ReporTor: Facilitating User Reporting of Issues Encountered in Naturalistic Web Browsing via Tor Browser

Nicholas Micallef
Swansea University
Swansea, Wales, United Kingdom
nicholas.micallef@swansea.ac.uk

Cameron Cartier
Black Hills Information Security, Inc.
Sturgis, South Dakota, United States
cameron@blackhillsinfosec.com

Kevin Gallagher
NOVA LINCS, NOVA School of Science and Technology
Lisbon, Portugal
k.gallagher@fct.unl.pt

Lucas Zagal
University of Utah
Salt Lake City, Utah, United States
lucas.zagal@utah.edu

Sameer Patil
University of Utah
Salt Lake City, Utah, United States
sameer.patil@utah.edu

Abstract

The privacy properties of Tor Browser and the privacy sensitivity of its user base preclude the collection of traditional telemetry and analytics to understand the problems users face. To address the lack of telemetry and analytics, we developed ReporTor, a plugin to facilitate anonymous, voluntary reporting of problems during naturalistic browsing via Tor Browser. We confirmed the utility and effectiveness of ReporTor by reporting the problems we encountered during a month of naturalistic web browsing via Tor Browser. Reports submitted via ReporTor enabled nuanced, in-depth analysis of the causes underlying the reported problems. Integrating ReporTor into Tor Browser can leverage its anonymous user-driven issue reporting to surface the challenges users encounter when visiting websites with Tor Browser. Analyzing and addressing the reports can enhance the user experience of Tor Browser for everyday web browsing.

Keywords

Tor, Tor Browser, User Experience, Privacy, Anonymity, Issue Reports

1 Introduction

Tor Browser [75] is an essential privacy-protecting tool that allows users to browse online resources with a level of anonymity far greater than that possible with other browsers. Each day, millions across the globe use Tor Browser to protect their privacy, ensure online safety, and assert civil liberties when engaging in online activities. Tor Browser is considered indispensable by many individuals from various vulnerable populations, such as civil rights activists, journalists, whistleblowers, etc. As online tracking—for advertising, surveillance, or otherwise [26, 58]—becomes increasingly challenging to counter [57], greater adoption of Tor Browser as a privacy-protective mechanism is important for *everyone*.

The level of anonymity Tor Browser can provide inherently increases with the number of users [20]. As a result, the utility and protection that Tor Browser can offer can be enhanced by mainstream adoption. However, users of Tor Browser tend to face challenges that are not typically encountered when using other browsers. For instance, the mechanisms of Tor Browser that guard against privacy-invasive features of websites make many websites practically unusable. Moreover, Internet infrastructure services, such as firewalls or Content Delivery Networks (CDNs), often flag users of Tor Browser as potentially malicious [40]. Such issues specific to Tor Browser create a subpar user experience compared to alternate browsers in which users do not face these obstacles, albeit at the cost of compromised privacy [30]. Uncovering and fixing the user experience challenges faced while using Tor Browser would not just benefit the users who experience these problems, but could also help promote greater adoption of Tor Browser by *others*, thus enhancing anonymity for the entire user base [20].

Many user experience problems in web browsers can be identified and mitigated by analyzing telemetry and analytics of user activities. Most web browsers automatically collect telemetry (unless users opt out). However, the privacy properties and privacy-sensitive user base of Tor Browser preclude automated collection of traditional telemetry and analytics. The unavailability of telemetry and analytics makes it challenging to detect and address the problems users of Tor Browser encounter.

Reporting problems regarding Tor Browser requires users to use one or more burdensome external tools, such as GitLab, Tor support forum, Tor mailing list, Internet Relay Chat (IRC), Signal, Telegram, etc. There are no first-party or third-party tools to collect and process user reports about Tor Browser without significant *manual* effort from the users and Tor Project. Researchers have proposed crowdsourcing as a means to address these shortcomings of Tor Browser [30]. To enable that approach, we designed, implemented, and evaluated a Tor Browser plugin called ReporTor[1] to gather anonymous, voluntary *structured* user-driven reports on issues experienced when browsing via Tor Browser. ReporTor aims to address the current lack of telemetry, analytics, and *contextual* user feedback regarding the user experience of accessing websites using Tor Browser.

Proceedings on Privacy Enhancing Technologies 2026(1), 393–410

https://doi.org/10.56553/popets-2026-0020

[1] The source code of ReporTor is available at: https://doi.org//10.7278/S5d-f8b6-satb.

We evaluated the utility and effectiveness of ReporTor through the following research questions:

- **RQ1:** Can an anonymous user-driven issue-reporting mechanism facilitate the collection of useful data from motivated users about the problems they face during everyday online browsing via Tor Browser?
- **RQ2:** Can issue reports from motivated users of Tor Browser enable a deeper understanding of the underlying causes of the problems encountered?

We addressed these research questions by evaluating the use of ReporTor during naturalistic web browsing via Tor Browser. Since users of Tor Browser tend to be highly privacy-sensitive, they are hesitant to respond to solicitations for research studies and can demand stringent conditions for participation [31]. Reporting visited websites to untrusted parties, such as researchers, raises additional privacy concerns, thus making it challenging to recruit privacy-conscious users of Tor Browser. Moreover, because of current user experience challenges, most individuals—regardless of whether they use Tor Browser—likely deem it prohibitively burdensome to use it as the primary means of web browsing over a long period. Since these challenges make it infeasible to collect meaningful real-world data from external participants, we evaluated ReporTor with an autobiographical approach in which we (i.e., the five authors of the paper) used it ourselves during a month of naturalistic web browsing with Tor Browser. The evaluation involved three types of data: anonymous issue reports submitted via ReporTor, online questionnaires completed at the end of the day, and semi-structured interviews at the end of the study.

We found that ReporTor effectively facilitates continuous anonymous collection and reproduction of issues users face during everyday web browsing. ReporTor issue reports gather information on problems *at the time they are encountered*. Responses to the daily questionnaires and post-study interviews helped identify improvements to enhance ReporTor to seek additional pertinent input.

Our work makes the following contributions:

- We provide ReporTor, an open-source Tor Browser plugin that enables users to submit anonymous reports of issues as they arise during naturalistic web browsing.
- We demonstrate that ReporTor can enable motivated users of Tor Browser to file structured issue reports during everyday web browsing.
- We show that domain experts can analyze issue reports submitted through ReporTor to identify their likely causes.
- We identify future improvements to ReporTor based on the insight from our data.

Our findings make the case for the inclusion of ReporTor within Tor Browser to support the efforts to make Tor Browser suitable for everyday browsing for a diversity of users.

In the sections that follow, we first describe the Tor ecosystem and situate our work in the literature on Tor, with a focus on its use and user experience. We then present the design of ReporTor to collect anonymous structured issue reports from users. We proceed to report the insight gained by analyzing the data and apply it to offer recommendations to enhance ReporTor. We conclude with a call for integrating ReporTor within Tor Browser.

2 Background

While most web traffic is encrypted to protect the content from eavesdropping during transmission, it is still possible for various parties to use the metadata about the traffic to identify who is communicating with whom. Moreover, the destination websites have access to the transmitted content in decrypted form and know the Internet Protocol (IP) address from which the access originates. The Tor network is designed to anonymize web traffic to prevent eavesdroppers from identifying users and to keep destination websites from knowing the IP addresses of end-user devices. We summarize how the Tor network enables anonymous communication to provide the background necessary to contextualize our research findings and contribution.

2.1 The Tor Network

Tor [21] is an *overlay* network that provides anonymity by routing network traffic through multiple hops using a variant of onion routing [32] to protect the information going over the network and to hide who is communicating with whom. At the end of the multiple hops, the traffic is directed to the requested Internet resource by exiting the Tor network via an exit node. To the resource, the request appears to originate from the exit node, thus shielding the identity of the end user making the request. The multiple hops protect the user's identity from the exit node as well. The list of all active Tor nodes and a marker of whether they are exit nodes is made publicly available to enable clients to connect to the Tor network. The design of the Tor network permits an exit node to be owned and operated by anyone, including malicious actors, without impacting the operational integrity and trustworthiness as long as a certain fraction of nodes is non-malicious [21].

The Tor network is a "low latency anonymity system" [50] in which users avoid deanonymization attacks, such as most classes of traffic analysis, by blending in with a large number of others, called an *anonymity set*. In such anonymity systems, the amount of achievable anonymity for any participating individual is positively correlated with the total number of users. An increase in the number of users increases the amount of noise in the network, thus making it harder to single out patterns that could identify individuals [20].

Like any network, the Tor network can transmit legal and illegal content. Many companies have reported a high number of cyberattacks arriving by the way of the Tor network [9]. For this reason, many organizations block traffic from some or all Tor exit nodes [40]. Similarly, online content providers, such as websites and apps, typically employ security mechanisms to flag potentially malicious network accesses [78]. For instance, sources of suspicious traffic get flagged by CDNs, such as CloudFlare [12], or similar services. Unlike other networks, it is challenging to differentiate between legitimate and malicious traffic on the Tor network because diverse traffic from multiple sources is lumped together at the exit nodes. As a result, if even a single actor associated with an exit node gets flagged as malicious, it can negatively impact all others whose traffic passes through that exit node.

All traffic in the Tor network destined for the general Internet must pass through one of the designated exit nodes. The Tor network additionally includes onion services that can be accessed only

via the Tor network using .onion addresses [84]. When users connect to onion services, the traffic is contained entirely within the Tor network without needing an exit node. The Tor network can anonymize any Transmission Control Protocol (TCP) based application, such as instant messaging, IRC, Secure Shell (SSH), and more. However, the most common use of the Tor network is for browsing the web [45].

2.2 Tor Browser

Tor Browser [75] is a privacy-enhancing fork of the Firefox browser. Unlike a regular web browser, Tor Browser provides anonymity by interacting with the Tor network rather than directly connecting to Internet addresses. Therefore, access to Internet resources via Tor Browser is often impacted by blocks on traffic originating from the Tor network. Such blocks cause legitimate users of Tor Browser to be treated differently compared to those who access the same resources via non-anonymous browsers [40].

To anonymize traffic by countering potential browser fingerprinting [37] at the application layer, Tor Browser implements several privacy-enhancing measures, such as providing a uniform `User-agent` string that specifies the browser version, returning less granular responses to time queries from servers, etc. [53]. Settings in Tor Browser can prevent websites from leveraging potentially privacy-compromising mechanisms, including but not limited to loading JavaScript over unencrypted (i.e., HyperText Transfer Protocol [HTTP]) connections.

3 Related Work

A majority of research on Tor is not directly relevant to the user experience because it is focused on the underlying technical aspects and deficiencies of the Tor network [4, 15, 27, 47, 85] or on Tor network measurements [11, 17, 45, 64, 67, 71]. In contrast, our work facilitates anonymous reporting and analysis of the issues affecting the user experience while browsing websites via Tor Browser. Therefore, we situate our work in the literature involving users, use cases, and the user experience/usability of Tor Browser and the Tor network. In addition, we summarize the research relevant to the functionality of ReporTor and the autobiographical method we used to evaluate it.

