

BARRIERS TO TOR ADOPTION: INSIGHTS FROM USER OPINIONS EXTRACTED FROM TWITTER

Surabhi Nayak

Abstract

Anonymization technologies have existed for a long time for protecting the privacy of users. The Onion Router (Tor) is one such example which prevents network surveillance and protects user privacy through layered encryption. Despite the technical functionalities and privacy benefits in their design, the usage of these systems is not as widespread as anticipated. For instance, a statistical report published in 2013 indicated that Tor's user base is only about 0.016% of approximately 3 billion internet users globally. Since Tor operates on a 1/n system, user adoption is crucial to enhancing its privacy features. Considering these factors, this study aimed to investigate the reasons associated with reluctance to adoption of Tor among users and, specifically, highlight critical issues that lead users to abandon Tor. To understand public sentiments regarding Tor adoption, this study analyzed available data on Twitter- a micro-blogging social network platform where users freely share their opinions and experiences. Specifically, the negative tweets about Tor were examined and classified into five categories for data analysis. An attribute data was created based on issue tolerance, and the density, homophily, clustering and correlation among the various reported issues were analyzed. Overall, this study shows that Tor's primary issues like trust, privacy, application compatibility, and user-interface design, altogether contribute to its low usability, with trust issues being a major factor leading users to abandon Tor. Hence, improving these aspects is critical for enhancing user acceptance and expanding Tor's user base.

Keywords: *Privacy preserving protocols, Social computing, Security and protection, Anonymity, Tor, Trust Issues, Web Applications.*

1 INTRODUCTION

Tor (The Onion Router) is a software designed to prevent network surveillance and protect user privacy by employing a 'layered encryption' where the data packets traverse a distributed network of servers, with each server decrypting only the information that is absolutely necessary [33]. Despite its benefits, the usage of Tor has not become widespread, and is often subjected to criticism based on security concerns. Tor is a 1/n system, where anonymity is enhanced by the presence of more users [2]. Hence, to improve the privacy features of Tor, it is crucial to increase its adoption by more and more internet users. Also, understanding the issues that lead users to stop using Tor is essential for enhancing the platform's effectiveness and user experience.

In this study, we analyzed tweets, from Twitter- a microblogging social platform, reporting issues with Tor software to understand the reasons for its low adoption rate. Twitter was selected to extract data, since it allows an average user to share their thoughts publicly either directly or by addressing it with various hash tags. Since Tor is an anonymization software, it was unlikely that any user would publicly tweet about using this software. However, we anticipated reviews from users not engaged in secretive activities. Also,

it was possible that some users might want to improve the system for everyone by enhancing its usability. Since our concern was identifying prevalent issues with Tor, which was classified as either deal breakers or tolerable in this study, only negative tweets were considered for construction of data for analysis.

Previous research studies indicate that user retention is heavily influenced by specific concerns such as privacy, security, and application performance [3], [4]. To confirm if this is the case with Tor, this study aimed to identify the most likely issues that discourage users from adopting use of Tor software. To achieve this, we employed hierarchical cluster analysis and correlation analysis to identify and validate the patterns in user-reported issues. Hierarchical cluster analysis helps reveal issues that frequently occur together, providing insights into how user-interface, application-related, privacy, and illegal usage concerns are interrelated. The correlation analysis evaluates the impact of these issues on users' decisions to classify them as 'deal breakers'. By understanding these patterns and relationships, targeted strategies can be developed to address the most critical concerns, thereby improving user satisfaction and retention. Thus, this study contributes significantly to understanding the barriers to Tor adoption, providing potential insights for enhancing user privacy and encouraging broader usage of anonymization technologies. Highlights of these contributions include the following:

- This study provides a detailed categorization and analysis of user concerns about Tor, highlighting the most critical issues that affect its adoption. At the same time it distinguishes between tolerable and intolerable issues that will allow developers to follow a focused approach while considering user behavior.
- A comprehensive visualization of user interactions and issue-reporting patterns generated based on UCINET and Net Draw tools, along the reported methodological framework provided in this study can guide similar future studies leading to overall improvements in Tor and other anonymization technologies.
- This study aids targeted interventions by identifying cliques and clusters of users based on reported issues, revealing social dynamics within the Tor user community.

