Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser

Kevin Gallagher
New York University
kevin.gallagher@nyu.edu

Sameer Patil
Indiana University Bloomington
patil@indiana.edu

Brendan Dolan-Gavitt
New York University
brendandg@nyu.edu

Damon McCoy
New York University
mccoy@nyu.edu

Nasir Memon
New York University
memon@nyu.edu

ABSTRACT

The strength of an anonymity system depends on the number of users. Therefore, User eXperience (UX) and usability of these systems is of critical importance for boosting adoption and use. To this end, we carried out a study with 19 non-expert participants to investigate how users experience routine Web browsing via the Tor Browser, focusing particularly on encountered problems and frustrations. Using a mixed-methods quantitative and qualitative approach to study one week of naturalistic use of the Tor Browser, we uncovered a variety of UX issues, such as broken Web sites, latency, lack of common browsing conveniences, differential treatment of Tor traffic, incorrect geolocation, operational opacity, etc. We applied this insight to suggest a number of UX improvements that could mitigate the issues and reduce user frustration when using the Tor Browser.

CCS CONCEPTS

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

KEYWORDS

Tor; Tor Browser; User Experience; UX; Usability; Privacy; Anonymity

ACM Reference Format:
Kevin Gallagher, Sameer Patil, Brendan Dolan-Gavitt, Damon McCoy, and Nasir Memon. 2018. Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser. In *2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), October 15–19, 2018, Toronto, ON, Canada.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3243734.3243803

CCS '18, October 15–19, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-5693-0/18/10. . . $15.00
https://doi.org/10.1145/3243734.3243803

1 INTRODUCTION

Anonymity plays a vital role in modern societies. Using the protective cloak of anonymity, whistleblowers are able to inform the public of malicious behaviors of governments and corporations, journalists are able to contact sources and perform research on subjects of interest, immigrants, abuse victims, and other at-risk individuals are able to seek help and information, and citizens are able to maintain privacy and express ideas without fear. Anonymity helps many people protect their rights or keep themselves safe from embarrassment, physical danger, or in some cases, even death. Achieving anonymity in the Internet age is becoming increasingly difficult due to the prevalence of tracking mechanisms and metadata collection and requires more advanced tools [31]. One such tool is Tor [9], an overlay network that provides metadata obfuscation by routing Internet traffic through randomly selected, volunteer-run relays, with each relay providing a layer of encryption.

The strength of an anonymity system such as Tor depends on the number of indistinguishable users, called its anonymity set [8]. In an effort to strengthen the network and expand the set of indistinguishable Tor users, the Tor Project provides the Tor Browser that makes users less distinguishable by countering some application-layer tracking techniques, such as cookies, `User-agent` strings, or browser fingerprinting mechanisms. Since the extent of anonymity is dependent on the number of indistinguishable users, it is important to provide user-centered security [44] by paying attention to the User eXperience (UX) of the Tor Browser. Poor UX tends to drive users away, thus negatively impacting the strength and quality of anonymity provided by the Tor network. Further, the more diverse the Tor user base, the less an adversary may infer about any individual user. Those whose anonymity needs may not be strict enough to tolerate UX frustrations and inconveniences may still be willing to use the Tor Browser if the UX is improved, thus diversifying the Tor user base.

Yet, there has been little research on the Tor Browser UX. Existing work related to the topic is outdated [5], narrow in focus [28], or limited to lab settings and specific tasks [32, 33], thus limiting the utility and impact of the findings. We aim to fill this gap via the following research question:
How do users experience routine Web browsing when using the Tor Browser?

We addressed this question via a study that examined the use of the Tor Browser in a naturalistic setting for a period of one week, focusing particularly on identifying frustrations, confusions, and problems. To this end, we collected quantitative and qualitative data on the use of the Tor Browser for routine Web browsing and online tasks. Based on 121 questionnaire responses, 11 interviews, and 19 write-ups from 19 study participants, we report on a number of UX issues, such as broken Web sites, latency, lack of common browsing conveniences, differential treatment of Tor traffic, incorrect geolocation, operational opacity, etc. Specifically, we make the following contributions:

(1) **Detailed account of naturalistic use of the Tor Browser.**
We collected data regarding Tor Browser usage for routine online activities in a naturalistic setting, uncovering a number of important UX issues.

(2) **Suggestions for improving the Tor Browser UX.**
Grounded in the UX issues encountered during our study, we identify and outline several practical solutions and design guidelines to address and mitigate the problems and improve the UX of the Tor Browser.

(3) **Method for privately collecting naturalistic quantitative data on the Tor Browser UX at scale.**
Our method for collecting quantitative UX data on Tor Browser usage could be deployed to allow privately gathering naturalistic data at scales significantly beyond those possible in typical laboratory studies.

In the sections that follow, we first summarize prior related research on the UX, usability, and users of Tor. We then describe our method, including study setup and sample. Next, we present and discuss the quantitative and qualitative findings on the Tor Browser UX. We discuss application of the findings to derive practical suggestions for improving the UX of the Tor Browser to help expand its user base and support non-experts. Finally, we point out important limitations of our study along with potential avenues for future exploration.

2 RELATED WORK

As Dingledine and Mathewson observed [8], the strength of an anonymity system depends on the number of users, thus highlighting the importance of UX and usability for these systems. Yet, in contrast to the large body of work on its technical aspects, such as attacks, defenses, measurements, etc. [19, 21, 22, 24, 29, 35, 39, 43], relatively little research has focused on the UX and users of Tor. Existing research on the user aspects falls under three main themes: UX of anonymity systems and the Tor network, UX of the Tor Browser in particular, and attitudes and practices of Tor users.

2.1 UX of Anonymity Systems

Köpsell et al. [27] performed one of the first studies on the UX of anonymity systems by introducing latency 'shocks' for the period of one month into '`AN.ON`,' an early anonymity network. These shocks occurred every 105 minutes, lasting for 15 minutes on each occasion. The results of the study indicated that the number of users who leave an anonymity network because of latency is linearly correlated to the amount of latency for latency periods lasting fewer than 60 seconds. In the same vein, Fabian et al. [11] attempted to quantify the latency introduced by Tor and the corresponding loss of user requests. They discovered that the median load time for a Web page over Tor was 5 times higher when compared to a direct connection, and the Domain Name System (DNS) requests were 40 times slower. These measurements led them to conclude that 74% of requests over Tor would be canceled, causing significant user frustration. In 2014, Griffith [16] examined the data on the Tor Metrics Web site and concluded that Tor achieves less than 2% of the throughput of non-Tor bandwidth which has remained relatively constant for small files (when normalized by non-Tor bandwidth). Tor performance for large files is however steadily improving, albeit slowly.

Due to its importance for an acceptable UX, reducing latency is an important topic of investigation. Jansen et al. [20] implemented KIST, a kernel-informed socket management algorithm which dynamically computes the amount of data to write to a given socket. In a limited trial, KIST was shown to reduce congestion by over 30% and latency by 18%, thus increasing overall network throughput by nearly 10%. Later, Jansen and Traudt [23] confirmed similar performance improvements in a real-world deployment of KIST within a portion of the Tor network. Geddes et al. [14] proposed the Avoiding Bottleneck Relay Algorithm (ABRA) which utilizes messaging between clients and relays to facilitate path selection in a manner that avoids over-utilized nodes, achieving nearly 20% increase in network utilization compared to vanilla Tor. Despite such efforts, latency is to be an issue for Tor users even today and addressing latency in the Tor network is a priority for the Tor Project [10].

2.2 UX of the Tor Browser

In addition to the network based approaches mentioned above, researchers have examined UX and usability considerations from the user point of view. One of the very first such efforts was a cognitive walk-through of four configurations of the Tor software performed by Clark et al. [5]. Several user interface improvements were proposed based on the difficulties users encountered while performing the study tasks. However, these results are no longer applicable as Tor has since switched to the Tor Browser as the user-facing front end for the Tor network.

Norcie et al. [33] identified the challenges individuals face in adopting and using the Tor Browser,[1] from installation through to browsing. Nearly 2/3rds of the participants in the laboratory based investigation involving 25 undergraduate students faced problems while installing or using the Tor

[1] At that time, the Tor Browser was referred to as the Tor Browser Bundle.