3.1 Tor Users and Uses

The privacy and anonymity characteristics of Tor make it challenging to obtain information about its users [53]. As an alternative, researchers have examined Tor network traffic to understand how people use such anonymity systems [62, 65, 66]. For instance, Sontag and Mayrhofer [67] found that 46% of Tor network traffic was for the web and 51% for BitTorrent, with other types of traffic making up less than 2% each. Gallagher et al. [31] interviewed Tor users and noted that experts and non-experts interact with Tor differently. Similarly, through semi-structured interviews and an online survey, Winter et al. [84] found that users have an incomplete mental model of Tor onion services, find it difficult to track them, and face challenges authenticating their legitimacy. For example, Fassl et al. [29] found that some non-experts believe the security folklore that they can protect themselves from the Tor network or increase their general security by accessing the Tor network over a Virtual Private Network (VPN). A few studies have compared the practices of Tor users with those of the general public. For instance, Mani et al. [45] collected data from several Tor network relay nodes under their control and found that Tor and non-Tor users visit similar websites.

The studies mentioned above provide initial insight into the motivations and practices of Tor users. However, the studies rely on decontextualized network measurements or user self-reports, both of which lack the detail necessary for a nuanced understanding of the challenges users face when using Tor Browser, especially for everyday tasks. ReporTor addresses this gap by enabling users of Tor Browser to submit anonymous reports on issues they encounter during naturalistic web browsing.

3.2 Tor User Experience

Using the Technology Acceptance Model (TAM), Harborth et al.[34, 35] found that usability can be a barrier to adopting Tor Browser. Even though improving the user experience can help increase their user bases and, in turn, the achievable anonymity, research on the user experience of low-latency anonymity systems, including Tor, is limited [20].

There is some research on improving the user experience of browsing over the Tor network and boosting the awareness and adoption of Tor Browser. Victors et al. [80] proposed a privacy-respecting system to make it easier for Tor users to find onion services. More recently, Story et al. [70] investigated informational and planning nudges to increase the use of Tor Browser. However, the efforts mentioned above focused on specific features (e.g., onion services [80]) or techniques (e.g., nudges [69]), rather than covering Tor Browser user experience as a whole as we do in our work.

Our work builds on Gallagher et al.'s [30] research on naturalistic use of Tor Browser in which non-expert undergraduates used Tor Browser by default for a week, reporting issues whenever they switched to another browser. Gallagher et al. [30] found that broken website functionality and network latency were the most common reasons for switching to another browser. While our research similarly used naturalistic web browsing with Tor Browser, our approach differs from that of Gallagher et al. [30] in several ways: (i) we addressed the limitations of the data collection approach of Gallagher et al. [30] by designing and deploying ReporTor as a browser plugin, rather than relying on browser switches as proxies for problems; (ii) we collected more relevant, detailed, and structured information on issues *at the time they were encountered*; (iii) we covered naturalistic web browsing over a period more than four times longer, facilitating the submission of more reports per user and more detailed analyses of the reported issues; and (iv) we gathered reports from domain experts who could provide more detailed and nuanced input because of their inherent interest in improving Tor Browser, akin to motivated users of Tor Browser. These differences enabled us to demonstrate the utility of ReporTor for facilitating anonymous, voluntary user-driven reporting of issues encountered during naturalistic web browsing via Tor Browser. In addition, our analyses of the reported issues confirm, complement, and extend the insight provided by Gallagher et al. [30] regarding the user experience of Tor Browser.

3.3 Reporting User Experience Issues

In Human-Computer Interaction (HCI) research, issue reports are commonly leveraged to uncover problems related to the user experience. User reporting of issues is an effective means of identifying real-world usability challenges [5, 7, 41, 55, 60, 82, 83]. Petrie and Power [55] examined differences between user-reported and expert-identified problems across interactive websites and found that user reports often capture real-world issues not included in expert evaluations.

Beyond website usability, Winckler et al. [82, 83] developed incident reporting systems that enable end users to report problems they encounter in their work activities to relevant authorities. Similarly, Kopackova et al. [41] developed a tool to encourage residents to improve their neighborhoods by reporting problems with the public infrastructure. ReporTor can similarly facilitate the discovery of problems by enabling motivated users to submit anonymous reports on issues encountered while using Tor Browser.

As a testimony to the need, importance, and utility of privacy-preserving telemetry, a recent project from the Internet Security Research Group, Divvi Up [22], seeks to collect telemetry data from the crowd in a private way by using the privacy-preserving aggregation protocol, Prio [14]. Prio employs multiple non-colluding servers to compute aggregate statistics over encrypted user reports. While useful, relying only on aggregated statistics from automatically gathered telemetry is insufficient to pinpoint the root causes of reported issues, as is possible with the data reported manually by end users. ReporTor can complement tools such as Divvi Up by providing a privacy-preserving mechanism for end users of Tor Browser to provide richer data about the issues they encounter as they browse.

3.4 Autobiographical Research Approaches

We evaluated the utility and effectiveness of ReporTor with an autobiographical approach. In autobiographical research, the researcher engages with the research topic from the perspective of the self [19, 79]. Such research can be carried out using a variety of methods, such as autoethnography [3, 24, 39], personal narratives [42, 56], autobiographical accounts [10, 48], microphenomenology [54, 56], etc. Autobiographical methods enable researchers to gain understanding from first-hand experience, which can facilitate richer analysis and lead to deeper insight [44, 51, 52]. Autobiographical experiences can produce authentic, vivid descriptions that add depth, context, and nuance [6]. Moreover, autobiographical approaches can uncover unique experiences often missed by other methods.

However, the personal connection of the researcher to the topic under investigation may introduce subjectivity and bias in data collection and interpretation [79]. For instance, the researcher being deeply involved in the research might present ethical challenges regarding objectivity and confidentiality [23, 25, 46]. Further, the generalizability of the findings from autobiographical research might not be readily verifiable because of the inherently small sample size [44]. Despite the above limitations, autobiographical approaches can be valuable in many situations, especially when combined with other methods to generate a more comprehensive understanding [6].

In research on usable privacy and security, autobiographical methods can provide a first-person perspective that traditional approaches typically exclude. For example, an autoethnographic study in which the researcher kept a five-month diary uncovered that even security experts found it challenging to perform authentication ceremonies in secure messaging apps because of issues such as cognitive load, social awkwardness, and forgetfulness [28]. Several studies on smart home devices have relied on autobiographical approaches and surfaced insight related to privacy and security issues. For instance, an autoethnographic diary, combined with reflexive analysis to investigate the challenges with smart home cybersecurity, highlighted that autobiographical methods provide a space for experts to reflect on their own experiences to understand what knowledge and actions might be reasonable to expect from end users [77]. Similarly, researchers have leveraged autoethnography to provide longitudinal insight into the process of learning to live with smart home technologies and their privacy implications for everyday domestic practices and routines [1]. Hine [38] incorporated autoethnographic elements in a reflexive ethnography that highlighted the 'dataveillance' capacities of smart home technologies and underscored the need to capture user perspectives on privacy. In that vein, an autoethnographic study of the Amazon Echo smart speaker pointed to significant privacy concerns related to continuous audio data collection [49].

The above research efforts demonstrate the utility of autobiographical methods to investigate privacy and security issues experienced by end users in real-world contexts. Inspired by these efforts, we leveraged our own browsing experiences to evaluate the utility and effectiveness of ReporTor. To ensure rigor and minimize the methodological shortcomings of autobiographical approaches mentioned above, we collected the independent experiences of five researchers (instead of a single person, as is typically the case in autobiographical approaches). Moreover, we gathered three types of data to capture relevant contextual detail and triangulate insight across data sources. Our approach is similar to the industry practice of 'dogfooding' [36] in which organizations first deploy and evaluate their products internally with real-world naturalistic use by their employees, including those who developed the products [16, 72].

4 ReporTor Plugin

The design of ReporTor[1] had two primary goals: (i) collecting information that could provide insight into the issue being reported, and (ii) providing an interface that integrates with Tor Browser. Importantly, we needed to ensure that we achieved the above goals while maintaining the privacy of those reporting information via ReporTor.

We took initial design inspiration from the data collection instrument Gallagher et al. [30] used to collect issue reports from the participants in their study. However, instead of using a Python script to ask questions whenever a user switches away from Tor Browser as Gallagher et al. [30] did, we packaged ReporTor as a browser plugin to integrate the reporting mechanism within Tor Browser. Because ReporTor is a plugin embedded within Tor Browser, users can invoke it to report an issue at any time. Thus, ReporTor enables users to submit information at the time an issue is encountered, regardless of whether the problem caused the user

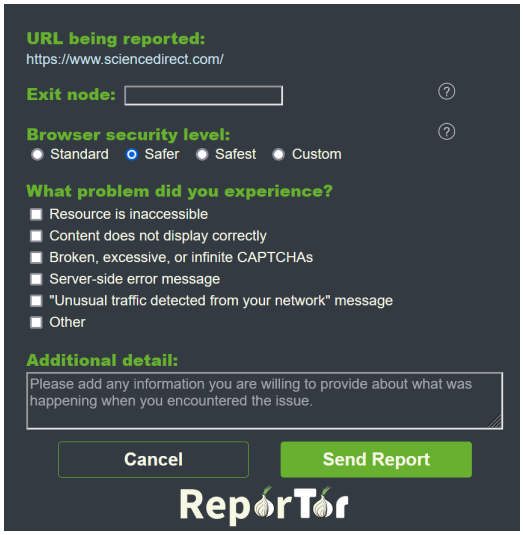

Figure 1: A screenshot of the ReporTor plugin for anonymously reporting issues encountered when browsing with Tor Browser.

to change browsers, consult a different online resource, or respond in another way. Apart from being in the plugin format that can be accessed quickly by pressing a button, ReporTor reduces the reporting burden by automating the input of some data (e.g., the Uniform Resource Locator [URL] of the current website) for inclusion in the report.

Packaging the reporting mechanism as a browser plugin introduced unique User Interface (UI) challenges, such as fitting the UI within the maximum permitted size for a plugin window. It was necessary to consider such constraints early in the design. We used an iterative design approach, starting with the problems identified by Gallagher et al. [30] to create a set of initial reporting choices to solicit information on an issue: (i) Resource is blocked or inaccessible; (ii) Some content appears broken; (iii) All page content appears broken; (iv) Excessive or impossible CAPTCHAs; (v) Server displays error messages; and (vi) Other. Next, we used non-functional UI mockups to seek feedback from a diverse set of undergraduates, graduate students, and postdoctoral scholars from the research group of the last author without requiring them to install and use ReporTor. Those providing feedback had expertise in cybersecurity and/or HCI, but were unconnected to the research on the design and development of ReporTor.

We revised the initial questions and answer options based on the feedback on the UI mockups and continued the iterative design approach by having three authors pilot ReporTor by using it for a week. The pilot confirmed the operational robustness of the plugin and the database used to collect the reports. Based on our experiences during the pilot, we made a few additional refinements to the ReporTor UI and to the common issues listed as answer options. For example, we decided to provide the 'Unusual traffic detected from your network' message as a separate option even though it is a subset of the broader category 'Resource is inaccessible' because the pilot revealed that the Google-specific error message [33] was encountered relatively frequently. Figure 1 shows the revised list of options.

The security protections of Tor Browser prevented us from automatically capturing the exit node or copying its IP address from the interface that displays the current circuit. Moreover, the circuit information that shows the IP address of the exit node cannot be kept visible while entering information in ReporTor, and the user cannot select and copy information from the circuit display. Therefore, the user must first memorize or jot down the IP address of the exit node to enter it in the report. The pilot revealed that the excessive cognitive burden and effort of typing the IP address of the exit node led to annoyance and caused inadvertent errors because of typos. To alleviate the burden, we implemented an auto-complete feature by periodically retrieving the publicly posted list of Tor exit nodes. We used the list to enable the selection of the exit node from a drop-down while typing the full IP address and to narrow the available choices as the user typed. Figure 1 shows a screenshot of the ReporTor UI after the above refinements.