The article is structured as follows. The present Section (1) provides an introduction to Tor, its associated benefits and issues along with a general introduction, aim of this study and outline of manuscript. In Section 2, we present an overview of relevant literature that discusses anonymization technologies and issues associated with them. The research questions and specific methods are described in Section 3 and Section 4, respectively. The various analyses providing insights into the prevalence of Tor issues, the nature of user connections, and the impact of specific concerns on user behavior is described in Section 5, while the implications of study outcomes are presented in Section 6. The Section 7 and Section 8 list the limitations of the study and concluding remarks, respectively.

2 BACKGROUND

2.1 PRIVACY ENHANCING TECHNOLOGIES

A study by David L. Chaum [1] on encrypted email was among the pioneering studies that portrayed the concept of anonymity by transmitting an encrypted message through a series of nodes. His proposed network for preserving a sender's anonymity closely resembles the relay network used in Tor. However, the study model was primitive requiring only 3 hops, and did not account for system latency. Over one and half decade later, Justin Boyan [10] proposed anonymization software based on computer-mediated communication, which used a single hop proxy. The idea of the previous transport network described in [1] has been improvised with 'freehaven' and 'freenet' that aimed to balance the anonymity and latency aspects by providing anonymous information storage and retrieval systems [3], [4]. Despite improvisations, these networks and softwares have not gained popularity among users. The most probable reason for low adoption rates may be the associated limitations of the software such as lack of anonymity at entry and exit nodes, the risk of using shared keys and very limited features like anonymous storage. The concept of privacy enhancing technologies has been explored for various applications such as storage of genomic data, customer data and biometrics [5], [6], [7], [8]. However, none of these anonymization technologies gained significant user popularity until the introduction of Tor in 1998, which became even more popular with its second generation proposed in 2004 [9].

Few studies have addressed user acceptance of Privacy-Enhancing Technologies (PETs). A study on RFID PET acceptance evaluated the influence of the Perceived Control through different PETs on consumers' intention to adopt the after-sales RFID services [11]. Harbach et al. [12] conducted focus group interviews to identify barriers to the user adoption of the privacy-preserving eID authentication services. These and few other studies have explored aspects like perceived control and perceived ease of use, to understand user adoption for various technologies such as email authentication mechanisms and single sign-on anti-spyware systems [13], [14], [15], [16]. These studies aim at creating technology acceptance models for solving the issues associated with low user acceptance.

2.2 USABLE SECURITY

The first study that combined the concept of usability in security was '**Why Johnny Can't Encrypt**', which described some confusing aspects of the user interface of PGP 5.0. The authors performed a cognitive walkthrough analysis and laboratory test, revealing some interface design flaws that led to security failures or discouraged encryption use altogether [17]. Their analysis concentrated on the importance of user-interfaces on user's perception and motivation to protect their information. Steve Sheng et al. [18] conducted a pilot study to understand the latest usability situation of email encryption software, particularly PGP 9 compared to PGP 5. A more recent study '**Why Johnny can't blow the whistle**' focused on identifying and fixing the usability issues in Tor by creating a set of design recommendations for each core issue [22]. However, this study did not consider other factors affecting user adoption except usability, and the design recommendations were not validated but simply based on hypotheses. Some research studies have suggested that rigid password policies can deter users from caring about security [19]. These findings were confirmed and extended to graphical passwords by Sacha Brostoff et al. [20].

While many of these studies have identified issues hindering user acceptance for anonymization technologies, few have explained user tolerance for these issues, which is something we hope to establish through this study. The study by Serge Egelman is one of the rare studies discussing how users are likely to cheat on Mechanical Turk tasks depending on whether they receive a proper security explanation for the tolerance time [21]. Our research aims to determine if users reporting specific issues are more or less likely to stop using the software because of them.