Browser. Norcie et al. proposed various interface modifications to address the uncovered problems, leading to notable UX and usability improvements [32]. Similar to Norcie et al., our goal was to uncover challenges and problems that led users to abandon the use of the Tor Browser for the task at hand. However, the participants of the studies of Norcie et al. [32, 33] used the Tor Browser in a laboratory setting for a short time, performing specific tasks dictated by the researchers. In contrast, our study examined use of the Tor Browser in a naturalistic setting for routine online tasks over a significantly longer period of one week.

On a different note, Victors et al. [40] proposed a DNS for onion services implemented as a Tor Browser plugin called OnioNS. OnioNS utilizes Tor network nodes and the Bitcoin mining system to assign human readable domain names to Tor Onion services, thus improving the UX by allowing individuals to access these services without the need to enter long cryptographically generated onion service names.

2.3 Tor Users

Improving the Tor Browser UX requires understanding the characteristics, attitudes, and needs of the Tor user population. In this regard, McCoy et al. [30] analyzed the traffic from an entry guard and an exit node under their control, finding that many Tor users came from Germany, Turkey, and Italy. They further discovered that a large amount of sensitive information was sent over the Tor network in plaintext. An investigation of the privacy perceptions of Americans following the government surveillance revelations of Edward Snowden found that 34% of those who were aware of the matter made greater efforts to protect their online personal information. Yet, only 2% of these individuals reported using anonymity software such as Tor. Forte et al. [12] reported that maintaining anonymity via Tor is used by some contributors to open collaboration projects (such as Wikipedia) in order to guard against risks, such as surveillance, harassment, violence, reputation loss, etc. Gallagher et al. [13] found that experts and non-experts approach Tor use in notably distinct ways and exhibit differences in understanding of Tor operation and threat model. They noted that the simplicity and misunderstandings of non-experts in particular could jeopardize anonymity due to a false sense of security. In a similar vein, Winter et al. [42] found that users struggle to understand onion services and face issues in navigating to these resources and determining their authenticity.

3 METHOD

We tackled our research objective by studying naturalistic use of the Tor Browser. In the following subsections, we describe the rationale behind our study design, details of participant recruitment and study deployment, and approaches used for data analyses, respectively.

3.1 Study Design and Instruments

We wished to collect data from individuals as they used Tor Browser for their routine online tasks. To ensure sufficient data quality and quantity, we used three separate data collection mechanisms: opportunistically timed short online questionnaires, open-ended written self reports, and one-on-one semi-structured interviews. Collectively, the three approaches were designed to meet the following requirements:

- Use a lightweight mechanism with minimal burden that does not require instructions.
- Respect privacy by avoiding capturing screens and URLs (unless provided voluntarily).
- Be independent of a specific place or time, thus allowing collection to occur at the participant's convenience.
- Capture sufficiently detailed information (as in a controlled laboratory setting).
- Span a reasonable period that constitutes extended use.

Specifically, we designed three online questionnaires to gather information whenever participants experienced a problem with the Tor Browser. Each questionnaire asked for the nature and details of the problem along with the option to provide the Web site(s) involved. If no problem was encountered, the questionnaire could be closed without answering. The questionnaires respectively targeted the following three circumstances: ending a Tor Browser session (*Tor Browser Questionnaire*), switching from the Tor Browser to another browser (*Switched Browser Questionnaire*), and starting a new browsing session directly with a non-Tor browser (*Other Browser Questionnaire*). The questionnaires are included in Appendix A.

In a laboratory setting, researchers have direct access to the participants and can trigger data collection upon observing relevant participant actions. In contrast, in a naturalistic setting, it is not straightforward to seek questionnaire input at the most opportune time. Relying on participants to remember to fill out a questionnaire each time they encounter a problem is unreliable. However, continually monitoring user activity to detect when an issue is encountered can be invasive and difficult. We addressed this aspect via a process-monitoring Python script that kept track of the creation and termination of the following browser processes: Tor Browser, Firefox, Chrome, Opera, Safari, and Edge. To detect browser processes, we used the `psutil` library [37]. For Windows, simply checking the existence of the browser process was sufficient to know whether the participant closed the application. On Mac computers, however, processes continue to run in the background even after closing the window(s) associated with them. Therefore, the Mac script used the `Quartz` library, which is part of `pyobjc` [34], to monitor active windows associated with each process. If the number of active windows fell below a pre-determined threshold unique to each browser, the browser was marked as closed. The thresholds for each browser were determined by counting the number of active browser windows with visible windows open and closed.

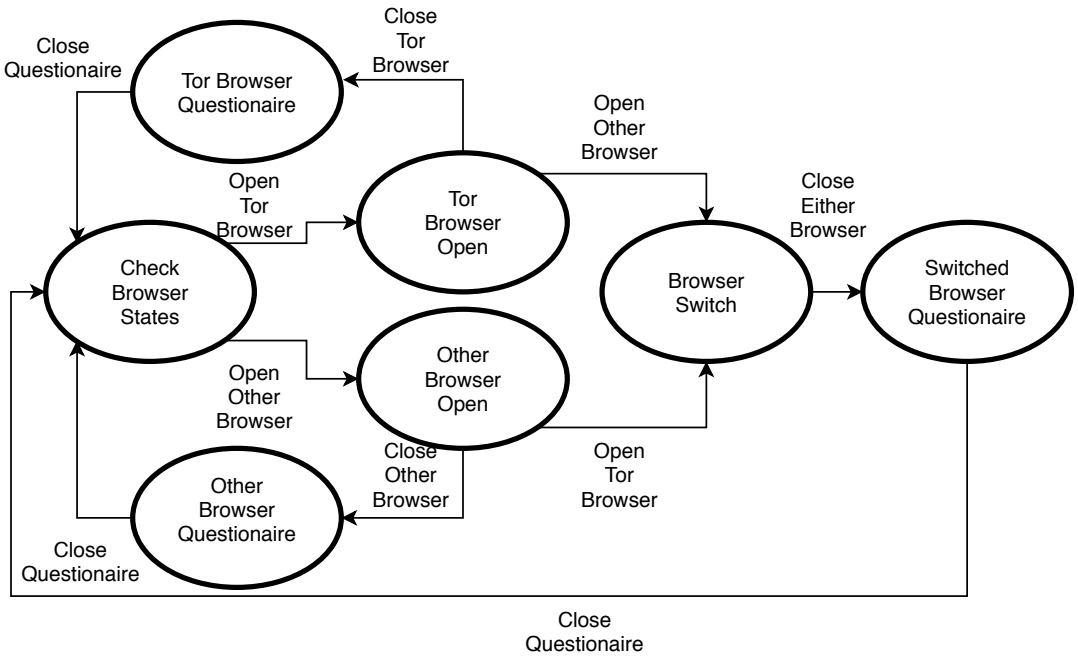

Figure 1: State and logic flow of the browser monitoring script used to select and present the appropriate questionnaire.

When the script detected that any of the browser processes were terminated, it launched the appropriate questionnaire according to the following rules:

- If Tor Browser was running and no other browsers were running, launch the Tor Browser Questionnaire.
- If Tor Browser was running along with another browser, launch the Switched Browser Questionnaire.
- If Tor Browser was not running and any other browser was running, launch the Other Browser Questionnaire.

Additionally, if no browser was closed within a 24-hour period, the script launched the Tor Browser Questionnaire. Figure 1 shows the script logic used to select the questionnaire to present. Source code for the script is available on GitHub[2] and was made available to study participants.[3]

To complement the insight captured via the questionnaire, we obtained detailed qualitative data in two ways. At the end of the study, participants provided 2-3 page write-ups reflecting on the experience of using the Tor Browser for routine online tasks (see Appendix C for the instructions provided for the write-up). In addition, we conducted brief 10-minute semi-structured interviews asking participants about the UX and challenges of using the Tor Browser (see Appendix B for the semi-structured interview guide). The write-ups and interviews served to provide context, add nuance, and corroborate information gathered via the other mechanisms.

[2]https://github.com/kcg295/TorUsabilityBrowserSensor

[3]We recognize that participants without a programming background needed to trust that our code is not malicious or engage a trustworthy individual to audit the code.