Those who encounter issues accessing a website with Tor Browser can click the ReporTor icon in the toolbar, provide the requested information, and submit the report. As shown in Figure 1, ReporTor automatically captures the URL of the website in the currently active tab, but strips off query parameters, if any, for privacy protection. Users can report issues by choosing one or more of the most common problems listed. ReporTor includes an 'Other' option that enables users to report additional problems. Users can optionally use a text box to add open-ended detail, such as contextual information that could help explain and diagnose the issue. The report additionally asks users to specify the exit node of the Tor circuit used to access the website and the current Tor Browser security level [74] since either could be relevant to diagnosing the issue being reported. Users need to enter the exit node and security level manually because ReporTor does not have access to request the dynamically chosen exit node for a circuit directly from the Tor control port or to read the browser configuration to obtain the current security level.

The 'Send Report' button transmits the information over the Tor network and saves it in a password-protected database hosted as a Tor onion service. The operational setup ensures that all data remains within the encrypted Tor network, thus being shielded from cyberattacks against Tor that are based on monitoring traffic that leaves Tor exit nodes. To enable cross-checking the times of publicly known website outages, the server on which the database is hosted adds a timestamp when saving each report to the database.

5 Evaluation of ReporTor

We addressed the research questions listed in Section 1 with a functional, real-world deployment of ReporTor that involved multiple types of data collection (see Figure 2). Specifically, all five authors (see Section 5.4 for author backgrounds) set Tor Browser as their default browser on their primary computers (i.e., the computer used the majority of the time for work and personal tasks) and used it as such for the entire month of November 2022. We strove not to use another browser during this period unless unavoidable (e.g., because a required resource was inaccessible via Tor Browser). During the month of web browsing with Tor Browser as the default, we

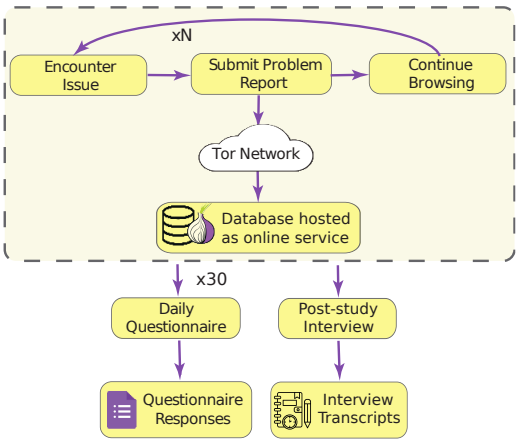

Figure 2: The figure shows the organization of the study procedures used to collect data using three methods: reporting issues, completing a daily questionnaire, and responding to a post-study interview. Whenever we encountered an issue, we submitted a report regarding the problem. The report was transmitted over the Tor network and stored in a database hosted as an onion service. Additionally, we completed a questionnaire each day of the study and participated in a post-study interview.

used ReporTor for anonymously reporting the issues we encountered as we engaged in routine browsing just as we would have naturalistically with any other browser. In addition, we completed short daily questionnaires reflecting on the use of ReporTor. After the monthlong data collection, the second author interviewed the other four authors using a semi-structured interview protocol.

5.1 Method Selection

Since ReporTor is targeted at users motivated to report issues, we needed to recruit *current* users of Tor Browser because non-users cannot be expected to be sufficiently motivated and experienced to submit reliable issue reports. Because of their heightened desires for privacy, Tor Browser users tend to be reluctant to participate in research studies, especially in those such as ours that require reporting information about their browsing destinations to other parties. In a prior study, we found it challenging to recruit a modest sample of 17 Tor users for an hourlong interview [31]. Requiring consistent engagement with ReporTor over an extended period amplifies the recruitment challenges and raises the potential for introducing bias because of attrition over time, making it practically infeasible to employ standard evaluation approaches. To overcome the recruitment and retention challenges, we leveraged the set of five authors as a reasonable proxy for motivated users of Tor Browser.

Since we were interested in evaluating the utility of ReporTor in real-world contexts, we avoided decontextualized approaches, such as a cognitive walkthrough that follows a structured protocol with predetermined tasks [68, 81]. While helpful in evaluating the usability of the UI, such approaches are unsuitable for our objective of understanding how ReporTor can facilitate *in context* reporting and analysis of issues encountered during naturalistic web browsing via Tor Browser. Therefore, we used an autobiographical approach aligned with established HCI research methods and industry dogfooding practices (see Section 3.4).

The autobiographical approach enabled us to overcome recruitment and retention challenges unique to our research and obtain rich, authentic data from motivated users of Tor Browser without compromising the validity of the results. By combining the contextual reports with daily questionnaires and post-study interviews, we captured experiences of using ReporTor at a level of detail that would have been challenging to obtain through conventional user studies with users of Tor Browser or role-playing exercises with experts or non-experts. We leveraged the diversity in our team's ages, genders, education levels, and expertise (see Section 5.4 below) to address the limitations of the autobiographical approach and strengthen our insight. As Tor Browser was not our default browser before the study, we approached the encountered issues without preconceived workarounds, ensuring authentic engagement with the problems as they arose.

5.2 Data Collection

To evaluate ReporTor and ensure that it facilitated the collection of useful reports, we gathered reports on the issues the five authors faced during naturalistic web browsing via Tor Browser. In addition, we leveraged the daily questionnaires and post-study interviews to verify that the collected issue reports were understood correctly and to identify how ReporTor could be improved.

5.2.1 In-situ Issue Reports. During the entire month of the study, the authors used ReporTor (see Figure 1) to report the issues they encountered during normal web browsing carried out with Tor Browser. Across all authors, we obtained 119 reports over the month. Since the reports are anonymous, we cannot associate a specific author with a given report. To evaluate that ReporTor facilitates reporting with sufficient information to identify the root cause(s) of the reported issue, the second author manually attempted to replicate each reported issue (see Section 5.5).

5.2.2 Daily Questionnaires. During the pilot, we observed that the issue reports sometimes could not capture all information connected to the user experience. For example, it is sometimes possible to access an inaccessible website by obtaining a new exit node by refreshing the Tor circuit. If it required several circuit refreshes to gain access, the intermediate refreshes were typically not captured in the collected reports because it was too cumbersome to report the same issue in quick succession with different exit nodes. In addition, the pilot revealed that some user experience issues were not connected to a single instance, but *cumulative*. For example, the unpredictability in accessing desired websites could build frustration and apprehension that cannot be captured in individual issue reports because it accumulates over many such experiences. We included daily questionnaires in the evaluation protocol to capture such aspects on an ongoing basis in a timely manner and identify how ReporTor could be improved to collect such information. Each daily questionnaire included the following questions:

- When you encountered issues using Tor Browser, which of the following solutions did you attempt? (None; Switching browsers;

Refreshing the circuit; Changing the browser security level; Loading alternative versions of the website [e.g., from the Internet archive]; and Other. Please specify:)
- What problems or frustrations did you encounter when using Tor Browser today that were not captured in the reports you submitted via ReporTor?
- What did you notice about your browsing experience with Tor Browser today that you appreciated or liked?

During the study period, each author received a daily email with a link to that day's questionnaire. The email was sent automatically each day at a time each author specified at the beginning of the study. Since questionnaire responses were anonymous, we assigned each author a unique identifier to include in the questionnaire responses to enable us to group responses by respondent. Only the second author had access to the mapping between the unique identifiers and the individual authors. We deleted the mapping after grouping the questionnaire responses of each respondent at the end of the data collection. Across all authors, we received 109 questionnaire responses over the course of the month. We applied the insight from the questionnaire responses to identify how ReporTor could be improved to make the reporting simpler and more user-friendly and facilitate more informative reports.

5.2.3 Post-Study Interviews. After the monthlong study period, the second author conducted semi-structured interviews with the other four authors. Since the second author led the analysis of the interview data, we deemed it unnecessary to interview the second author. The interview protocol included the following questions:

- Overall, what was it like to use Tor Browser as the default browser?
- How many issue reports did you submit per day on average?
- How did the number of issue reports you submitted each day change over the month? Why?
- How often did you switch to another browser during the study? Why?
- What did you observe about your browsing habits and patterns during the study?
- What are your suggestions for improving ReporTor?
- What are your suggestions for improving Tor Browser?
- Is there anything else you would like to mention?

The interview responses enabled us to capture detail and nuance that contextualized the submitted reports and helped us understand where ReporTor succeeded and where it needed improvement (see Section 6.3).

5.3 Ethical Considerations

We submitted the above evaluation protocol for review by the Institutional Review Board (IRB) of the University of Utah. The submitted protocol was designed for study participation by *any* user (i.e., not just the researchers) and specified explicitly that we aimed to understand how the encountered issues affect users and to administer daily questionnaires and conduct interviews in addition to submitting issue reports through ReporTor. The IRB considered the research to be evaluation of a tool (i.e., ReporTor) and not human-subjects research that requires its approval. Regardless, we carefully considered ethical aspects and took several steps to ensure ethical conduct of the research.

When designing ReporTor, we minimized the risk of identifying individuals in several ways: not asking for identifiable information in the reports; not collecting metadata that could potentially identify the person filing the report; not collecting the query parameters in website addresses as these sometimes contain sensitive information; not collecting timestamps from the reporting computers since they could reveal the user's current timezone; transmitting reports over the encrypted Tor network rather than in plaintext over the regular Internet; and storing the anonymous reports in a database accessible only to the second author. As mentioned in Section 6.3, our approach to prevent accidental inclusion of sensitive information in the reported URLs might need further hardening to guarantee that links with individually identifying information would not be exposed in a larger-scale real-world deployment. That said, we emphasize that submitting a report is voluntary and requires explicit user action (i.e., there is no automated continuous data collection of browsing destinations). If a user feels that reporting a URL would compromise anonymity, the user can choose not to report the issue. In other words, it is possible to browse with Tor Browser without reporting anything via ReporTor.

Even though we evaluated ReporTor within our trusted team, we collected the data with appropriate privacy-protecting safeguards, such as anonymizing the data using anonymous identifiers. As mentioned above, we employed similar precautions when collecting responses to the daily questionnaires by assigning each author a unique identifier to link all responses of the same person across multiple days without requiring personally identifying information, such as names. As noted above, only the second author knew the link between an identifier and the individual and deleted the linking information after pooling the questionnaire responses by respondent. We anonymized the transcripts of the semi-structured interviews before analysis. Thus, all raw data, regardless of the collection method, was anonymized prior to analysis. Only those authors involved in the data analysis had access to the raw data. In addition, all questions were limited to inquiring about the user experience and did not involve sensitive/uncomfortable topics or personal information.

5.4 Author Backgrounds

Our varied individual backgrounds and expertise in cybersecurity and HCI make us well-suited to employ the above autobiographical research approach as a collective. The first author holds a Ph.D. in usable cybersecurity and conducts research on protecting online personal information as a Senior Lecturer in Computer Science at a university in the United Kingdom. The second author was a Computer Science Master's student in the United States at the time of data collection and is currently a penetration tester in industry with more than three years of experience in offensive and defensive information security. The third author is an Assistant Professor in Computer Science focusing on cybersecurity at a university in Portugal and is involved in the Tor community as a Tor Core Contributor. The fourth author is an undergraduate in Computer Science in the United States interested in the social aspects of cybersecurity and computing. The fifth author is a tenured professor of Computer Science in the United States with multiple decades of

academic and industry experience in researching usable privacy and security.