2.3 USER ACCEPTANCE AND TRUST

The Technology Acceptance Model (TAM) has significantly influenced the field of user acceptance for software. The contributions of Fred Davis are considered a benchmark since they introduced the concepts of perceived usefulness, perceived ease of use, and user acceptance for software [23], [24]. He also published progressive improvements on his previous work through incorporation of longitudinal studies, and additional factors [25], [26]. In these studies he created several versions of TAM, in addition to what was initially proposed. In the most recent version, a unified theory of acceptance and use of technology derived from the theoretical and empirical investigation of eight technology acceptance models is described [27], [28]. While these models provide frameworks for designing user acceptance studies, integrating trust and perceived risk into TAM remains an emerging research area.

In our work, we define the concept of ‘trust’ as a ‘belief that this technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible’ [29]. The relationship between trust and perceived risk in a privacy calculus model designed for e-commerce suggests that risk influences trust [30]. However, another research study on consumer acceptance of e-commerce contradicts these findings [31]. Among the rare studies, one study clarifies this relationship in context of consumer acceptance of e-services [32].

3 RESEARCH QUESTIONS

This research addresses two questions, the answers to which can prioritize areas for Tor improvement.

1. Do the reported issues influence their classification as deal breakers?
2. Which issues are most likely to be deal breakers?

4 METHODS

Social media platforms like Twitter serves as a powerful tool for surveying user issues with Tor since it provides real-time feedback and highlights areas that require attention. The user-generated content on social media is also an excellent source for developing strategies that can help prioritize user-centric improvements in the Tor network. To fulfill these objectives, the methodological approach in this study involved data collection, classification of tweets and data analysis.

4.1 DATA COLLECTION

We gathered tweets from Twitter, made in English language, or that could be translated easily with Google translate tool, using an MS Excel plug-in called Node XL. This tool allowed us to extract tweets for the selected hash tags such as #tor #torissues #tor problems and #torproject. The data collection was done over a period of two months between 1st May 2024 and 1st July 2024. The raw data collected during this period underwent a cleaning process to eliminate any irrelevant tweets that were not related to tor. This is because the hashtag search also resulted in extraction of tweets from users having the phrase 'tor' in their username and other such irrelevant data. Additionally, some tweets in Chinese and Spanish languages that were translated to English, led to meaningless translations, and hence were eliminated. Poorly translated tweets could potentially interfere with data analysis and lead to misinterpretation of results. Thus, the cleaning process ensured that the dataset was relevant for analyzing user opinions about Tor. The final dataset after data collection and cleaning process comprised 300 relevant tweets. Node XL organized the data that consisted of the user who posted the tweet (author), and users who mentioned, retweeted or replied to the tweet, URLs and hashtags mentioned in the tweet, the actual content of the tweet and ID of tweet. Overall, Node XL provided data attributes such as tweet content, user interactions, and metadata detailing the views of user sentiments as well as issues related to Tor.

4.2 CLASSIFICATION OF TWEETS

While several studies have examined Tor's usability, such as [17] and [33] they mainly focus on designing heuristics to increase the usability of Tor based on survey study results. These studies do not address factors like trust, perceived risk and illegal usage reports. Some usability issues like lack of a properly designed user interface, latency in launching, and browsing has been well documented in both these studies. These are known issues with the software that exist even today. This research attempts to identify the other aspects of user acceptance that might hinder the adoption of Tor.

4.2.1 User-interface issues

The notable studies [17] and [33] highlight the user-interface issues with Tor by addressing the usability enhancing heuristics. These issues include:

- Download clarity: There exists an uncertainty among users regarding where to download Tor on the website, indicating unclear download instructions.
- Window discriminability: Users find it difficult to distinguish between Tor Browser Bundle (TBB) and normal browser.
- Archive confusion: Users face challenges with unzipping the TBB package.
- Icon Saliency: Users struggle to find 'Start Tor Browser' icon.

These issues basically stem from the outdated TBB user interface 'Vidalia'. Another major issue, after successful download and installation of software, is manual configuration requirement of Tor by the user without sufficient guidance. The prompted instructions on the website for configuration direct users to an

online document without any step-by-step guidance. Although this configuration is a one-time process for each device, the overall poor interface design can deter users, making them less likely to adopt or continue using Tor due to the complexity of initial setup.

4.2.2 Latency

The study [33] reports two major latency issues. These include:

- Long launch time: The users report a lag between clicking the TBB icon and the window appearing.
- Browsing delay: The users also report a noticeable lag during browsing with TBB.