3.2 Study Procedures

The study was deployed as an assignment within an undergraduate course in the Department of Information and Library Science at Indiana University Bloomington. This sample is similar to those in previous works [13, 32, 33] and is composed of novice and non-expert users of the Tor Browser, a population whose adoption of Tor is particularly important for making Tor more inclusive and diverse in terms of its user base.

While the assignment counted toward 10% of the grade for the course, allowing the assignment data to be used for research purposes was optional and voluntary. Moreover, the grading and research aspects of the assignment were kept completely separate with the course instructor playing no part in the research and the researchers having no involvement in the grading. This separation allowed us to avoid potential coercion for research participation and prevent undue influence of grade considerations on the collected research data. To maintain anonymity during data collection, each participant was assigned a unique identifier composed of an alliterative adjective-noun pair, such as 'elegant eagle,' to be used as the participant ID when providing responses. Participants did not receive any compensation.

We first sought informed consent for study participation via a brief in-class presentation on assignment procedures and requirements followed by answering questions and providing clarifications as needed. Next, participants received detailed instructions to download and install the Tor Browser and our monitoring script. After installation, participants filled out a brief pre-study questionnaire (see Appendix D). Prior to

the start of the study, we ensured that all participants had successfully installed the Tor Browser and the monitoring script and set the Tor Browser as default browser on their primary computer.

The study lasted for one week, beginning Monday and ending the following Sunday. For the entire week, participants were asked to use the Tor Browser for all online browsing activities just as they would use any other browser. As described above, our script monitored browser processes, presenting participants with appropriate online questionnaires.[4] In some respects, our approach resembles the Experience Sampling Method [17] used in other studies [6, 7, 36]. At the end of the one-week study period, participants were provided guidance to uninstall our monitoring script and the Tor Browser, if they desired. Within a few days of study completion, participants submitted 2-3 page reports on their use of the Tor Browser during the study. In addition, we interviewed those willing to talk to us about their experiences. Each interview was audio recorded, and the audio was destroyed after transcription.

All study procedures were reviewed and approved by the Institutional Review Boards (IRBs) of Indiana University and New York University.

3.3 Data Analysis

A total of 19 students consented to participate in our research (8 female, 7 male, and 4 who did not provide demographic information) with ages ranging from 18 to 22 (average 20). Of the 15 participants who provided demographic information, one was Hispanic, two Asian, and the rest Caucasian. Only 3 of the participants indicated having used the Tor Browser prior to the study. Overall, we received 121 questionnaire responses (102 Tor Browser questionnaires, 13 Switched Browser questionnaires, and 6 Other Browser questionnaires) from 13 of the 19 participants (mean: 9.3, median: 6, and mode: 7 per participant across the 13 respondents). All 19 participants provided thorough post-study write-ups, and 11 of the 19 agreed to be interviewed.

3.3.1 Issue Categorization. In addition to choosing from the provided list of categories of issues, the online questionnaires allowed participants to enter open-ended text responses to describe the encountered problems. These open-ended responses were assigned one of the following seventeen labels generated after examining all collected responses:

(1) **Broken Web site**
(2) **Unresponsive Web site**
(3) **Streaming Content**
(4) **Reduced Productivity**
(5) **Login**
(6) **Browser Update Required**
(7) **Browser Dependent Content**
(8) **Shopping**
(9) **Specific File Types**
(10) **Latency**
(11) **Inconvenience**
(12) **Tor Traffic Block**
(13) **CAPTCHAs**
(14) **Geolocation**
(15) **Browser Crash**
(16) **Other**
(17) **No Perceived Need for the Tor Browser**

The above labels were generated by analyzing all of open-ended text responses across all questionnaires. Voluntarily provided URLs were used along with the open-ended text to generate the labels and them to responses. In 83 cases, the categories selected by the participants matched the labels assigned to the open-ended responses. In 26 cases, the open-ended responses and URLs led us to assign labels more specific than the categories chosen by the participants. In the remaining 12 cases, the text responses did not match the categories the participants selected in the questionnaires. In such cases, we labeled the issues according to the open-ended text.

After assigning labels to questionnaire responses, some labels were combined to reflect a higher-level issues, resulting in the following larger issues:

(1) **Broken Functionality**
The Web site or some functionality within the Web site was not accessible via the Tor Browser.
(2) **Latency**
The Tor Browser was unacceptably slow.
(3) **Differential Treatment**
The Web site treated Tor traffic differently.
(4) **Geolocation**
The Web site provided content based on the locale of the Tor exit node which did not match the participant's locale.
(5) **Crash**
The Tor Browser crashed or encountered an error.
(6) **Other**
The participant reported an issue not specific to the Tor Browser.

For instance, the first 9 labels were combined under the Broken Functionality aspect. Table 1 provides the full list of issues along with the respective underlying labels and counts.

3.3.2 Qualitative Coding.
Qualitative data collected via write-ups and interviews was analyzed with techniques based on Grounded Theory approaches [15]. The first author began coding the qualitative data after completing the first interview, continuing the coding process throughout the qualitative data collection activities. The analysis utilized two stages of coding: open and axial. During open coding, data was coded sentence-by-sentence and codes were created without an initial hypothesis. The first author labeled each sentence with an underlying concept. Although more attention was given to UX-relevant codes, sentences were open coded even if they did not contain a UX issue. Subsequently, the codes were examined for similarity and connections and grouped together into overarching categories via axial coding. These categories were used to

[4]The questionnaires were hosted on Qualtrics: https://qualtrics.com.

generate insight pertaining to UX problems faced by our participants. All coding and categorization was done by the first author and verified independently by the second author. RQDA [18] was used for carrying out the qualitative analyses.

4 FINDINGS

Table 1 provides quantitative details on the various issues reported in the online questionnaires broken down into the various types of problems falling under each issue. In the following subsections, we provide details regarding these issues uncovered by integrating the numeric counts with the insight gained from the analyses of the qualitative data.

4.1 Broken Functionality and Latency

As Table 1 shows, Broken Functionality and Latency were by far the most frequently and broadly encountered UX issues, with 54/121 questionnaires reporting some type of functional hindrance and 41/121 questionnaires expressing frustration with latency. Of the 13 participants who filled out the online questionnaires, 9 reported functionality breaks while 8 reported slow speeds.

Notably, breaks in desired functionality occurred in a number of different ways, ranging from completely inaccessible Web sites to a lack of support for specific operations, such as the ability to access streamed content. Seven participants reported sites that did not load within the Tor Browser at all while six mentioned being able to access a site only partially. Participants also encountered more specific functional issues, such as the inability to complete productivity tasks necessary for work or school, problems with logins, or failure in checking out online purchases.

"*Sometimes the Tor browser simply would fail to load the page or just continue to load, never reaching its goal of going to the page that I wanted to go to.*" – (P17, M, unspecified age, write-up)

"*In some cases of using Tor, certain Web sites did not work at all.*" – (P3, F, 19, write-up)

Participants reported experiencing great frustration when they could not access all features of a Web site with reasonable speed. The most common reason for the frustration was the impact on productivity. For instance, a few participants stated that the two-factor authentication scheme deployed at their workplaces did not function within the Tor Browser. Some participants could not load specific files, such as PDFs, while others were unable to access needed translation services. A few were not able to read news.

"*In my opinion, I think the ability to access all sorts of sites needs to be improved in Tor, along with the overall running speed.*" – (P3, F, 19, write-up)

Anonymity can potentially be useful for a variety of individuals, such as journalists, activists, law enforcement, or even ordinary citizens wishing to read the news without fear of retribution. Therefore, losing the ability to access Web sites that aid in productivity, learning, and information acquisition makes many beneficial uses of Tor impossible.

Although slow speeds were found annoying, when we explained that the latency is an artifact of Tor operations required to protects identity, many participants stated during the interviews that in certain circumstances they would be willing to deal with increased latency for anonymity benefits.

"*Yeah, definitely. I didn't know it was that. I knew that Tor was a much more secure way to browse the Internet but I did not know that the slowness of it was part of how it did it. Now that I know that, if for whatever reason I wanted to make sure it was really secure, I would definitely use Tor even though it is slower. I did not know that was a thing!*" – (P5, F, 19, interview)

"*Because, I mean, some things are worth waiting for to make sure I can accomplish whatever I need to.*" – (P7, F, 21, interview)

Yet, no participant provided specifics regarding the amount of tolerable latency or the acceptable level of identity protection, underscoring the difficulties in ascribing precise quantities to these subjective and contextual needs and experiences.

