinion, what does the role of privacy play in your life?

Q2: Then, how does the technology change that aspect?

Q3: When adopting new home technologies, previous research has shown that some older adults encounter a challenge between maintaining independence and personal privacy. What do you think about it? Have you ever encountered similar challenge(s)? Please elaborate your experience.

Q4: Have you ever been worried about your privacy while using the Internet technologies? What did you do when having privacy concerns toward the technology? Please elaborate your experience.

Appendix D. Technical Terminologies

Cookies: cookies are the messages that web servers send to users' web browser when they visit online websites. The browser stores each message in a small file (e.g., cookie.txt). When users request another webpage from the server, the browser sends the cookie file back to the websites' server. The cookie files usually include users' information such as their visits to web pages, name and their interests.

Tracking Script: Tracking script is a piece of JavaScript code that can track the activity of a web user. Tracking script can collect and send users' data to the web servers.

Proxy: A proxy is a server that acts as an intermediary between the online users and the Internet Service Providers. Proxy can be operated by a computer system or an application.

HTML5 Image Canvas Data: The HTML5 Canvas is a form of image data (e.g., font, picture) that can be used by web servers to track online users. This type of rendered image data is almost identical to a tracking cookie.

Latency of network: Latency indicates the delay happening to the data. Since Tor Network is designed with three-layered routing services, users may experience the delay or slowness of the website, which is termed as latency of network in this thesis.

NoScript Cross-Site Attack: NoScript is an addon extension on Tor Browser that can prevent Cross-Site Scripting (XSS) attacks, which allow an attacker to steal users' authentication credentials by adding malicious code from a certain site into a different site.