Technically, latency is an inherent issue associated with anonymous browsing softwares due to the encrypted data packet being relayed through a worldwide network of servers (nodes). Keeping the users informed about these delays wherever possible can increase their tolerance. Research studies suggest that users are more tolerant to software delays if they understand the security rationale behind them [21].

4.2.3 Lack of integration with third-party applications

One of the most commonly discussed issues related to Tor on discussion forums as well as platforms like twitter is its lack of integration with other applications like IM clients and email applications among several others. Although significant upgrades have been made for the software by the company over time, with each upgrade providing more functionality and supporting more applications like Facebook messenger, the issues related to lack of integration over a wider scale still persists; thereby preventing Tor to gain worldwide popularity.

4.2.4 Lack of trust in anonymity

As described earlier in this study, the TAM laid the foundation in understanding software acceptance focusing on perceived usefulness and ease of use. Although such models are the frameworks for designing user acceptance studies, the integration of Trust and Perceived Risk in the model is still an emerging field of research. In this context, trust refers to the belief that Tor will perform as expected despite potential negative outcomes.

4.2.5 Reluctance due to its association with illegal activities

The association of Tor with illegal activities, such as those conducted on the dark web by criminals and terrorists has caused reluctance among users to install it. Unfortunately such misuse of the concept of anonymity and its association with cons, is a default disadvantage of every anonymity enhancing software. Although there is no apparent fix for this issue, there is a need to address it since it influences users' decisions to adopt or discontinue using Tor. Since tor is a 1/n system, more users adopting the software would enhance anonymity for all the users, and hence the reports of illicit activities could negatively impact a user's perspective of Tor.

4.3 DATA ANALYSIS

This study addressed both usability and non-usability issues. The categories of Tor associated issues were selected based on their frequent mention in related studies [17], [33]. The dataset was organized as a 2-mode network with Twitter usernames and issues reported. The binary nature of the dataset indicated whether each issue was present in a tweet, helping to identify which issues are critical. Additionally, an attribute dataset was created describing details about the various nodes like demographic information (age, gender) and a variable called 'deal breaker', which defined if the user who reported a particular issue actually stopped using Tor because of the issue. Thus, the deal breaker variable was intended to help identify critical issues and provide insights into the most significant factors affecting user retention. UCINET was utilized for dataset analysis, while visualizations were created using Net Draw tool [34]. Different metrics were assessed to understand user behavior, identify user interface issues, and analyze user groups with similar concerns and their connections. The relationship between issues and their tolerance were evaluated based on density, homophily, cliques and hierarchical cluster analysis, and confirmation of deal breaker issues were done based on correlation analysis.

5 RESULTS

The analysis of different metrics followed by evaluation of their correlation was helpful in clearly highlighting the tolerable and intolerable issues of Tor. The detailed outcome of each analysis is described in this section.

5.1 DENSITY

The density metric helps in understanding which issues are most prevalent and impactful. The density of the network was 23.8% and average hybrid reciprocity was 1. Here, density measures the average strength across all possible (not all actual) connections. The average hybrid reciprocity value indicates that any connections between users were reciprocated i.e., if two users are connected, their connection was mutual. The highest degree centrality observed was 44 corresponding to the tweets discussing the misuse of Tor for illegal activities. It reflects the number of connections a particular tweet (or user) has. In this case, tweets about the misuse of Tor for illegal activities are central to the network, suggesting they generate significant attention and interactions. Majority of users (56.4%) reported only 1 issue in their tweet, with privacy and illegal use (40.9% each) being the most prominent concerns. These were followed by user-interface issues in popularity.

5.2 HOMOPHILY

The E-I index for the number of issues reported was -0.1333. This indicates that users who report a similar number of issues were more connected to each other rather than with users who report different numbers of issues. The E-I index treats the edges as binary and ignores any values on the edges. When considering 'deal breaker' as the attribute, the E-I index was 0.9494, which represents a strong heterophily. This indicates that users who view these issues as deal breakers are not strongly connected to each other, and are more connected to users who do not view these issues as deal breakers. This suggests that while a group of

users may share thoughts and concerns about certain issues, their perception of classifying them as deal breakers varies significantly.