4.2 Inconvenience

As two of our participants pointed out, the Tor Browser lacks a number of mechanisms present in other browsers to make browsing more convenient and efficient, such as easy access to bookmarks, password saving capabilities, etc. These two participants often switched to other browsers when they needed to access a bookmarked site or a saved password that they could not easily recall.

"*The Tor browser also does not provide a lot of the ease of access quirks that a traditional browser provides. For example, it does not save your passwords which forces you to put them in manually every time.*" – (P17, M, unspecified age, write-up)

"*To elaborate on what I mean by 'ease of access,' because Google Chrome was my default browser of choice, none of my bookmarks or pre-saved information (i.e., passwords, payment information, etc.) were readily available to me while using the Tor Browser.*" – (P12, M, unspecified age, write-up)

While the questionnaire responses indicated the lack of browser conveniences to be a hindrance and, sometimes, a cause for switching to an alternate browser, we found that many participants understood that these conveniences are often a double-edged sword and including them might compromise Tor's anonymity goals.

"*I know that the goal of Tor is to allow for anonymity and privacy, so it does not store any information or have the capability to save passwords, but it was really inconvenient to have to log back into things whenever I opened the browser again.*" – (P5, F, 19, write-up)

"*I think many of the things the average user would want in a browser to make usage more efficient would counteract the*

anonymity aspect of Tor — things like having a most visited sites page, having passwords saved for certain sites, and using bookmarks at the top of the page to make navigating faster." – (P14 F, 19, write-up)

"*It also did not have some of the useful perks that a normal web browser has. I had to input my passwords in every time which is not bad; it is actually good and more secure, just inconvenient and time consuming.*" – (P17, M, unspecified age, write-up)

4.3 Differential Treatment

Two of our participants stumbled onto Web sites that treated Tor traffic differently from other network traffic (5 questionnaire reports). Such differential treatment included total blockage of traffic coming from known Tor exit nodes and an incorrect presumption of automated activity or denial-of-service attempts leading to being presented with CAPTCHAs for verifying that a human was attempting to access the resource.

"*I was going to read articles on the online news site derspiegel.de and I was trying to open articles, but it would not let me read them further.*" – (P14, F, 19, interview)

Yet, the number of incidences reporting differential treatment was much lower than our expectations based on the large amount of differential treatment for Tor traffic measured in the past [26].

4.4 Geolocation

Perhaps surprisingly, only two participants reported issues due to Web site features that depend on IP address based geolocation. Interviews and write-ups revealed that wrong geolocation due to the Tor exit node being located in another country was particularly problematic when accessing multimedia content, which is often geographically restricted, or checking email, which is often timestamped with time zone determined via geolocation.

"*When I tried to get on the site, it told me that Pandora was not active in my country just yet, just the United States.* " – (P3, F, 19, write-up)

4.5 Web Searching and Operational Messaging

Our qualitative analyses surfaced two aspects not captured in the questionnaire responses: Web searching and operational messaging.

The default search engine for the Tor Browser is DuckDuckGo which claims to provide Web search functionality without user tracking or record keeping. As a participant noted, the switch in the default search engine could potentially be confusing:

"Someone who is using Tor and does not understand IP anonymity may be confused why when they search 'Google' in the search bar it turns into 'DuckDuckGo' which may lead users to believe they are doing something incorrect and feel lost." – (P18, M, 19, write-up)

Some participants noted a number of undesirable DuckDuckGo characteristics, such as a lack of auto-complete capability, inability to revisit past search results via the 'Back' button, etc.

"I personally did not care for DuckDuckGo at all. My one big complaint is that when I was searching something it would not autocomplete like Google does. That means I had to know what specifically I was looking for and how to spell it." – (P9, F, 20, write-up)

"I did run into a quirk, and I do not know if this was due to Tor or DuckDuckGo. I use StackOverFlow to get help on coding problems and whenever I clicked back it took me to the main page of Tor and not to the list of search events. This was very frustrating because I had to retype my query and look for it again." – (P6, F, 22, write-up)

The reaction to DuckDuckGo's search results was mixed; some participants liked the results while others found them to have lower relevance and utility compared to those from other search engines.

Participants expressed a need for promoting greater operational transparency and facilitating learning via Tor messaging and communication designed to be accessible to non-experts. The need for greater and clearer information was perceived in a number of contexts: motivating Tor use, describing Tor functionality, and explaining errors.

Many participants lacked appropriate understanding of how Tor achieved the anonymity it promises and why and when online anonymity is important and useful. For instance, some participants believed that Tor was useful only in countries where freedom of expression is limited, but did not see any benefit to using it in the United States. These findings echo the results of our prior work which pointed out that non-experts typically hold simplistic mental models regarding Tor operation and the threats it counters [13].

"One thing I really wish would be explained at the beginning of the study is the difference between Tor and a VPN service, like HideMyAss or TunnelBear. I tried Googling it (or in the case of the past week, DuckDuckGoing it) but I still do not understand exactly what differentiates them." – (P4, F, unspecified age, write-up)

Several participants ran into situations in which they were puzzled by why the Tor Browser was performing specific operations or encountered error messages full of jargon that they did not comprehend. For instance, many of those who reported unresponsive Web sites stated that they did not understand why the Tor Browser was not able to access sites that seemed to pose no problems for other browsers.

". . . at home, the Tor browser would refuse to launch and would have a 'proxy server is refusing connections' message. I was

Issue	Category Labels	Description	Reports	Participants	Total Reports	Total Participants
Broken Functionality	Broken Web Site	Some part of the Web site did not work.	13	6	54	9
	Unresponsive Web Site	The Web site did not load.	13	7		
	Streaming Content	Video streaming did not work.	9	3		
	Reduced Productivity	A productivity-oriented feature could not be used.	9	3		
	Login	Logging into the Web site failed.	2	1		
	Browser Update Required	Accessing the content required a different browser version.	2	1		
	Browser Dependent Content	Accessing the content required a specific browser.	2	1		
	Shopping	A financial transaction could not be completed.	1	1		
	Specific File Types	A specific file type could not be viewed.	3	1		
Latency	Latency	Access was slow.	41	8	41	8
Inconvenience	Inconvenience	A feature present in other Web browsers was missing.	2	2	2	2
Differential Treatment	Tor Traffic Block	The Web site blocked connections from the Tor network.	2	2	5	2
	CAPTCHAs	The Web site wanted to verify that the access was by a human.	3	1		
Geolocation	Geolocation	The Web site was customized to the locale of the Tor circuit's exit node.	2	2	2	2
Crash	Browser Crash	The Tor Browser crashed.	3	3	3	3
Other	Other	The participant provided no information or reported a non-UX problem.	13	5	14	5
	No Perceived Need for the Tor Browser	The participant saw no reason to use the Tor Browser for the task at hand.	1	1		

Table 1: Participant reported UX issues along with associated report counts and number of reporting participants.

unsure of the cause of this message, but no Web pages would launch." – (P10, M, 20, write-up)

Error messages were often unhelpful for troubleshooting. The error message referred to in the above quote by P10, for example, is full of jargon and could have been caused as a result of any one of multiple problems, such as a lack of Internet connectivity or the failure to launch the Tor daemon. Similar lack of clarity was mentioned regarding messages encountered in a number of situations.

"I went to launch Tor and it got stuck on the 'loading relay information' part of connecting. It said 'this may take several minutes' but it ended up never connecting." – (P4, F, unspecified age, write-up)

4.6 Lack of Trust

Importantly, qualitative analyses showed that the lack of a "smooth and polished" UX caused more than mere frustration; it led some participants to associate the problems with a general lack of trustworthiness and reliability.

"*I experienced only two Web sites crashing but it lessened my trust in regards to the reliability of the Tor browser.*" – (P10, M, 20, write-up)

"*This was not always the case but its unreliability also made me not trust the Tor service as much.*" – (P1, M, 22, write-up)

The reduced trust further led to feelings of less security compared to other browser alternatives, thus defeating the central promised benefit of Tor.