5.5 Data Analysis

To evaluate ReporTor by answering our research questions, we conducted an in-depth analysis of each issue report submitted via ReporTor in conjunction with analyzing the open-ended responses from the daily questionnaires and semi-structured interviews.

5.5.1 Issue reports. Each report represents a specific issue experienced at a specific exit node at a specific time. While an exact reproduction of these conditions cannot be achieved, it is possible to visit the reported URL from the same exit node (assuming the node is active and has the same IP address). Even then, external conditions, such as the threat score that various CDNs assign to that IP address, could be different at the time of verification compared to when the issue was reported. Additionally, several URLs in the issue reports required authentication and could not therefore be checked. Despite these challenges, the second author browsed to each of the URLs included in the issue reports from several exit nodes and observed the JavaScript console and the Network tab within the Web Developers Tool console of Tor Browser. The process reproduced roughly half of the reported issues exactly as described. We could additionally reproduce some of the other issues, but not with the specifics in the issue report. We could not replicate the remainder of the issues due to a variety of reasons, such as page load errors, timeouts potentially linked to low-bandwidth Tor circuits, exit nodes that could not be accessed despite multiple refreshes of the Tor circuit, etc. It is likely that some of these issues are non-deterministic and cannot be replicated reliably. Nonetheless, our investigation of the URLs from the issue reports was vital to uncovering discrepancies between the user experience and the technical root causes of the reported issues.

5.5.2 Open-ended responses. The first two authors acted as independent coders to analyze the open-ended responses in the daily questionnaires and the transcripts of the semi-structured interviews. The two coders independently generated an initial list of codes by examining the daily questionnaire responses. Following a meeting between the two coders, one of them consolidated the two lists into a single set. The two independent coders then used the consolidated list to code the daily questionnaire responses using thematic analysis [8]. While the coders were free to suggest refinements to the existing codes and add codes to the list as warranted, no new codes emerged during the coding. Subsequently, the two independent coders used the same list of codes to code the transcripts of the post-study interviews, refining existing codes or adding new ones as warranted. The coders achieved an inter-rater agreement of 0.789 using Cohen's kappa [59].

5.6 Limitations

While the small number of reporters may have impacted our findings, our diverse backgrounds (see Section 5.4) temper that limitation, especially since our research differs from more traditional studies in which the goal is to generate generalizable insight regarding users and/or issues with specific websites, networks, etc. We obtained a reasonable sample of 119 issue reports to achieve our research goal of demonstrating the utility of the structured information captured by ReporTor for providing insight regarding the causes of the reported issues and identifying improvements to ReporTor. The commonalities in the issues we collectively encountered during the study indicate that these are likely to be common across browsing destinations. That said, evaluating the real-world operation of ReporTor does not require that the participants and the reported URLs be representative of current users of Tor Browser and their browsing destinations, respectively. Moreover, representativeness of the URLs in relation to current *users* of Tor Browser is not a suitable metric for our research because ReporTor is designed to support the goal of enhancing the user experience of Tor Browser to facilitate adoption by current *non-users*.

We judged the effectiveness of ReporTor based on the ability to reproduce the reported problems and/or identify their root causes based on the information in the issue reports. Relying on the quality of the information obtained via ReporTor was the most reasonable evaluation metric given the need to employ an autobiographical research approach. Metrics that rely on directly soliciting opinions about ReporTor would not have been appropriate given that we are the developers of ReporTor.

Despite our domain expertise in privacy and security, we could not always easily attribute specific causes to each issue we encountered because of unclear, misleading, or inaccurate error messages or the non-deterministic nature of the issues. The difficulty in readily determining the reasons behind the encountered issues underscores that appropriate evaluation of ReporTor could not have been carried out with participants who lacked the motivation to determine relevant information to include in the issue reports.

Because of the holiday period (Thanksgiving in the United States) during the data collection month and lower levels of browser use in general (possibly because of the use of apps and mobile devices), we obtained fewer ReporTor reports and daily questionnaire responses than we anticipated. Reporting could additionally have been affected by the social desirability bias that prevented reporting of issues on websites deemed unsuitable to reveal to others. However, as explained above, our research is not dependent on the representativeness of the reported URLs and is thus unaffected by the inclusion or exclusion of specific websites. Moreover, issues encountered repeatedly were typically reported only once to avoid repeated reporting of the same matter or because of proactive switching to another browser for accessing websites known to present issues based on previous experience of visiting the website in Tor Browser. As a result, the reports undercount the extent to which we encountered issues. Although we received fewer reports than expected, the three types of data we collected (i.e., anonymous issue reports, daily questionnaires, and post-study interviews) provided sufficient information to evaluate ReporTor and answer our research questions.

6 Evaluation Results

We deployed ReporTor as a functional proof-of-concept to confirm its effectiveness as a tool that enables motivated users of Tor Browser to report issues they experience during everyday browsing (*RQ1*). We evaluated the utility and effectiveness of ReporTor for understanding the issues in depth and surfacing their underlying

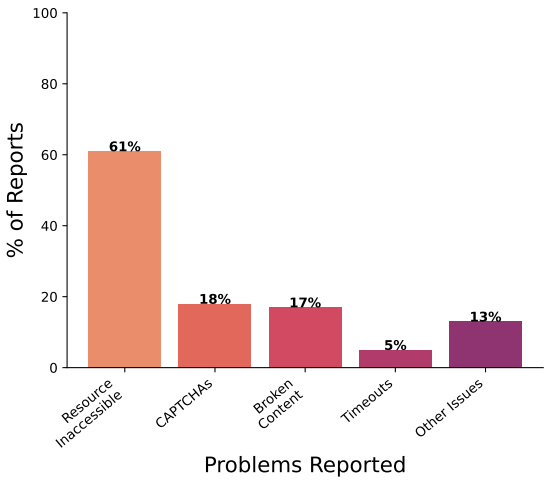

Figure 3: Distribution of the issues reported via ReporTor showing "Resource Inaccessible" as the most frequently reported issue.

causes by analyzing the individual issue reports we collected during the real-world deployment (*RQ2*). Analyzing the issue reports additionally revealed aggregated insight across the issues (see Section 6.2). Further, the deployment helped us identify how the user experience of ReporTor could be improved (see Section 6.3).

6.1 Individual Issue Reports

ReporTor proved valuable during its monthlong deployment, facilitating the collection of 119 detailed issue reports covering 84 distinct URLs. The standardized reporting mechanism enabled consistent reporting across problems, providing rich contextual information that would have been difficult to capture through conventional reporting mechanisms and support channels. We categorized the reported URLs using SimilarWeb [61] and analyzed them based on popularity rankings. The reported URLs spanned a range of website categories: Arts and Entertainment; Business and Consumer Services; Computers, Electronics, and Technology; E-commerce and Shopping; Education; Finance; Food and Drink; Health; Home and Garden; Jobs and Careers; Law and Government; News and Media; References and Materials; Science and Education; Sports; Travel and Tourism; and Vehicles. Most reported URLs came from relatively popular domains (i.e., SimilarWeb rankings 1–10,000), though some reported issues included less frequently visited websites.

As described in Section 5.5, the second author used the data in the issue reports to investigate each URL and replicate the reported problems. We found that *'Resource Inaccessible'* was the most frequently reported issue (61% of submitted reports), followed by 'CAPTCHAs,' 'Broken Content,' 'Other issues,' and 'Timeouts' (see Figure 3). Notably, the structure of ReporTor reports contains timeouts as a separate category, enabling a more nuanced analysis despite the end result being similar (i.e., the resource being inaccessible). Our attempts to replicate the reported problems revealed several distinct themes:

6.1.1 Resources Inaccessible. Nearly half (46%) of the reports that indicated 'Resource Inaccessible' included another problem in them as well. For instance, 'CAPTCHAs' were reported in 23% of reports with 'Resource Inaccessible.' Overall, 14% of the reports included either or both of these issues. The issue reports enabled us not just to replicate the reported problems but also to determine that the inaccessibility of resources seems to have been caused by two types of traffic blocks:

- **Explicit Blocks:** Some content providers explicitly block Tor traffic by choice or unknowingly due to their CDN or Web Application Firewall (WAF) configuration. For example, websites that use the Akamai Bot Manager [2] (e.g., AirBnB) are inaccessible over Tor.
- **Dynamic Blocks:** Dynamic Tor blocks do not directly block Tor traffic. Such blocks typically result from various abuse detection systems deployed to block, rate-limit, or scrutinize potentially malicious IP addresses. Because Tor exit nodes pool large amounts of traffic from diverse users, they are significantly more likely to be flagged as potentially malicious, thus triggering protective measures against potential abuse [62]. The Cloudflare CDN, for example, does not block Tor users by default, but its aggressive IP scoring system leads to Tor users being disproportionately blocked in practice. One common manifestation of such occurrences is the 'Unusual traffic detected from your computer' error message reported in 5% of the issue reports.

Though these problems have been encountered and reported in previous work, facilitating their identification and surfacing the relationship between inaccessible resources and CAPTCHAs demonstrates the utility of the data collection facilitated by ReporTor.

6.1.2 CAPTCHAs. ReporTor surfaced several CAPTCHA-related issues. In most instances (70%) in which CAPTCHAs were reported, 'Resource Inaccessible' was also reported. The descriptive comments in these reports mentioned infinite press and hold CAPTCHAs, excessive CAPTCHAs, and CAPTCHAs with unreachable servers. Content providers and CDNs typically show CAPTCHAs to clients with IP addresses suspected to be malicious or automated (i.e., bots). Since these protective mechanisms do not account for Tor traffic being inherently different from regular Internet traffic, users of Tor Browser often get bombarded with CAPTCHAs. Gallagher et al. [30] briefly discussed CAPTCHAs as an aspect of differential treatment of Tor traffic. Although we could not establish with certainty what caused the CAPTCHAs, the additional detail in the ReporTor reports allowed us to uncover two common types of problems: an excessive number of CAPTCHAs and CAPTCHAs that do not display or function properly. The latter problem often made it impossible to access the underlying website.

6.1.3 Broken Content. ReporTor captured several instances of 'Broken Content,' with 17% of the reports mentioning this issue. Replicating these problems using the descriptive information in the reports revealed that the broken content resulted from the following causes:

- **JavaScript:** Most 'Broken Content' reports were related to JavaScript. Tor Browser blocks JavaScript for better security and privacy, depending on the security slider setting. All reports of broken content indicated that the security slider was set to the 'Safer' setting, which does not block JavaScript on Secure HTTP

(HTTPS) websites. Upon checking the websites reported as having broken content, we discovered that some instances of broken content were (at least partially) differential treatment in disguise. Specifically, several reported websites showed the HTTP 403 error (i.e., an error indicating that access to the requested resource was forbidden) when accessed through Tor Browser but not Firefox. The blocked resources included advertising platforms (such as https://t.co, an X/Twitter domain). Other blocked content included JavaScript files that deal with cookie consent dialogs.
- **Authentication:** Ten issue reports (8%) contained an authentication-related URL. The reports revealed that a website would load initially, only for the authentication to fail subsequently.

ReporTor issue reports enabled the discovery that many websites which appear broken in Tor Browser are actually engaging in differential treatment of Tor traffic, thus demonstrating that the data collection mechanism is superior to that used by Gallagher et al. [30].