To make the network visualization manageable, 50 tweets were randomly selected from the total of 300. Displaying all 300 nodes would have been overwhelming and less informative. Figure 1 is a representation of the visualization of a subset of the **'network'** indicating the relationships between users based on the issues they reported. This helps in understanding the connections and patterns in user feedback on Tor.

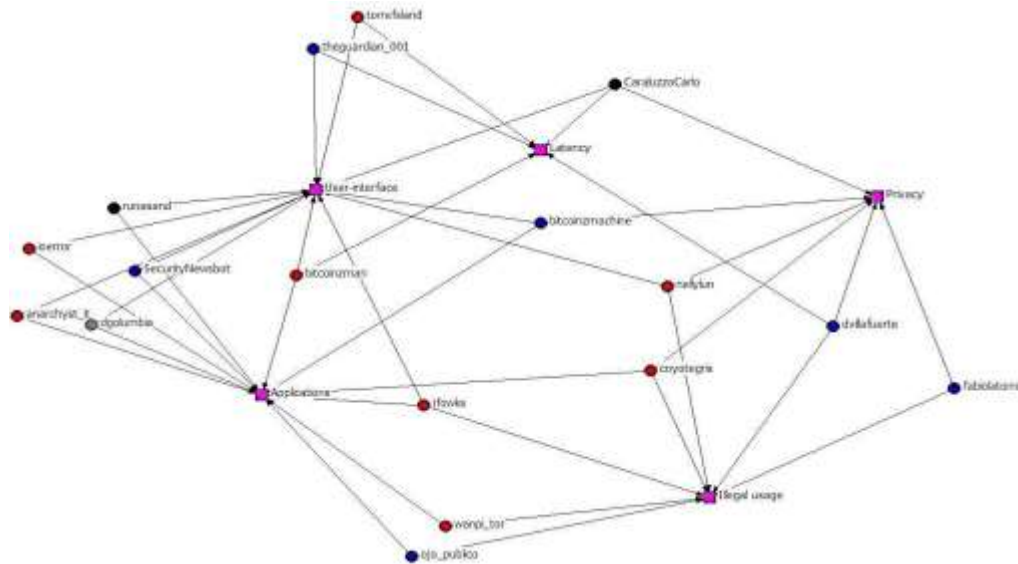


Figure 1: A 2-mode network visualization

The colors in above figure highlight the users reporting the number of issues, with red corresponding to users reporting only 1 issue, blue means 2 issues, black means 3 issues and gray means 4 issues; Pink color indicates the issues with Tor

Figure 2 is a representation of the visualization of a subset of the **'users'** indicating the relationships between them based on the issues they reported.

5.3 CLIQUES

Cliques represent tightly-knit groups within a network where members are more closely connected to each other than to those outside the group. Identifying the cohesive subgroups, or cliques, in a network can help reveal how various users tend to group themselves based on the issues they reported. By setting the minimum set size of 10 we identified 6 distinct cliques. Analysis of these cliques showed that users who reported similar issues about Tor were in the same cliques. Figure 3 represents the structure of the cliques.