"*...it felt less secure and smooth than the official browsing options (Firefox, Safari, Microsoft Edge, Chrome, etc).*" – (P10, M, 20, write-up)

4.7 Benefits

On a positive note, qualitative analyses revealed several aspects of the Tor Browser participants deemed beneficial and enjoyable. For instance, participants appreciated that the Tor Browser was easy to install and enjoyed the anti-tracking advertising-free browsing experience in the Tor Browser. For one participant, the Tor Browser solved an `SSL` certificate issue, potentially preventing a Man-in-the-Middle attack.

"For some reason, a few days before the study started, the laptop started tweaking, saying that it did not trust the certificates for [some] sites and would not let me navigate to them. It was incredibly frustrating, but when I accessed the same sites via Tor once the study began, there were no error messages and I could go straight to the sites with no issues." – (P11, F, unspecified age, write-up)

Several participants perceived using the Tor Browser as a learning experience. For instance, some Tor Browser warnings made them aware of threats to anonymity they had not previously considered, such as `HTML5` canvas data, window maximization, etc.

"I really enjoyed that when you resize the Tor window, it notifies you that, while you may choose to do so, it actually makes your device more vulnerable. I had no idea that this was an issue and was very pleased that Tor let me know this." – (P11, F, unspecified age, write-up)

Similarly, participants found it illuminating to consult the circuit information, which many felt was well-presented and useful.

"One really cool tool that Tor offers is the map of where the IP address is being rerouted — seeing that the circuit is being bounced around back and forth to other countries." – (P1, M, 22, write-up)

"I loved that I was able to see the circuit that the browsing session was being routed through and how it bounced around different countries." – (P5, F, 19, write-up)

Notably, when using the Tor Browser, many participants reported an overall feeling of anonymity and privacy which was typically characterized as desirable.

"Upon starting to use the Tor browser, it felt pretty good and unique to be able to browse the Internet without concern of being watched or surveilled, I felt like I had more liberties and

discretion in what Web pages I visited without the concern of surveillance." – (P8, M, unspecified age, write-up)

5 DISCUSSION AND IMPLICATIONS

Our naturalistic approach was able to uncover a number of UX considerations that were not noted in previous studies of Tor use carried out in the laboratory where the settings and the study designs imposed constraints on the tasks and the time. In the following subsections, we discuss the most salient UX insight derived from our findings and apply it to suggest solutions to tackle the corresponding issues and improve the Tor Browser UX.

5.1 Broken Functionality and Latency

Although Broken Functionality and Latency were the most frequently encountered and the most frustrating for our participants, the causes behind the issues were often unknown or unclear. Participants experienced that the site did not load or function as expected but received no explanatory warnings or errors from the Tor Browser. There are, of course, a number of possible reasons behind broken site functionality within the Tor Browser, such as blocked JavaScript, server time outs, dependencies on plug-ins, Tor traffic blocks, etc. The reasons remain opaque since users merely experience that the site failed to operate as desired. Moreover, it is typically unclear to users that many of the issues arise due to the mechanisms needed to provide anonymity or restrictions on Tor imposed by external parties. As a result, users may incorrectly conclude that the Tor Browser is buggy, unreliable, and ineffective compared to alternate browsers. For example, two of our participants were unable to view PDF files. We suspect that the problem arose because of the specifics of the PDF generation and serving mechanisms used by the sites involved. However, in the absence of any information regarding why the files could not be viewed, the participants assumed that the Tor Browser could not handle PDF files.

In anonymity systems such as Tor, there is an inherent tradeoff between anonymity and latency. Much research is devoted to improving access speeds over the Tor network, mostly addressing traffic routing, and the Tor Project engages in outreach aimed at growing the number of volunteer-run relays in order to boost available resources, thus helping reduce latency. Despite these efforts, latency remains a UX challenge. Additional research on sophisticated approaches that alleviate traffic congestion in the Tor network [1–4, 14, 20, 23, 25] may provide noticeable speed improvements. Such approaches involve improved path selection that avoids overloading nodes and fixing the slowness induced by TCP mechanisms, such as head-of-the-line blocking. It may also be fruitful to explore whether the UDP protocol could be incorporated to help reduce latency.

Solution: Inform users about potential causes for broken functionality and latency. Perhaps the most straightforward way to address broken functionality is informing users why a Web site does not work with Tor. If the Tor Browser or a browser extension blocks content, users should be able to determine what was blocked and understand why. Of course, such explanatory information must avoid jargon and technical detail that non-experts may not follow.

A similar approach could be used for latency as well. For example, until a page loads, the Tor Browser could explain latency within a local page that is replaced when the desired page is ready to be rendered (i.e., HTTP 200 is received). Another possibility is to measure Round-Trip Time (RTT) between the client and the exit node by having the exit node acknowledge a Tor cell. If the RTT is above a specified threshold, the user could be alerted that higher latency should be expected as long as RTT remains high. As recommended by Norcie et al. [32], it may be useful to remind users that latency is an artifact of anonymity protection. As mentioned earlier, our participants were more willing to tolerate slower speeds when they understood those as necessary to benefit from the anonymity offered by onion routing. It is important that such messages are delivered unobtrusively, avoiding invasive techniques like pop-ups that are likely to be dismissed as an annoyance.

Solution: Provides means to generate Tor-friendly pages. In order to facilitate content delivery in a manner that fits the constraints imposed by the Tor Browser, content and site developers could be encouraged to support 'Tor-friendly' versions of Web pages. To that end, tools could developed to analyze Web pages and provide a Tor-friendliness rating along with a list of actionable suggestions that could be implemented to improve the rating. Web sites are often built on top of content management systems (CMS), such as Wordpress, that use templates and plug-ins with features that may not work within the Tor Browser. A potential solution is to provide plug-ins and templates that function in a Tor-friendly manner. For example, a Wordpress login plug-in could be built to handle user authentication without requiring the use of JavaScript. Further, existing CMS plug-ins could be tested and certified as Tor-friendly if they meet the appropriate criteria. These suggestions, however, involve addressing several challenges. First, 'Tor-friendliness' needs to be defined and measured. Second, content and service providers must be encouraged and incentivized to adopt the tools and provide Tor-friendly versions. Third, the tools will need to work in conjunction with other mechanisms that can get around Tor traffic blocks or other forms of Tor censorship.

5.2 Inconvenience

Many users have come to rely on common browser features, such as password managers, bookmarks, history, session tracking, cookies, etc., that make browsing convenient and efficient. The amnesiac property of the Tor Browser forgoes such features in order to provide protection against certain adversaries, especially those that could potentially gain access to the user's machine. Against other adversaries, however, a lack of these features creates an inconvenience with no benefit. That said, as our participants correctly discerned, implementation of some of these features could potentially compromise privacy and security. For instance, password

managers with lax auto-fill policies have been shown to introduce attacks that otherwise would not have been possible [38]. Additionally, lenient treatment of cookies could cause Web activities to be tracked. More research is needed to determine the potential effects of including these convenience features in the Tor Browser. Such features are particularly important for novices, who often begin using the Tor Browser out of curiosity [13]; inconveniences may make them give up using the Tor Browser before they have had the chance to learn and experience its benefits.

Solution: Modify the security slider settings to allow convenience features at lower anonymity levels. Perhaps a reasonable solution is allowing convenience features when the Tor Browser is set for the lowest level of security, i.e., the security slider setting is set to 'Standard.' This would allow users to maintain many of the familiar browsing conveniences while still allowing those who require stronger protections to disable the features easily by raising the security level via the slider settings. Since the security slider is currently set to 'Standard' by default, an alternative implementation could add another setting level that enables convenience features without affecting the currently implemented settings.

Solution: Provide the ability to specify threats of relevance to the user. The security slider settings within the Tor Browser already address various threat models. However, most of the differences among the different settings of the slider pertain to user tracking and identification mechanisms and capabilities of remote adversaries. The security slider functionality could be extended to consider other adversaries, such as those with physical access to the user's computer. In addition to being controlled via the security slider, convenience features could be selectively enabled based on user input regarding threats and use cases of importance. For instance, at the time of installation, the Tor Browser could launch a 'threat selection dialog' that allows the user to specify the threat(s) from which protection is desired, e.g., mass surveillance, censorship, advertiser profiling, etc. Based on user selections, and potentially other relevant aspects, such as country of use, features within the browser could be activated to achieve an optimal balance between convenience and privacy. Research is needed to determine the potential anonymity impact of the convenience features and the criteria for achieving the desired balance between convenience and privacy. Further, users should be able to invoke the threat selection dialog as needed in order to account for changes in needs and contexts.