6.1.4 Timeouts. Analysis of the ReporTor reports revealed that 'Network Timeouts' caused by the server taking too long to respond were mentioned in 5% of the issue reports. The reasons for the error are not always related to Tor [63]. The issue reports submitted via ReporTor enabled us to replicate the issues using the descriptive information entered by the submitter. We found that a few websites connected to these issue reports load successfully in Tor Browser. However, URLs within the `utah.edu` domain failed with a timeout even after trying to access them via several different exit nodes. The above observation implies that some timeouts are likely an indirect form of explicit Tor blocking in which the server does not respond, instead of responding with a message confirming the block.

6.1.5 Other issues. The issue reports surfaced various other issues encountered when browsing with Tor Browser. The flexible reporting structure, which included predefined options and an open-ended text field, enabled reporting problems that may have otherwise gone unreported. We reviewed each issue report that indicated 'Other Issues' to characterize the reported problems. The examination led to the discovery of issues not captured by prior research on the user experience of Tor Browser. When 'Other issues' was one of several reported problems, the descriptive comments helped reclassify the reported issue as one of the other types mentioned above. The ability to connect individual problems reported by users to larger systemic issues demonstrates the effectiveness of ReporTor as a comprehensive tool that bridges the gap between quantitative metrics and qualitative user experiences.

The examination of reports categorized exclusively under 'Other Issues' surfaced a few additional problems:

- The password manager LastPass [43] allows access over the Tor network, but it is turned off by default. Trying to log into LastPass via Tor Browser results in a 'Cannot identify country based on IP address' message without indicating the existence of the option to enable access over Tor.
- Many media players, such as YouTube, use adaptive streaming [13] to adjust the quality of the video playback based on available bandwidth. Adaptive streaming in Tor Browser frequently results in media players delivering the content at the lowest quality (i.e., 144p), making video streams incomprehensible.
- Tor Browser defaults to encrypted (i.e., HTTPS) connections unless the user specifies otherwise. The HTTPS-only mode prevents access to unencrypted (i.e., HTTP) websites even on the local network or localhost. In addition, when legitimate websites redirect their insecure (i.e., HTTP) URLs to the corresponding secure (i.e., HTTPS) ones, Tor Browser displays an error rather than following the redirect.
- Following links to Zoom meetings using Tor Browser begins a download of the installation file for the Zoom application rather than opening the installed Zoom software.

Without the structured reporting capabilities of ReporTor, these diverse issues would likely be treated as isolated incidents rather than recognized as user experience concerns warranting further investigation.

6.2 Aggregated Insight Across Issue Reports

The structured data collected through ReporTor can facilitate the generation of aggregated insight across multiple issue reports. Unlike previous research approaches and current support channels, the structured data enables quantitative analysis of issue frequency along with qualitative understanding of user experiences, revealing patterns that could otherwise remain undetected.

6.2.1 Uncertainty Toward Outcomes. One of the important contributions of the issue reports is the documentation of outcome uncertainty when using Tor Browser. We used the timestamping and categorization of the ReporTor reports to compare separate attempts at accessing the same resource, providing concrete evidence of the unpredictable nature of Tor connectivity. The reports confirmed that all participants experienced this uncertainty. For instance, the issue reports documented multiple cases where refreshing the circuit resolved the issue sometimes but failed in seemingly identical scenarios. Similarly, we leveraged the structured reporting to quantify CAPTCHA-related uncertainties, recording instances where the user encountered varying numbers of CAPTCHAs with unpredictable functionality. The quantification facilitated by the structured reports helped identify patterns across websites by pooling similar individual experiences across websites.

6.2.2 Problem Attribution. The deployment of ReporTor uncovered significant challenges end users face in attributing causes to the problems they encounter. The analysis of the open-ended text within the issue reports revealed that it was sometimes difficult for the person reporting the issue to figure out why the problem occurred and whether it was possible to address it. For example, if a website loaded partially, it was challenging to determine what caused it to stall and if and when the remaining elements would load. The reports indicated that the limited ability to identify whether the problem was specific to Tor or caused by external factors was particularly frustrating. The frustration underscores the need to help users accurately understand the nature of the problems they encounter when browsing websites with Tor Browser. The data collected by ReporTor, specifically the URL and the time the report was submitted, could be used to check known website outages and inform users if an outage caused the encountered issue.

6.2.3 Unfamiliar Languages. ReporTor documented language-related challenges through its issue categorization options and metadata collection. The exit node locations included in the user reports helped confirm the finding of Gallagher et al. [30] that language-related access issues typically result from circuits that end in exit nodes from locales with languages unfamiliar to the user. Language-related problems can be annoying and significantly degrade the overall user experience, making routine browsing tasks unnecessarily burdensome.

6.3 User Experience of ReporTor

The above findings derived from the deployment of ReporTor demonstrate that the information included in the issue reports was instrumental in understanding the causes of the reported issues. For instance, the deployment of ReporTor enabled a more nuanced understanding of the differential treatment of Tor traffic and its likely causes. In this regard, the issue reports collected via ReporTor were significantly richer and more informative than those in past work in which users reported problems experienced when using Tor Browser [30].

While we did not encounter any significant problems in using ReporTor during the monthlong deployment, the daily questionnaires and post-study interviews pointed to a few improvements to the functionality and user experience of ReporTor. Manually typing the IP address of the exit node was the most cumbersome aspect of reporting issues:

> *"I had a lot of instances when the exit node was not present in the dropdown list. Most of the time, I needed to enter the node myself."* — Senior Lecturer, United Kingdom, Interview

The technical challenges that necessitate manual entry of the exit node can be overcome by integrating ReporTor within Tor Browser, thus permitting direct access to relevant information, such as the nodes in the Tor circuit, the current setting of the security slider, the version of Tor Browser, etc. Making it faster and more convenient for users to submit reports that include information on such factors that materially influence the problems experienced could enhance the analysis of the reported issues. Similarly, ReporTor could benefit from a mechanism to help users quickly report previously reported issues that are encountered again, thus facilitating a better understanding of the frequency with which users encounter specific issues. While our approach of anonymizing URLs by stripping off query parameters was adequate and reasonable for an initial deployment within a trusted team (especially since the reporting was voluntary), it is not foolproof. For example, the approach would not anonymize URLs containing identifying information. To strengthen the anonymity of reported URLs, users could be permitted to edit the URLs before submission as one of us suggested:

> *"Let me edit the URL because there are a lot of individual identifiers, content identifiers, etc. that don't really matter [to the problem being reported]."* — Assistant Professor, Portugal, Interview

Prior to broader deployment, ReporTor can be easily and quickly updated to enable users to edit the URL before submitting the report in case they wish to anonymize the URL beyond the automatic stripping off of query parameters.

7 Discussion, Implications, and Future Work

Our evaluation of ReporTor (see Section 6) demonstrated its utility and effectiveness as an anonymous issue-reporting tool to enable motivated users of Tor Browser to report the challenges they encounter during everyday browsing and provide information to facilitate reproducing the issues by those processing the reports *(RQ1)*. We confirmed that the reports facilitate reproduction of the reported issues for deeper insight into the underlying causes of the reported problems *(RQ2)*. In addition, our approach generated aggregated insight across issue reports that surfaced higher-level inconveniences *(RQ2)*. Below, we highlight the broader utility of ReporTor compared to alternatives, discuss larger-scale deployment of ReporTor, reflect on our methodological approach, and point out implications of our work for improving the user experience of Tor Browser.

7.1 Utility of ReporTor in Comparison to Alternatives

Unlike privacy-invasive browsers, Tor Browser does not automatically collect telemetry that could help identify problems and improve user experience because such collection conflicts with its mission of providing anonymity. The lack of telemetry makes it challenging to detect user experience issues in Tor Browser at scale. Though other reporting options exist [73], all of them require substantial *manual* effort from users as well as the Tor Project. Moreover, many of these options require posting through an account on Tor forum or a third-party platform. In addition to the burden of account creation and sign-in, such forms of interaction may be deemed undesirable by users with heightened anonymity needs, as is the case with the user base of Tor Browser. Further, some of the forums are publicly accessible, thus burdening moderators with removing identifying information that users may post accidentally and hateful or illegal content that trolls may post to harm the reputation of Tor. To sidestep these challenges, ReporTor implements anonymous crowdsourced issue reporting to gather more information on problems faced by users of Tor Browser without requiring them to interact with anyone or to create an account on any service. Compared with alternatives, ReporTor provides significant advantages, such as less burdensome anonymous reporting, more nuanced and contextual information gathering, easier deployability, and better extensibility.

Compared to the current support channels of the Tor Project, ReporTor imposes less burden on users and the Tor Project. Current report resolution practices in the Tor Project require large amounts of manual effort. User reports must be manually parsed because they could come in many different formats and may not contain the detail the Tor Project needs to reproduce and address the reported problem. If the number of reports submitted were to spike suddenly, the Tor Project would need to allocate additional manual effort to separate those that contain previously reported issues from those reporting new problems. The structured data provided by ReporTor reports could help detect a large percentage of duplicates automatically, thus substantially reducing human effort and enabling scaling through automated issue parsing and classification. For issues that require additional information beyond the structured data, ReporTor allows users to enter open-ended

text so that the Tor Project can investigate the root causes of the reported issues. It is important to note that ReporTor is not intended to *replace* the current mechanisms for reporting issues that the Tor Project already provides. Instead, it complements these methods to encourage *more* end users to report the issues they encounter with sufficient detail for the Tor Project to identify the root causes. The existing reporting methods might be preferable when troubleshooting an issue requires interactive discussion between the user and the Tor Project.

Our findings provide evidence that ReporTor effectively facilitates a deeper and more nuanced understanding of user experience problems encountered in Tor Browser than that achieved with the tools and methods employed in prior research efforts. For example, Gallagher et al.'s [30] method of prompting users to fill out a questionnaire whenever they switched to another browser or closed Tor Browser could not identify the root causes of the reported issues. In contrast, reports filed through ReporTor provide structured data that can be leveraged to identify the root causes of many reported issues. The example of differential treatment highlights the higher utility of ReporTor. The reports gathered by Gallagher et al. [30] treated differential treatment as a single category, while reports collected via ReporTor enabled us to expand on different types of differential treatment and their likely causes. ReporTor additionally enabled us to shine light on evolving trends in the user experience of Tor Browser, such as lower latency and less frequent incorrect geolocation. Moreover, we confirmed many of the findings regarding the user experience of Tor Browser reported in the literature and uncovered additional detail on their root causes.

For real-world deployment, Gallagher et al.'s [30] approach is unrealistic and would not scale because it requires end users to install new software external to Tor Browser, which many Tor users simply would not do. ReporTor instead empowers users to submit reports *in context* and at the time they encounter issues. If adopted by Tor Browser, ReporTor would be instantly available at scale to all Tor Browser users and is already available as an open-source plugin. Unlike the custom script employed by Gallagher et al. [30], ReporTor is easily extensible because of the streamlined update mechanism available to browser plugins.

Comparing ReporTor to similar tools is challenging, as it is the first tool that allows users to submit anonymous issue reports without the burden of side-channel communication while browsing with Tor Browser. Studies that assessed Tor network usage through network measurements and server status responses [66, 67] are the closest to our work. However, such assessments do not capture sufficient detail and nuance on the issues encountered by the end users of Tor Browser. For example, a website that appears accessible in network measurements might present users with infinite CAPTCHAs, making it inaccessible in practice. The open-ended comments in the issue reports submitted via ReporTor played a key role in deciphering plausible causes that are not apparent in network-based data. The comments can benefit developers and researchers who wish to analyze and reproduce the problems. The comments can additionally help aggregate insight across issue reports even when the root causes of the problems are not apparent to the end users filing the reports (see Section 6.2). Our experience with ReporTor further suggests that the crowdsourcing approach can be instrumental in surfacing differential treatment on a larger scale. We hope that enabling end users to flag and raise awareness of problems in accessing online content would incentivize content creators to address the issues and serve their content in Tor-friendly ways.