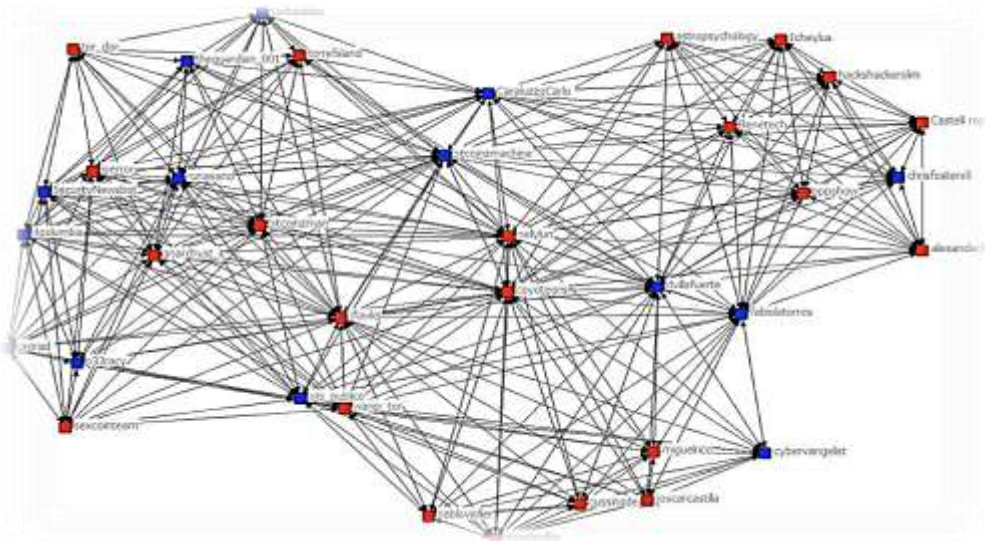


Figure 2: A row transformed dataset

The red color indicates users reporting the issues as tolerable and blue indicate users reporting issues as deal breakers

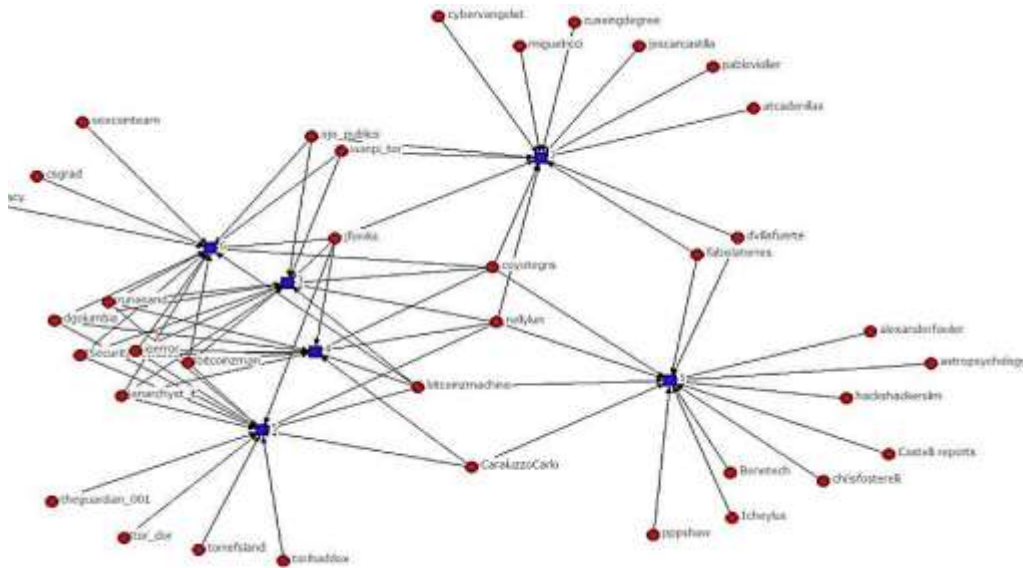


Figure 3: Structure of cliques

5.4 HIERARCHICAL CLUSTER ANALYSIS

Hierarchical cluster analysis helps reveal issues that tend to occur together frequently. Figure 4 represents a dendrogram developed in this study to analyze the column-transformed data, which grouped related issues.

The results indicated that user-interface and application related issues often occur together, followed by privacy and illegal usage concerns. This finding was confirmed by visualizing an attribute-based network model, represented in Figure 5, where the thickness of connections between issues reflected their betweenness. The strong betweenness for user-interface and application issues aligns with our hierarchical cluster analysis.