5.3 Differential Treatment

A notable portion of the difficulties faced by Tor users are not technical, but political. Many Web site operators as well as powerful corporate and government entities block connections from the Tor network entirely. Moreover, it is not straightforward to determine who is blocking Tor traffic and why. Unless users are able to connect via an unpublished Tor exit node or use a proxy after the Tor exit node, it is difficult to avoid such blocks. Currently, the best countermeasure is working with Web site operators and security software vendors to create exceptions for Tor. However, such a process could be time and resource consuming, especially for a small entity like the Tor project.

Solution: Crowdsource the reporting of differential treatment of Tor traffic. It might be expedient to detect and report Tor traffic blocks by distributing the effort among Tor users via crowdsourcing techniques. For instance, the Tor Browser could include a 'Report connection problem' button that allows users to flag offending resources, thus facilitating monitoring and prioritization based on reporting frequency and problem severity. The crowd could perhaps also be leveraged to monitor and maintain the database of reports. Such reporting mechanisms could be extended to provide lightweight features for collecting and processing voluntary and anonymous user feedback regarding UX issues in general.

Solution: Explore alternative ways to deliver blocked content. When a resource cannot be reached via the Tor Browser, it may still be possible to access the content through the use of services that archive or cache Internet content. For instance, the Tor Browser could incorporate mechanisms that allow searching for content on Internet archives such as the Wayback Machine [41] and within search engine caches, thus facilitating access to the content without sacrificing anonymity by accessing the blocked content in another browser.

5.4 Geolocation

Many Web sites customize content delivery based on the location determined by the user's IP address. For instance, such customization is utilized to set the appropriate language, display prices in the local currency, enforce intellectual property restrictions, etc. If the Tor Browser routes a user's traffic through an exit node in a country other than where the user is located, the delivered content ends up being wrongly customized from the user's point of view. Currently, specifying the desired country for exit nodes requires modifying the Tor run-time configuration file, `torrc`. This file can be complicated to handle and difficult to edit correctly, especially for non-experts.

Solution: Allow easy specification of desired exit node location. The ability to switch the preferred location of the exit node could be included within the set of settings that can be adjusted within the Tor Browser's graphical user interface. Such a feature must be accompanied by clear warnings that choosing to limit exit nodes to a specific country reduces the number of potential circuits, thus reducing the level of anonymity. The ability to set exit node location could be disabled at higher security levels as indicated by the security slider settings or based on the threats and adversaries selected by the user in the threat selection dialog mentioned above.

5.5 Operational Messaging

Novices and non-experts lack sophisticated operational understanding of Tor and anonymity compromising mechanisms [13]. As a result, it is important that the UX provide operational transparency and facilitate user learning. However, our participants found messaging within the Tor Browser to be inadequate and inaccessible, leading to confusion, frustration, and lack of trust.

Solution: Deliver contextually relevant information during user sessions. Most users lack the time or the patience to read long manuals or view tutorials. However, short messages relevant to the user's context delivered appropriately during use could be an effective means of communication, as demonstrated by the engagement of our participants with warnings related to screen maximization and `HTML5` canvas data extraction and the visualization related to traffic routing. Such mechanisms could be used for further text messages and visual indicators that help users relate the UX with operational detail. Useful information snippets could also be made available when the Tor Browser is first launched as well as on the `about:tor` and https://check.torproject.org pages. The UX for the delivery of such messages should be carefully designed to avoid unduly interrupting or distracting the user.

Solution: Craft errors, warnings, and other user communication in language accessible to non-experts. Information provided to users is useful only if they can understand it and take appropriate action. Therefore, messages should be crafted to avoid jargon and ensure understanding without requiring in-depth technical knowledge. To this end, evaluating message text via user studies could help improve its readability for a general audience.

6 LIMITATIONS

A few limitations must be kept in mind when considering the generalizability of these findings. Our sample is small and homogenous in terms of age, education, and cultural background. Moreover, the research was carried out in the United States where the nature of threats to civil liberties is different from that encountered in other places across the world. Further research is needed to uncover additional UX aspects that might be salient in other types of populations.

Most of our participants were not familiar with Tor prior to the study, thus representing novice and non-expert users. While UX considerations for experts may be somewhat different, increasing Tor adoption and use requires a greater focus on novices and non-experts who constitute the majority of the population.

One participant mentioned changing browsing activities during the study because of the monitoring of browser state transitions by our script. In contrast, it is possible that the privacy protection of Tor led our participants to access resources that they might not otherwise have sought in the course of routine "non-private" browsing. Additionally, given the nature of our study, participants may have been more tolerant of errors than they would be in a typical browsing session. Although such deviations from normal browsing practices may have slightly reduced the naturalistic aspect of our data, we note that only one participant reported engaging in browsing behavior during the study that differed from typical online practices.

Since our browser monitoring script relied on various heuristics to determine browser state transitions, it was prone to the occasional false positives that led to unnecessary presentation of questionnaires, evoking pop-up fatigue in some participants. Similarly, it is possible that the script missed some browser transitions and failed to present a questionnaire even when warranted, thus missing the opportunity for collecting data. Moreover, the script covered only traditional desktop or laptop computers, missing coverage of browsing activities from mobile devices, such as smartphones and tablets, which are increasingly becoming the dominant mode of online access for a large proportion of the population. A few participants reported that the study did not capture the full extent of their Web use because they utilized their mobile devices for most of their Web browsing activities during the study period. As Web access via mobile devices continues to increase at a rapid pace, our study would need to be replicated in order to capture UX problems specific to Tor based mobile applications.

Additional quantitative data and finer grained information could potentially have shed more light on some of the issues we discovered. For instance, an in-depth analysis of broken functionality issues was infeasible due to the limited information available in participant self-reports. A potential solution could combine self-reports with information collection within the Tor Browser on relevant aspects such as load times, blocked page elements, etc. It is difficult, if not impossible, to collect such data privately, thus leading to a tension between the goals of the research and the Tor Browser.

7 FUTURE WORK

Our findings point to several opportunities for future UX research involving the Tor Browser and the Tor anonymity network. Section 5 outlines a number of suggestions for improving the Tor Browser UX. The effectiveness of these suggestions needs to be validated through empirical studies with Tor users, preferably in naturalistic settings. Many advanced aspects of Tor use, such as setting up relays, accessing or running Onion services, etc., were not examined in our study. Evaluating and improving the UX of these aspects could further help Tor become more accessible to the general population. Such investigations could also tackle specialized uses targeted at specific populations and use cases, such as SecureDrop for journalists and their sources.

Future work could also address some of the limitations of our study outlined in Section 6. For instance, a mechanism that allows private collection of Tor Browser telemetry to augment user self-reports can be particularly useful. Such browser-collected information could include load times, blocked page elements, JavaScript profiling, and URLs pertaining to resources that lead to UX problems. Similarly, our

study could be replicated to cover other populations, such as experts or users in different political climates, to surface UX issues that our sample may not have encountered.

8 CONCLUSION

Increasing surveillance of online activities by corporate and state actors has led to growing adoption of anonymity-preserving tools such as Tor. As Tor expands to a mainstream user base composed of novices and non-experts, the UX becomes an increasingly important factor for facilitating adoption and continued use. Our mixed-methods study is an important first step in studying the Tor Browser UX in a naturalistic setting. Parts of our approach could be deployed to collect anonymous user input at scale. We offer a number of actionable suggestions to mitigate the various UX challenges uncovered by our study. Next steps involve implementing the proposed solutions and evaluating their effectiveness in improving the Tor Browser UX for routine use by the general population.

ACKNOWLEDGEMENTS

We are grateful to Carol Choksy for allowing us access to the students in her course. We would like to thank those who participated in our study. We also thank the anonymous reviewers for valuable feedback. We acknowledge Dennis Röllke, Hossein Siadati, and Santiago Torres for editorial input on draft versions of this paper. This work was made possible in part by NPRP grant 7-1469-1-273 from the Qatar National Research Fund (a member of the Qatar Foundation) and gifts from Comcast and Google. The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] Masoud Akhoondi, Curtis Yu, and Harsha V Madhyastha. 2012. LASTor: A low-latency AS-aware Tor client. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy (S&P 2012)*. IEEE, 476–490.