The utility of the ReporTor issue reports could be enhanced with a few refinements. For instance, ReporTor could include additional types of reports in which users can report issues without tying them to specific URLs. Such non-URL-specific reports could be leveraged to flag higher-level inconveniences, such as latency spikes, that may apply across multiple URLs. The higher-level reports could be scaffolded with prompts similar to the questions we used in the daily questionnaires and post-study interviews to gather relevant data. For example, users reporting an issue could be provided the option to describe their attempts to resolve the issue, along with the outcomes of these efforts.

7.2 Large-Scale Deployment of ReporTor

Our findings indicate that ReporTor can facilitate large-scale anonymous collection of user-reported telemetry that can help measure the extent and severity of the problems users face and prioritize the efforts to address them. Future work to deploy ReporTor at a larger scale in the real world consists of two independent threads.

Apart from making the URL field editable before submitting an issue report, ReporTor could be enhanced to collect issue reports with threshold encryption for single-server private data aggregation using a method such as that proposed by Davidson et al. [18]. Ongoing work has developed a prototype implementation of a solution based on the STAR protocol [18], leveraging threshold encryption, a remote randomization server, and an aggregation server to decrypt received reports. With the approach implemented in the prototype, the reported data can be decrypted only after $k(> 1)$ reports with an identical URL are received. The prototype ensures that no individual can submit a report for a given URL more than once, thus guaranteeing that reports for the URL would be decrypted only after multiple users report it. The approach provides URL privacy by trading off utility. Reports about rarely visited websites are unlikely to be decrypted, while those about frequently visited websites can be available quickly. As a result, reports of website problems that impact more users will be available without much delay, thus permitting the issues to be identified and addressed faster. Once the work matures beyond its current prototype stage, we plan to integrate it within ReporTor to anonymize the URL associated with an issue report. Although the technique could render many reports unreadable if the set of reporters is small (such as in our research), it is unlikely to be an issue if the functionality is deployed at scale (e.g., to all users of Tor Browser).

As mentioned earlier, several limitations of ReporTor can be overcome simply by its inclusion within Tor Browser. We will engage with the Tor Project and the Tor developer community to facilitate the integration of ReporTor functionality within Tor Browser.

7.3 Methodological Reflection

Our approach of evaluating our own tool in a real-world deployment by using it ourselves and documenting our own experiences helped us overcome the difficulties inherent to recruiting current

users of Tor Browser [31]. As indicated by previous research with non-expert users of Tor Browser [30], if we had instead turned to recruiting current non-users to use Tor Browser by default for a month, it is unlikely that the participants would have diligently submitted detailed reports with relevant technical detail and context. It was critical for us to ensure that the issue reports contained sufficiently reliable and high-quality information to enable us to evaluate the utility and effectiveness of ReporTor in diagnosing the problems experienced while browsing websites with Tor Browser. Involving multiple researchers with diverse backgrounds and domain expertise helped ensure that a single person's experiences did not disproportionately influence the findings. Moreover, collecting data via three distinct methods (i.e., issue reports, daily reflections, and post-study interviews) enabled us to triangulate across the data sources and develop a more comprehensive understanding of how ReporTor could be improved. Based on this experience, we call for greater acceptance and adoption of methods that leverage researcher experiences as an alternative to more traditional methods when studying user experience in contexts that pose insurmountable access difficulties and privacy-related challenges in recruiting end users.

7.4 Implications for Tor Browser

The insight we gained from our ReporTor deployment could be applied to enhance the user experience of Tor Browser.

7.4.1 Privacy-Preserving Crowdsourcing. Our findings demonstrate that a privacy-preserving voluntary reporting mechanism can enable Tor Browser to crowdsource information gathering on problems encountered by end users and overcome some of the disadvantages of the lack of telemetry and analytics. Such a mechanism could be extended to support additional features that use reports from the crowd to enhance the user experience for *everyone*. For instance, if multiple user reports indicate that a website presents problems, Tor Browser could proactively warn anyone trying to access it about the issues and offer manual or automatic mitigating actions, such as refreshing the circuit to obtain a different exit node. Such a proactive approach can save the time and effort involved in attempting to access websites that are known to be inaccessible or problematic in Tor Browser.

7.4.2 Routing to Less Popular Exit Nodes. The onion routing currently employed by the Tor network allocates circuits based on the bandwidth of the nodes, with higher-bandwidth nodes handling more traffic. Our findings indicate that the resulting higher traffic at the high-bandwidth exit nodes makes them more likely to be flagged as malicious, leading to dynamic blocks. Lower-bandwidth exit nodes that handle less traffic may be less likely to be flagged for anti-bot checks such as CAPTCHAs. Allowing users to configure Tor Browser to favor circuits that exit at nodes with less traffic could reduce the chances of running into dynamic blocks and alleviate the problem of dealing with excessive anti-bot measures, albeit at the expense of potentially higher latency. Since malicious actors are likely to favor higher bandwidths, avoiding the most popular nodes could additionally reduce the risk of a user sharing an exit node with such parties and getting flagged or blocked as a consequence. It is, however, important to note that the Tor Project advises against specifying individual exit nodes as it can compromise anonymity [76]. Further research is needed to investigate the extent to which the proposed approach of disfavoring high-bandwidth exit nodes can circumvent dynamic blocks, increase latency, and impact the user experience.

8 Conclusion

ReporTor is a plugin that enables users to report challenges in accessing websites through Tor Browser. By using ReporTor to report the problems encountered during a month of naturalistic web browsing with Tor Browser, we demonstrated the utility and effectiveness of the reports for identifying the causes of the problems and surfacing aggregated insight across issues. ReporTor provides a more structured and less burdensome reporting mechanism that improves substantially on similar approaches in prior research and complements existing Tor support channels. Our deployment of ReporTor revealed that the data collected through ReporTor is instrumental in understanding the underlying causes of the reported issues. Integrating ReporTor within Tor Browser can enable large-scale anonymous user reporting that empowers end users to flag problems and facilitate fixes to the challenges they experience. Analyzing the issue reports and addressing the problems could improve the user experience and encourage more use of Tor Browser by current users and increase its adoption by non-users. ReporTor is thus a step toward achieving the larger vision of making usable anonymity protection available to everyone by promoting broader adoption of Tor Browser for everyday web browsing.

Acknowledgments

We wish to thank those who gave us initial feedback on the UI of ReporTor. We thank anonymous reviewers and the participants of the Human-Centered Computing seminar at the University of Utah for their valuable feedback on draft versions of this paper. The authors used generative AI-based tools to detect and correct typos, refine grammar, and improve punctuation. This work is supported by UID/04516/NOVA Laboratory for Computer Science and Informatics (NOVA LINCS) with the financial support of FCT.IP.

References

[1] Line Kryger Aagaard, Toke Haunstrup Christensen, and Kirsten Gram-Hanssen. 2023. My smart home: An auto-ethnography of learning to live with smart technologies. *Personal and Ubiquitous Computing* 27, 6 (2023), 2121–2131. https://doi.org/10.1007/s00779-023-01725-0

[2] Akamai. 2025. *Bot Manager.* https://www.akamai.com/products/bot-manager

[3] Leon Anderson. 2006. Analytic Autoethnography. *Journal of Contemporary Ethnography* 35, 4 (2006), 373–395. https://doi.org/10.1177/0891241605280449

[4] Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2007. Low-resource routing attacks against Tor. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society* (Alexandria, Virginia, USA) *(WPES '07)*. Association for Computing Machinery, New York, NY, USA, 11–20. https://doi.org/10.1145/1314333.1314336

[5] Marilyn Hughes Blackmon, Muneo Kitajima, and Peter G. Polson. 2005. Tool for accurately predicting website navigation problems, non-problems, problem severity, and effectiveness of repairs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Portland, Oregon, USA) *(CHI '05)*. Association for Computing Machinery, New York, NY, USA, 31–40. https://doi.org/10.1145/1054972.1054978

[6] Arthur P. Bochner and Carolyn S. Ellis. 2006. Communication as autoethnography. In *Communication as…: Perspectives on theory*, Gregory Shepherd, Jeffrey St. John, and Ted Striphas (Eds.). SAGE Publications Inc., Thousand Oaks, CA, USA, 110–122. https://doi.org/10.4135/9781483329055.n13

[7] Athanasios Bousios, Damianos Gavalas, and Lambros Lambrinos. 2017. CityCare: Crowdsourcing daily life issue reports in smart cities. In *2017 IEEE Symposium*

on Computers and Communications (Heraklion, Greece) *(ISCC 2017)*. 266–271. https://doi.org/10.1109/ISCC.2017.8024540

[8] Virginia Braun and Victoria Clarke. 2021. *Thematic analysis: A practical guide* (1st ed.). SAGE publications Ltd.

[9] Matthew Broersma. 2015. *IBM Tells Companies To Block Tor On Security Grounds*. https://www.silicon.co.uk/security/ibm-companies-tor-175468

[10] Jerome Bruner. 1995. The Autobiographical Process. *Current Sociology* 43, 2 (1995), 161–177. https://doi.org/10.1177/001139295043002015

[11] Giovanni Cherubin, Rob Jansen, and Carmela Troncoso. 2022. Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World. In *31st USENIX Security Symposium (USENIX Security '22)*. USENIX Association, Boston, MA, 753–770. https://www.usenix.org/conference/usenixsecurity22/presentation/cherubin

[12] Cloudfare. 2025. *Connect, protect, and build everywhere.* https://www.cloudflare.com/

[13] Cloudfare. 2025. *What is adaptive bitrate streaming?* https://www.cloudflare.com/learning/video/what-is-adaptive-bitrate-streaming/

[14] Henry Corrigan-Gibbs and Dan Boneh. 2017. Prio: Private, Robust, and Scalable Computation of Aggregate Statistics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI '17)*. USENIX Association, Boston, MA, 259–282. https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/corrigan-gibbs

[15] Rasmus Dahlberg, Tobias Pulls, Tom Ritter, and Paul Syverson. 2021. Privacy-preserving & incrementally-deployable support for certificate transparency in Tor. *Proceedings on Privacy Enhancing Technologies* 2021 (2021), 194–213. Issue 2. https://doi.org/10.2478/popets-2021-0024

[16] Adriana Lopes Damian, LíGia Teixeira, Bsc. Cinthia Carrenho, Bsc. Bruna Ferreira, Bsc. Ariel Bentes, Mba Gustavo Tordin, Mba Graziela Martin, Msc. Lucas Castro, Mba Bruna Brotto, Bsc. Valéria Pereira, and Mba Raquel Pignatelli. 2023. Exploring UX Factors through the Dogfooding Approach: An Experience Report. In *Proceedings of the XXII Brazilian Symposium on Software Quality* (Brasília, Brazil) *(SBQS '23)*. Association for Computing Machinery, New York, NY, USA, 236–243. https://doi.org/10.1145/3629479.3630020

[17] George Danezis and Paul Syverson. 2008. Bridging and Fingerprinting: Epistemic Attacks on Route Selection. In *Privacy Enhancing Technologies (PETS 2008, Vol. 5134)*, Nikita Borisov and Ian Goldberg (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 151–166.