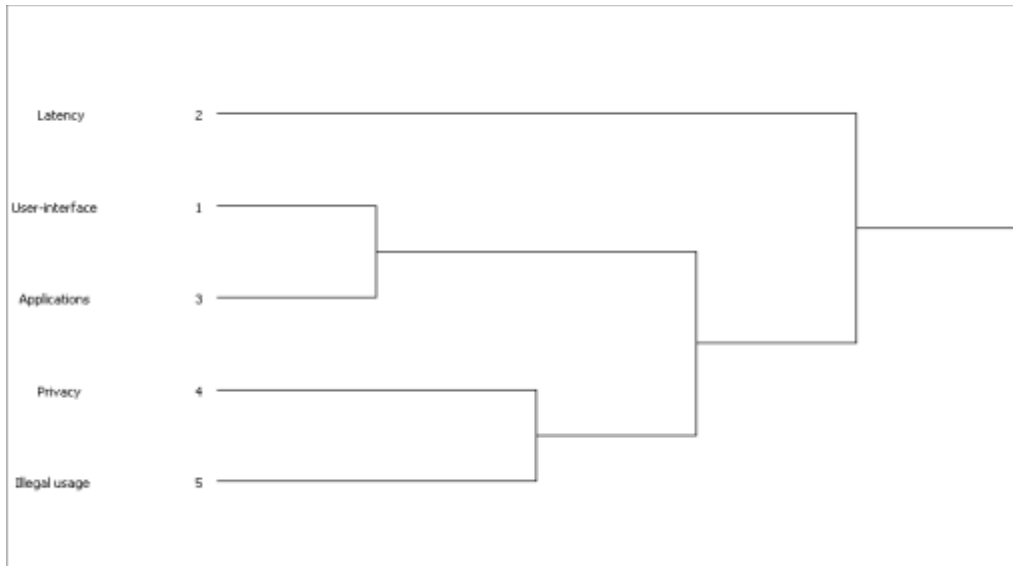


Figure 4: Dendrogram for hierarchical structural analysis

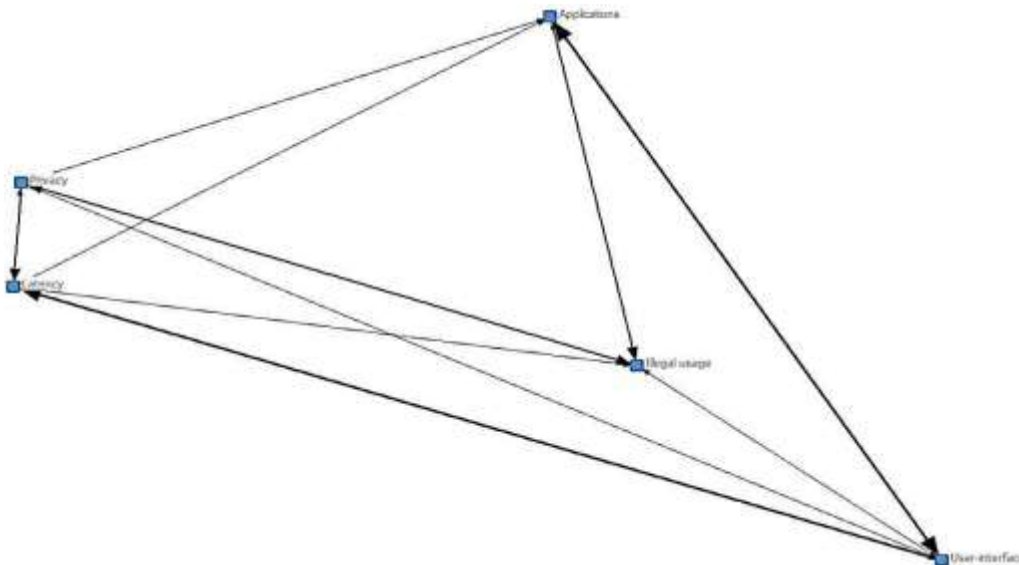


Figure 5: Visualization of attribute-based network model

5.5 CORRELATION ANALYSIS

Firstly, we tested if the type of issue reported by the user affected the users' decision to stop using the software. Our hypothesis was that the nature of the issue reported has an effect on whether or not it gets classified as a deal breaker. We evaluated our hypothesis by correlating two matrices; one for user-reported issues and the other with the 'deal breaker' attribute. The Pearson's correlation coefficient of 0.527 ($p < 0.00001$) was significant, and thus supported our hypothesis. It indicates that the nature of the issue influences whether it is viewed as a deal breaker. This hypothesis was important because it helped us to understand if being classified as a 'deal breaker' depended on the reported issue or the behavioral characteristics of the user. For instance, some users might treat all issues as deal breakers regardless of the nature of the issue. However, this analysis distinguished between deal breakers and tolerable issues.