[2] Mashael AlSabah, Kevin Bauer, Tariq Elahi, and Ian Goldberg. 2013. The path less travelled: Overcoming Tor's bottlenecks with traffic splitting. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 143–163.

[3] Mashael AlSabah, Kevin Bauer, and Ian Goldberg. 2012. Enhancing Tor's performance using real-time traffic classification. In *Proceedings of the 2012 ACM conference on Computer and Communications Security (CCS 2012)*. ACM, 73–84.

[4] Mashael AlSabah, Kevin Bauer, Ian Goldberg, Dirk Grunwald, Damon McCoy, Stefan Savage, and Geoffrey M Voelker. 2011. DefenestraTor: Throwing out windows in Tor. In *Proceedings of the 11th Privacy Enhancing Technologies Symposium (PETS 2011)*. Springer, 134–154.

[5] Jeremy Clark, Paul C Van Oorschot, and Carlisle Adams. 2007. Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS 2007)*. ACM, 41–51.

[6] Sunny Consolvo, Frank R Bentley, Eric B Hekler, and Sayali S Phatak. 2017. Mobile user research: A practical guide. *Synthesis Lectures on Mobile and Pervasive Computing* 9, 1 (2017), i–195.

[7] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI 2005)*. ACM, 81–90.

[8] Roger Dingledine and Nick Mathewson. 2006. Anonymity Loves Company: Usability and the Network Effect. In *Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006)*.

[9] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-generation Onion Router. In *Proceedings of the 13th Conference on USENIX Security Symposium (USENIX Security 2004)*. USENIX Association, 21–21. http://dl.acm.org/citation.cfm?id=1251375.1251396

[10] Roger Dingledine and Steven J. Murdoch. 2009. Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it. https://www.torproject.org/press/presskit/2009-03-11-performance.pdf. (2009). Accessed: 2017-06-15.

[11] Benjamin Fabian, Florian Goertz, Steffen Kunz, Sebastian Müller, and Mathias Nitzsche. 2010. Privately waiting–A usability analysis of the Tor anonymity network. In *Sustainable e-Business Management*. Springer, 63–75.

[12] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. 2017. Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians. In *Proceedings of the 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2017)*. 1800–1811.

[13] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. 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)*. USENIX Association, 385–398.

[14] John Geddes, Michael Schliep, and Nicholas Hopper. 2016. ABRA CADABRA: Magically Increasing Network Utilization in Tor by Avoiding Bottlenecks. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2016)*.

[15] Barney G Glaser and Anselm L Strauss. 2009. *The discovery of grounded theory: Strategies for qualitative research*. Transaction Publishers.

[16] Virgil Griffith. 2014. *Tor Growth Rates and Improving Torperf Throughput*. Technical Report 2014-10-001. The Tor Project. https://research.torproject.org/techreports/tor-growth-2014-10-04.pdf

[17] Stefan E Hormuth. 1986. The sampling of experiences in situ. *Journal of personality* 54, 1 (1986), 262–293.

[18] Ronggui Huang. 2018. *RQDA: R-based Qualitative Data Analysis*. http://rqda.r-forge.r-project.org R package version 0.3-1.

[19] Aaron D Jaggard, Aaron Johnson, Sarah Cortes, Paul Syverson, and Joan Feigenbaum. 2015. 20,000 in League under the Sea: Anonymous Communication, Trust, MLATs, and Undersea Cables. In *Proceedings on Privacy Enhancing Technologies (PoPETS 2015)*. De Gruyter Open, 4–24.

[20] Rob Jansen, John Geddes, Chris Wacek, Micah Sherr, and Paul Syverson. 2014. Never Been KIST: Tor's Congestion Management Blossoms with Kernel-Informed Socket Transport. In *23rd USENIX Security Symposium (USENIX Security 14)*. USENIX Association, San Diego, CA, 127–142. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/jansen

[21] Rob Jansen and Aaron Johnson. 2016. Safely Measuring Tor. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS 2016)*. ACM, 1553–1567.

[22] Rob Jansen, Marc Juarez, Rafa Gálvez, Tariq Elahi, and Claudia Diaz. 2017. Inside Job: Applying Traffic Analysis to Measure Tor from Within. In *Network and Distributed System Security Symposium (NDSS 2017)*. IEEE Internet Society.

[23] Rob Jansen and Matthew Traudt. 2017. Tor's Been KIST: A Case Study of Transitioning Tor Research to Practice. *arXiv preprint arXiv:1709.01044* (2017).

[24] Rob Jansen, Florian Tschorsch, Aaron Johnson, and Björn Scheuermann. 2014. The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network. In *Proceedings of the Network and Distributed System Security Symposium 2014 (NDSS 2014)*. Internet Society.

[25] Aaron Johnson, Rob Jansen, Nicholas Hopper, Aaron Segal, and Paul Syverson. 2017. PeerFlow: Secure Load Balancing in Tor. *Proceedings on Privacy Enhancing Technologies (PETS 2017)* 2017, 2 (April 2017).

[26] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Damon McCoy, Vern Paxson, and Steven J Murdoch. 2016. Do You See What I See? Differential Treatment of Anonymous Users. In *Proceedings of the Network and Distributed Systems Security Symposium (NDSS 2016)*, Vol. 16. 21–24.

[27] Stefan Köpsell. 2006. Low Latency Anonymous Communication – How Long Are Users Willing to Wait?. In *Proceedings of Emerging*

Trends in Information and Communication Security (ETRICS 2006). Springer, 221–237. https://doi.org/10.1007/11766155_16

[28] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. 2017. A Usability Evaluation of Tor Launcher. *Proceedings on Privacy Enhancing Technologies (PETS 2017)* 2017, 3 (2017), 90–109.

[29] Srdjan Matic, Platon Kotzias, and Juan Caballero. 2015. CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS 2015)*. ACM, 1455–1466.

[30] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2008. Shining Light in Dark Places: Understanding the Tor Network. In *Proceedings of the 8th International Privacy Enhancing Technologies Syposium (PETS 2008)*. Springer, 63–76. https://doi.org/10.1007/978-3-540-70630-4_5

[31] Helen Nissenbaum. 1999. The meaning of anonymity in an information age. *The Information Society* 15, 2 (1999), 141–144.

[32] Greg Norcie, Jim Blythe, Kelly Caine, and L. Jean Camp. 2014. Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. In *Proceedings of the 2014 Workshop on Usable Security (USEC 2014)*. Internet Society. https://doi.org/10.14722/usec.2014.23022

[33] Greg Norcie, Kelly Caine, and L Jean Camp. 2012. 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 2012)*.

[34] Ronald Oussoren. 2018. PyObjC. https://bitbucket.org/ronaldoussoren/pyobjc/src. (2018).

[35] Rebekah Overdorf, Mark Juarez, Gunes Acar, Rachel Greenstadt, and Claudia Diaz. 2017. How Unique is Your .onion?: An Analysis of the Fingerprintability of Tor Onion Services. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017)*. ACM, 2021–2036.

[36] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI 2018)*. ACM, 512.

[37] Giampaolo Rodolà. 2018. psutil. https://github.com/giampaolo/psutil. (2018).

[38] David Silver, Suman Jana, Dan Boneh, Eric Yawei Chen, and Collin Jackson. 2014. Password Managers: Attacks and Defenses. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 2014)*. 449–464.

[39] Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang, and Prateek Mittal. 2015. RAPTOR: Routing Attacks on Privacy in Tor. In *Proceedings of the 24th USENIX Security Symposium (USENIX Security 2015)*. USENIX Association, 271–286. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sun

[40] Jesse Victors, Ming Li, and Xinwen Fu. 2017. The Onion Name System: Tor-powered Decentralized DNS for Tor Onion Services. *Proceedings on Privacy Enhancing Technologies (PETS 2017)* 2017, 1 (January 2017).