[18] Alex Davidson, Peter Snyder, E. B. Quirk, Joseph Genereux, Benjamin Livshits, and Hamed Haddadi. 2022. STAR: Secret Sharing for Private Threshold Aggregation Reporting. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 697–710. https://doi.org/10.1145/3548606.3560631

[19] Audrey Desjardins, Oscar Tomico, Andrés Lucero, Marta E. Cecchinato, and Carman Neustaedter. 2021. Introduction to the Special Issue on First-Person Methods in HCI. *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 37 (December 2021), 12 pages. https://doi.org/10.1145/3492342

[20] 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)*. Cambridge, UK.

[21] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-Generation Onion Router. In *13th USENIX Security Symposium (USENIX Security '04)*. USENIX Association, San Diego, CA. https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router

[22] DivviUp. 2025. *Divvi Up: A privacy respecting telemetry service.* https://divviup.org/

[23] Carolyn Ellis. 2004. *The ethnographic I: A methodological novel about autoethnography*. Bloomsbury Publishing PLC.

[24] Carolyn Ellis, Tony E. Adams, and Arthur P. Bochner. 2011. Autoethnography: An Overview. *Historical Social Research / Historische Sozialforschung* 36, 4 (138) (2011), 273–290. http://www.jstor.org/stable/23032294

[25] Carolyn Ellis and Art Bochner. 2000. Autoethnography, Personal Narrative, Reflexivity: Researcher as Subject. In *Handbook of Qualitative Research* (2nd ed.), N. K. Denzin and Y. S. Lincoln (Eds.). Sage Publications, 733–768.

[26] Steven Englehardt and Arvind Narayanan. 2016. Online Tracking: A 1-Million-Site Measurement and Analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 1388–1401. https://doi.org/10.1145/2976749.2978313

[27] Nathan S. Evans, Roger Dingledine, and Christian Grothoff. 2009. A Practical Congestion Attack on Tor Using Long Paths. In *USENIX Security Symposium*. 33–50. https://www.usenix.org/event/sec09/tech/full_papers/evans.pdf

[28] Matthias Fassl and Katharina Krombholz. 2023. Why I Can't Authenticate – Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 72, 15 pages. https://doi.org/10.1145/3544548.3581508

[29] Matthias Fassl, Alexander Ponticello, Adrian Dabrowski, and Katharina Krombholz. 2023. Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 344 (October 2023), 26 pages. https://doi.org/10.1145/3610193

[30] 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 *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1290–1305. https://doi.org/10.1145/3243734.3243803

[31] 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, Santa Clara, CA, 385–398. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher

[32] David Goldschlag, Michael Reed, and Paul Syverson. 1999. Onion routing. *Commun. ACM* 42, 2 (February 1999), 39–41. https://doi.org/10.1145/293411.293443

[33] Google Search Help. 2025. *Resolve Google Search's "Unusual traffic from your computer network" message.* https://support.google.com/websearch/answer/86640?hl=en

[34] David Harborth and Sebastian Pape. 2020. How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor. *SIGMIS Database* 51, 1 (January 2020), 51–69. https://doi.org/10.1145/3380799.3380805

[35] David Harborth, Sebastian Pape, and Kai Rannenberg. 2020. Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 111–128. https://doi.org/10.2478/popets-2020-0020

[36] Warren Harrison. 2006. Eating Your Own Dog Food. *IEEE Software* 23, 3 (2006), 5–7. https://doi.org/10.1109/MS.2006.72

[37] Chris Hauk. 2024. *What is Browser Fingerprinting? How it Works And How To Stop It.* https://pixelprivacy.com/resources/browser-fingerprinting

[38] Christine Hine. 2020. Strategies for Reflexive Ethnography in the Smart Home: Autoethnography of Silence and Emotion. *Sociology* 54, 1 (2020), 22–36. https://doi.org/10.1177/0038038519855325

[39] Stacy Holman Jones. 2007. Autoethnography. In *The Blackwell Encyclopedia of Sociology*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781405165518.wbeosa082

[40] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. 2016. Do You See What I See? Differential Treatment of Anonymous Users. In *23rd Annual Network and Distributed System Security Symposium* (San Diego, CA, USA) *(NDSS 2016)*. The Internet Society, 15 pages. https://doi.org/10.14722/ndss.2016.23342

[41] Hana Kopackova, Jitka Komarkova, and Jakub Jech. 2019. Technology helping Citizens to express their Needs and Improve their Neighborhood. In *2019 International Conference on Information and Digital Technologies (IDT 2019)*. 229–236. https://doi.org/10.1109/DT.2019.8813471

[42] Kristin M. Langellier. 1989. Personal narratives: Perspectives on theory and research. *Text and Performance Quarterly* 9, 4 (1989), 243–276. https://doi.org/10.1080/10462938909365938

[43] LastPass. 2025. *Every login lives in LastPass.* https://www.lastpass.com/

[44] Mariza Mẽndez. 2013. Autoethnography as a research method: Advantages, limitations and criticisms. *Colombian Applied Linguistics Journal* 15, 2 (December 2013), 279–287. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-46412013000200010&nrm=iso

[45] Akshaya Mani, T. Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. 2018. Understanding Tor Usage with Privacy-Preserving Measurement. In *Proceedings of the Internet Measurement Conference 2018* (Boston, MA, USA) *(IMC '18)*. Association for Computing Machinery, New York, NY, USA, 175–187. https://doi.org/10.1145/3278532.3278549

[46] Tina Miller and Linda Bell. 2002. Consenting to what? Issues of access, gate-keeping and 'informed' consent. In *Ethics in qualitative research*, Tina Miller, Maxine Birch, Melanie Mauthner, and Julie Jessop (Eds.). SAGE Publications Ltd., 61–75. https://doi.org/10.4135/9781473913912.n5

[47] Milad Nasr, Alireza Bahramali, and Amir Houmansadr. 2018. DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1962–1976. https://doi.org/10.1145/3243734.3243824

[48] Carman Neustaedter and Phoebe Sengers. 2012. Autobiographical Design in HCI Research: Designing and Learning through Use-It-Yourself. In *Proceedings of the Designing Interactive Systems Conference* (Newcastle Upon Tyne, UK) *(DIS '12)*. Association for Computing Machinery, New York, NY, USA, 514–523. https://doi.org/10.1145/2317956.2318034

[49] Stephen Neville. 2021. Aural Expectations of Home: An Autoethnography of the Amazon Echo Smart Speaker. *Journal of Sonic Studies* (December 2021). https://doi.org/10.22501/JSS.1426664

[50] Azin Oujani. 2011. *Tools and Protocols for Anonymity on the Internet.* https://www.cse.wustl.edu/~jain/cse571-11/ftp/anonym/index.html

[51] Aneta Pavlenko. 2002. Narrative Study: Whose Story Is It, Anyway? *TESOL Quarterly* 36, 2 (2002), 213–218. https://doi.org/10.2307/3588332

[52] Aneta Pavlenko. 2007. Autobiographic Narratives as Data in Applied Linguistics. *Applied Linguistics* 28, 2 (June 2007), 163–188. https://doi.org/10.1093/applin/amm008

[53] Mike Perry, Erinn Clark, Stephen Murdoch, Georg Koppen, and Richard Pospesel. 2024. *The Design and Implementation of Tor Browser [DRAFT].* https://gitlab.torproject.org/tpo/applications/wiki/-/blob/master/Design-Documents/Tor-Browser-Design-Doc.md

[54] Claire Petitmengin. 2006. Describing one's subjective experience in the second person: An interview method for the science of consciousness. *Phenomenology and the Cognitive Sciences* 5, 3 (2006), 229–269. https://doi.org/10.1007/s11097-006-9022-2

[55] Helen Petrie and Christopher Power. 2012. What do users really care about? A comparison of usability problems found by users and experts on highly interactive websites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 2107–2116. https://doi.org/10.1145/2207676.2208363

[56] Mirjana Prpa, Sarah Fdili-Alaoui, Thecla Schiphorst, and Philippe Pasquier. 2020. Articulating Experience: Reflections from Experts Applying Micro-Phenomenology to Design Research in HCI. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376664

[57] Franziska Roesner, Tadayoshi Kohno, and David Wetherall. 2012. Detecting and Defending Against Third-Party Tracking on the Web. In *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI '12)*. USENIX Association, San Jose, CA, 155–168. https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner

[58] Ritik Roongta and Rachel Greenstadt. 2024. From User Insights to Actionable Metrics: A User-Focused Evaluation of Privacy-Preserving Browser Extensions. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security* (Singapore, Singapore) *(ASIA CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1753–1769. https://doi.org/10.1145/3634737.3657028

[59] Christof Schuster. 2004. A Note on the Interpretation of Weighted Kappa and its Relations to Other Rater Agreement Statistics for Metric Scales. *Educational and Psychological Measurement* 64, 2 (2004), 243–253. https://doi.org/10.1177/0013164403260197

[60] Sujan Shrestha. 2007. Mobile web browsing: Usability study. In *Proceedings of the 4th International Conference on Mobile Technology, Applications, and Systems and the 1st International Symposium on Computer Human Interaction in Mobile Technology* (Singapore) *(Mobility '07)*. Association for Computing Machinery, New York, NY, USA, 187–194. https://doi.org/10.1145/1378063.1378094

[61] SimilarWeb. 2025. *The World's Leading AI-Powered Digital Data Company.* https://www.similarweb.com/

[62] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. 2017. Characterizing the Nature and Dynamics of Tor Exit Blocking. In *26th USENIX Security Symposium (USENIX Security '17)*. USENIX Association, Vancouver, BC, 325–341. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/singh

[63] SiteGround. 2025. *How to Fix the ERR_CONNECTION_TIMED_OUT_Error.* https://www.siteground.com/kb/err_connection_timed_out/

[64] Peter Snyder, Soroush Karami, Arthur Edelstein, Benjamin Livshits, and Hamed Haddadi. 2023. Pool-Party: Exploiting Browser Resource Pools for Web Tracking. In *32nd USENIX Security Symposium (USENIX Security '23)*. USENIX Association, Anaheim, CA, USA, 7091–7105. https://www.usenix.org/conference/usenixsecurity23/presentation/snyder

[65] Michael Sonntag. 2018. DNS Traffic of a Tor Exit Node – An Analysis. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCC 2018, Vol. 11342)*, Guojun Wang, Jinjun Chen, and Laurence T. Yang (Eds.). Springer International Publishing, Cham, 33–45. https://doi.org/10.1007/978-3-030-05345-1_3

[66] Michael Sonntag. 2019. Malicious DNS Traffic in Tor: Analysis and Countermeasures. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP)*. INSTICC, SciTePress, 536–543. https://doi.org/10.5220/0007471205360543

[67] Michael Sonntag and René Mayrhofer. 2017. Traffic Statistics of a High-Bandwidth Tor Exit Node. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP)*. INSTICC, SciTePress, 270–277. https://doi.org/10.5220/0006124202700277

[68] Rick Spencer. 2000. The streamlined cognitive walkthrough method, working around social constraints encountered in a software development company. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (The Hague, The Netherlands) *(CHI '00)*. Association for Computing Machinery, New York, NY, USA, 353–359. https://doi.org/10.1145/332040.332456

[69] Peter Story, Daniel Smullen, Rex Chen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2022. Increasing Adoption of Tor Browser Using Informational and Planning Nudges. *Proceedings on Privacy Enhancing Technologies* 2 (2022), 152–183. https://doi.org/10.2478/popets-2022-0040

[70] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies* 3 (2021), 308–333. https://doi.org/10.2478/popets-2021-0049

[71] Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang, and Prateek Mittal. 2015. RAPTOR: Routing Attacks on Privacy in Tor. In *24th USENIX Security Symposium (USENIX Security '15)*. USENIX Association, Washington, D.C., 271–286. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sun

[72] Edgar Tanaka, Edilson Silva, and Gustavo Tordin. 2019. Dogfooding: "Eating our Own Dog Food" in a Large Global Mobile Industry Player. In *2019 ACM/IEEE 14th International Conference on Global Software Engineering* (Montreal, Quebec, Canada) *(ICGSE '19)*. 62–67. https://doi.org/10.1109/ICGSE.2019.00024

[73] The Tor Project. 2025. *Get in Touch.* https://support.torproject.org/get-in-touch/

[74] The Tor Project. 2025. *Security Settings.* https://tb-manual.torproject.org/security-settings/

[75] The Tor Project. 2025. *Tor Browser User Manual.* https://tb-manual.torproject.org/

[76] The Tor Project. 2025. *Tor FAQ.* https://2019.www.torproject.org/docs/faq.html.en

[77] Sarah Turner, Jason R. C. Nurse, and Shujun Li. 2022. "It Was Hard to Find the Words": Using an Autoethnographic Diary Study to Understand the Difficulties of Smart Home Cyber Security Practices. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 34, 8 pages. https://doi.org/10.1145/3491101.3503577

[78] Tom van Goethem, Ping Chen, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen. 2014. Large-Scale Security Analysis of the Web: Challenges and Findings. In *Trust and Trustworthy Computing (Trust 2014, Vol. 8564)*, Thorsten Holz and Sotiris Ioannidis (Eds.). Springer International Publishing, Cham, 110–126.

[79] Francisco J. Varela and Jonathan Shear. 1999. First-person methodologies: What, why, how. *Journal of Consciousness studies* 6, 2-3 (1999), 1–14.

[80] Jesse Victors, Ming Li, and Xinwen Fu. 2017. The Onion Name System. *Proc. Priv. Enhancing Technol.* 2017, 1 (2017), 21–41. https://doi.org/10.1515/popets-2017-0003

[81] Cathleen Wharton, John Rieman, Clayton Lewis, and Peter Polson. 1994. *The cognitive walkthrough method: A practitioner's guide.* John Wiley & Sons, Inc., USA, 105–140.

[82] Marco Winckler, Cedric Bach, and Regina Bernhaupt. 2013. Identifying User Experience Dimensions for Mobile Incident Reporting in Urban Contexts. *IEEE Transactions on Professional Communication* 56, 2 (2013), 97–119. https://doi.org/10.1109/TPC.2013.2257212

[83] Marco Winckler, Regina Bernhaupt, and Cédric Bach. 2016. Identification of UX dimensions for incident reporting systems with mobile applications in urban contexts: A longitudinal study. *Cognition, Technology & Work* 18, 4 (2016), 673–694. https://doi.org/10.1007/s10111-016-0383-1

[84] 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 '18)*. USENIX Association, Baltimore, MD, 411–428. https://www.usenix.org/conference/usenixsecurity18/presentation/winter

[85] Zhao Zhang, Wenchao Zhou, and Micah Sherr. 2020. Bypassing Tor Exit Blocking with Exit Bridge Onion Services. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, USA) *(CCS '20)*. Association for Computing Machinery, New York, NY, USA, 3–16. https://doi.org/10.1145/3372297.3417245

A Categories and Ranking of URLs in Each Report

Report Number	Domain	Category	Global Rank
1	adventofcode.com	Computers, Electronics, and Technology – Programming and Developer Software	199,459
2	airbnb.com	Travel and Tourism – Accommodation and Hotels	171
3	allrecipes.com	Food and Drink – Cooking and Recipes	590
4	ally.com	Finance – Banking, Credit, and Lending	2,575
5	americanexpress.com	Finance – Banking, Credit, and Lending	334
6	americanexpress.com	Finance – Banking, Credit, and Lending	334
7	argentina.gob.ar	Law and Government – Government	1,120
8	azlyrics.com	Arts and Entertainment – Music	6,928
9	bankofthewest.com	Finance – Banking, Credit, and Lending	1,262,662
10	bensbargains.net	E-commerce and Shopping – Coupons and Rebates	1,720,379
11	blackbeltwiki.com	Sports – Martial Arts	191,641
12	capitalone.com	Finance – Banking, Credit, and Lending	198
13	chase.com	Finance – Banking, Credit, and Lending	115
14	chevrolet.com	Vehicles – Makes and Models	5,877
15	coursera.org	Science and Education – Education	560
16	csrankings.org	Science and Education – Math	141,257
17	delta.com	Travel and Tourism – Air Travel	704
18	digitalocean.com	Computers, Electronics, and Technology – Web Hosting and Domain Names	7,275
19	digitalocean.com	Computers, Electronics, and Technology – Web Hosting and Domain Names	7,275
20	dilbert.com	Arts and Entertainment – Humor	445,147
21	dilbert.com	Arts and Entertainment – Humor	445,117
22	doodle.com	Science and Education – Biology	7,382
23	doodle.com	Science and Education – Biology	7,382
24	duckduckgo.com	Computers, Electronics, and Technology – Search Engines	45
25	espn.com	Sports	86
26	espncricinfo.com	Sports	279
27	fda.gov	Health – Pharmacy	7,025
28	flyfrontier.com	Travel and Tourism – Air Travel	3,295
29	google.com	Computers, Electronics, and Technology – Search Engines	1
30	google.com	Computers, Electronics, and Technology – Search Engines	1
31	google.com	Computers, Electronics, and Technology – Search Engines	1
32	google.com	Computers, Electronics, and Technology – Search Engines	1
33	google.com	Computers, Electronics, and Technology – Search Engines	1
34	google.com	Computers, Electronics, and Technology – Search Engines	1
35	google.com	Computers, Electronics, and Technology – Search Engines	1
36	google.com	Computers, Electronics, and Technology – Search Engines	1
37	google.com	Computers, Electronics, and Technology – Search Engines	1
38	google.com	Computers, Electronics, and Technology – Search Engines	1
39	google.com	Computers, Electronics, and Technology – Search Engines	1
40	hackthebox.com	Computers, Electronics, and Technology – Computer Security	16,982
41	hertz.com	Travel and Tourism – Car Rentals	5,296
42	homedepot.com	Home and Garden	183
43	hotels.com	Travel and Tourism – Accommodation and Hotels	651
44	ieee.org	Science and Education	3,300
45	imgflip.com	Arts and Entertainment	6,671
46	indeed.com	Jobs and Careers – Jobs and Employment	40
47	instagram.com	Computers, Electronics, and Technology – Social Networks and Online Communities	4

Report Number	Domain	Category	Global Rank
48	jblearning.com	Science and Education – Universities and Colleges	20,390
49	joyoftech.com	Arts and Entertainment – Humor	3,985,757
50	kayak.com	Travel and Tourism	911
51	krispitech.com	Computers, Electronics, and Technology	812,941
52	lastpass.com	Computers, Electronics, and Technology	4,391
53	list-manage.com	Computers, Electronics, and Technology – Email	541
54	medium.com	Business and Consumer Services	319
55	mit.edu	Science and Education – Universities and Colleges	731
56	momondo.co.uk	Travel and Tourism	79,177
57	nature.com	Science and Education – Biology	1,705
58	news.google.com	News and Media	118
59	nih.gov	Health	153
60	nyu.edu	Science and Education – Universities and colleges	5,280
61	nytimes.com	News and Media	73
62	nytimes.com	News and Media	73
63	orcid.org	Science and Education	8,606
64	orcid.org	Science and Education	8,608
65	ostechnix.com	Computers, Electronics, and Technology – Programming and Developer Software	209,858
66	overleaf.com	Science and Education – Math	2,105
67	overleaf.com	Science and Education – Math	2,105
68	piazza.com	Science and Education – Education	11,268
69	protonmail.com	Computers, Electronics, and Technology	123,386
70	qualtrics.com	Business and Consumer Services – Business Services	796
71	qualtrics.com	Business and Consumer Services – Business Services	796
72	qualtrics.com	Business and Consumer Services – Business Services	796
73	qualtrics.com	Business and Consumer Services – Business Services	796
74	questdiagnostics.com	Health	3,007
75	rei.com	Sports	1,255
76	ryanair.com	Travel and Tourism – Air Travel	603
77	sciencedirect.com	Reference Materials – Dictionaries and Encyclopedia	482
78	sciencedirect.com	Reference Materials – Dictionaries and Encyclopedia	482
79	slack.com	Computers, Electronics, and Technology – Social Networks and Online Communities	428
80	slack.com	Computers, Electronics, and Technology – Social Networks and Online Communities	428
81	southwest.com	Travel and Tourism – Air Travel	568
82	spotify.com	Arts and Entertainment – Music	68
83	swan.ac.uk	Science and Education – Universities and Colleges	385,872
84	swan.ac.uk	Science and Education – Universities and Colleges	385,872
85	swansea.ac.uk	Science and Education – Universities and Colleges	48,137
86	teamblind.com	Finance	3,465
87	thehill.com	News and Media	1,489
88	thoughtco.com	Science and Education – Education	11,334
89	torproject.org	Computers, Electronics, and Technology – Computer Security	18,299
90	tribpub.com	News and Media	770,299
91	twitter.com	Computers, Electronics, and Technology – Social Networks and Online Communities	5
92	usnews.com	News and Media	1,075
93	utah.edu	Science and Education – Universities and colleges	8,874
94	utah.edu	Science and Education – Universities and colleges	8,874
95	utah.edu	Science and Education – Universities and colleges	8,874
96	utah.edu	Science and Education – Universities and colleges	8,874
97	utah.edu	Science and Education – Universities and colleges	8,874

Report Number	Domain	Category	Global Rank
98	utah.edu	Science and Education – Universities and colleges	8,874
99	utah.gov	Law and Government – Government	5,572
100	utcourts.gov	Law and Government – Government	98,603
101	utcourts.gov	Law and Government – Government	98,603
102	utcourts.gov	Law and Government – Government	98,603
103	uvu.edu	Science and Education – Universities and Colleges	51,445
104	virustotal.com	Computers, Electronics, and Technology – Computer Security	3,112
105	voterrecords.com	Law and Government	22,187
106	walmart.com	E-commerce and Shopping – Marketplace	87
107	walmart.com	E-commerce and Shopping – Marketplace	87
108	walmart.com	E-commerce and Shopping – Marketplace	1,814,471
109	way.com	Travel and Tourism – Air Travel	35,592
110	webmd.com	Health – Health Conditions and Concerns	698
111	webmd.com	Health – Health Conditions and Concerns	698
112	wellsfargo.com	Finance – Banking, Credit, and Lending	180
113	wsu.edu	Science and Education – Universities and Colleges	25,008
114	wundeground.com	Science and Education – Weather	1,208
115	yewtu.be	Computers, Electronics, and Technology	21,266
116	youtube.com	Arts and Entertainment – TV Movies and Streaming	2
117	zoom.us	Computers, Electronics, and Technology	60
118	zoom.us	Computers, Electronics, and Technology	60
119	zoom.us	Computers, Electronics, and Technology	60