[41] Wayback Machine. 2018. Wayback Machine. (2018). http://archive.org/web/

[42] Philipp Winter, Anne Edmundson, Laura M. Roberts, Agnieszka Dutkowska-Żuk, Marshini Chetty, and Nick Feamster. 2018. How Do Tor Users Interact With Onion Services?. In *27th USENIX Security Symposium (USENIX Security 2018)*. USENIX Association, Baltimore, MD, 411–428.

[43] Philipp Winter and Stefan Lindskog. 2012. How the Great Firewall of China is Blocking Tor. In *Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 2012)*. USENIX Association. https://www.usenix.org/conference/foci12/workshop-program/presentation/Winter

[44] Mary Ellen Zurko and Richard T. Simon. 1996. User-centered Security. In *Proceedings of the 1996 Workshop on New Security Paradigms (NSPW 1996)*. ACM, 27–33. https://doi.org/10.1145/304851.304859

A QUESTIONNAIRES

A.1 Tor Browser Questionnaire

(1) Please enter your participant ID:
(2) Which of the following best describes the issue(s) you encountered? (*Check all that apply.*)
  (a) The Tor Browser was slow.
  (b) Some parts of the Web site I wanted to view did not work.
  (c) Many Web sites wanted to verify that I was human.
  (d) The Tor Browser crashed.
  (e) The Web site I wanted to view did not load in the Tor Browser.
  (f) The Web site blocked the Tor Browser.
  (g) I did not need the Tor Browser for the task at hand.
  (h) I did not know how to proceed via the Tor Browser.
  (i) The Web site I wanted to view was in an incorrect language or currency or showed results for a location far from me.
  (j) The Web site I wanted to view prevented me from performing a specific action (e.g., logging in, posting a comment, etc.).
  (k) I experienced an issue other than those mentioned above.
(3) Please provide more details on the above issue(s) you encountered:
(4) (*Optional*) Please specify the address (URL(s)) of the Web site(s) that you were browsing when you encountered the above issue(s):

A.2 Switched Browser Questionnaire

(1) Please enter your participant ID:
(2) Did you encounter any issues with the Tor Browser that caused you to switch to another browser?[5]
  (a) Yes
  (b) No
  (c) Not Applicable: I did not switch to another browser from the Tor Browser.
(3) Which of the following best describe the issue(s) you encountered? (*Check all that apply.*)
  (a) The Tor Browser was slow.
  (b) Some parts of the Web site I wanted to view did not work.
  (c) Many Web sites wanted to verify that I was human.
  (d) The Tor Browser crashed.
  (e) The Web site I wanted to view did not load in the Tor Browser.
  (f) The Web site blocked the Tor Browser.
  (g) I did not need the Tor Browser for the task at hand.
  (h) I did not know how to proceed via the Tor Browser.
  (i) The Web site I wanted to view was in an incorrect language or currency or showed results for a location far from me.
  (j) The Web site I wanted to view prevented me from performing a specific action (e.g., logging in, posting a comment, etc.).
  (k) I experienced an issue other than those mentioned above.
(4) Please provide more details on the above issue(s) you encountered:
(5) (*Optional*) Please specify the address (URL(s)) of the Web site(s) that you were browsing when you encountered the above issue(s):

[5] If the participant did not answer 'Yes,' he or she was not presented further questions.

A.3 Other Browser Questionnaire

(1) Please enter your participant ID:
(2) Which browser did you use during this browsing session?
  (a) Edge
  (b) Chrome
  (c) Firefox
  (d) Safari
  (e) Opera
  (f) Other. Please specify:
(3) Why did you use the above browser instead of the Tor Browser? (*Check all that apply.*)
  (a) I forgot to use the Tor Browser.
  (b) I was annoyed with using the Tor Browser.
  (c) I did not want to use the Tor Browser for this session.
  (d) The Tor Browser was slow.
  (e) Some parts of the Web site I wanted to view did not work in the Tor Browser.
  (f) Many Web sites wanted to verify that I was human.
  (g) The Web site I wanted to view did not load in the Tor Browser.
  (h) The Web site I wanted to view blocked the Tor Browser.
  (i) I did not need the Tor Browser for the task at hand.
  (j) I did not know how to proceed via the Tor Browser.
  (k) The Web site I wanted to view prevented me from performing a specific action (e.g., logging in, posting a comment, etc.).
  (l) None of the above.
(4) Please provide more details regarding the above reason(s):
(5) Which category of Web sites were you browsing during this session? (*Check all that apply.*)
  (a) Adult
  (b) Arts
  (c) Business
  (d) Communication (e.g., emails, chat, conferencing, etc.)
  (e) Computers
  (f) Games
  (g) Health
  (h) Home
  (i) Kids and Teens
  (j) Lifestyle
  (k) News

(l) Recreation
(m) Reference
(n) Regional
(o) Social Media
(p) Science
(q) Shopping
(r) Society
(s) Sports
(t) Technology
(u) World

B INTERVIEW QUESTIONS

Please keep in mind that there are no incorrect answers to these questions. Any answers you provide will remain strictly confidential with access limited only to the research team unless otherwise required by law. Additionally, you may refuse to answer any question. All questions are optional.

This interview will be recorded to aid in the analysis performed by the researchers. After the interview is transcribed, the audio data will be deleted. Anonymous transcribed data will be retained indefinitely. If you wish, you can request that the recording device be disabled at any time.

Do you consent to the audio recording of this interview?

Do you consent to the indefinite retention of the anonymous transcribed interview data?

(1) Please describe your experience using the Tor Browser.
(2) Please tell us about some of the issues you encountered using the Tor Browser as your default browser.
  (a) Could you elaborate on the issue?
  (b) Did you encounter this issue more times than you reported it in the online questionnaires?
  (c) On which categories of Web sites did this issue occur?
  (d) Would this issue hinder you from using the Tor Browser in the future?
(3) Will you continue using the Tor Browser after this study? Why or why not?
(4) In your opinion, which of the issues you encountered while using the Tor Browser caused the most confusion and/or frustration?
(5) One issue many Tor Browser users face is long waiting times (high latency). However, this latency can be an artifact of how Tor protects your identity. Indeed, in some instances latency and anonymity are transactional: higher latency can lead to better protection. Knowing this, are there certain tasks for which you would be willing to tolerate latency to gain anonymity?
(6) Are there any other issues that you encountered while using the Tor Browser that you wish to report?
(7) Is there anything else I should have asked?

C WRITE-UP PROMPT

Write an essay of about 2-3 single-spaced pages about your experience of using the Tor Browser as your default and primary browser for the duration of one week. Your essay should describe your positive and negative experiences with the user interface and user experience of the Tor Browser. Please provide specific examples along with respective relevant contextual details. Please include a discussion of what you learned specifically about the Tor Browser and Tor as well as generally about Web technology, anonymity, surveillance, etc. Feel free to propose creative solutions or improvements that could have helped you utilize the Tor Browser more effectively. Please also indicate whether your browsing behavior during the study period was typical of your browsing behavior at other times. If your browsing practices during the study period differed from your typical practices, please explain how and why. You may also comment on your study participation experience, such as the questionnaires prompted by the script throughout the week.

D PRESTUDY QUESTIONNAIRE

[Information about Study Procedures]

(1) Do you agree to participate in this study?
(2) Please enter your participant ID:
(3) What is your year of birth?
(4) What is your current nationality?
(5) How long have you lived in the US?
(6) What is your gender?
  • Male
  • Female
  • Other
  • Do not wish to specify
(7) What is your ethnicity?
  • American Indian or Native American
  • Asian
  • Black or African American
  • Hispanic
  • Native Hawaiian or Other Pacific Islander
  • White / Caucasian
  • Other
  • Do not wish to specify
(8) What is your major field of study?
(9) What is your current employment status?
  • Employed full time
  • Employed part time
  • Unemployed looking for work
  • Unemployed not looking for work
  • Retired
  • Homemaker
  • Unable to work
  • Do not wish to specify
(10) Have you used the Tor Browser before?
  • Yes
  • No
  • Not sure
(11) What is the operating system of the computer (desktop or laptop) that you use as your primary computer?
  • Windows
  • MacOS
  • Linux
  • Other
(12) What is the operating system of your primary phone?
  • iOS

- Android
- Other

(13) Have you successfully installed the Tor Browser on your computer(s), and, if you wish, your mobile device(s)?
- Yes
- No

(14) Have you successfully installed our script on your computer?
- Yes
- No