Next, we assessed the correlation between various issues and their tolerance among users, using Independent (User-interface, latency, application integration, privacy and trust issues, illegal usage) and Dependent (Deal breaker) variables. Table 1 represents the correlation matrix built to evaluate the interdependency between the dependent and independent variables. It showed significant correlation between all the reported issues and their tolerance. Specifically, the user-interface issues were least likely, while the privacy & trust issues were most likely to be deal breakers. The correlation matrix also revealed interdependencies among issues. Figure 6 is a visual representation of correlation through Net Draw, indicating the strongest link between 'deal breaker' and 'privacy,' followed by 'application integration' and 'deal breaker.' Overall, this study suggests that distrust in Tor's privacy and anonymity and limited integration with third-party applications are major factors leading users to discontinue its use.

Table 1: Styles available in the Word template

	User interface	Latency	Application Integration	Privacy and trust	Illegal issues	Deal breaker
User interface	1	0.055	0.164	0.036	-0.032	0.159*
Latency	0.055	1	0.041	0.001	-0.160	0.180*
Application integration	0.164	0.041	1	-0.097	-0.057	0.221**
Privacy and trust	0.036	0.001	-0.097	1	0.067	0.269***

Illegal issues	-0.032	0.160	0.057	0.067	1	0.185*
Deal breaker	0.159*	0.180*	0.221**	0.269***	0.185*	1

* = $p < 0.05$; ** = $p < 0.001$; *** = $p < 0.00001$

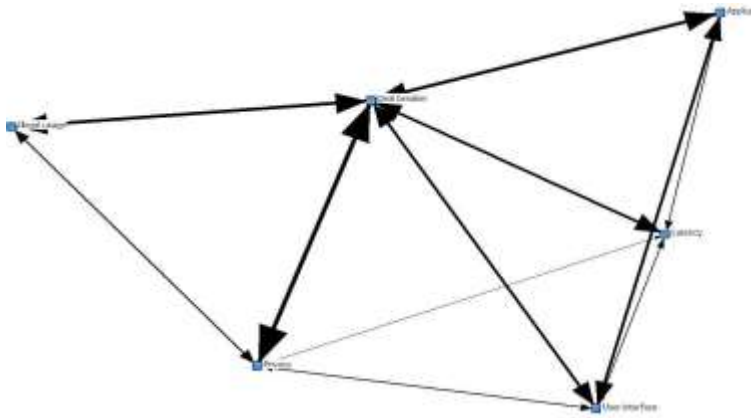


Figure 6: Visualization of attribute-based network model

6 IMPLICATIONS OF THE STUDY

This study was carried out to identify the most likely barriers in adoption of Tor software. The research was conducted in a stepwise manner, where we first evaluated the prevalence of Tor issues, the nature of user connections, and the impact of specific concerns on user behavior. This was followed by an assessment of the interconnectedness of these issues, users' perceptions of deal breakers, and the correlation between various issues and user tolerance. Overall, the key findings of the study addressing the research questions are as follows:

- Reported issues with Tor significantly influenced their classification as deal breakers.
- Privacy and trust concerns, followed by the potential for illegal use, were most likely to be considered deal breakers, whereas user-interface issues were least likely.

The study highlights the high density and visibility for the deal breaker (privacy and trust, and illegal use) issues, emphasizing their critical role in the discourse around Tor. It is reasonable to infer the interconnectedness of privacy and misuse concerns among users' of anonymization tools as supported by this study on Tor users, and another recent study on VPN users [35]. However, there may occur differences in the hierarchy of user issues, as described in a study on encrypted messaging apps, where the privacy issues among users' significantly overshadowed the misuse issues [36]. Factors such as user interconnection and engagement on Twitter may also affect the data outcomes in these studies. For example, issues like data breaches were reportedly less engaging among users [37], and those related to darknet forums had fewer interconnected users on Twitter [38], in contrast to the mutual engagement and user

interconnectedness observed for Tor in this study. These findings are interesting because they imply that users may not consider privacy and misuse issues to be as significant on a broader scale, except when these concerns are associated with anonymization softwares. Unfortunately, there are no detailed analytical reports of similar data extracted from several social media sites to compare and gain more conclusive insights into whether demographic characteristics influence these outcomes.

7 LIMITATIONS

There are certain limitations to this study. While the dataset of 300 nodes is substantial, it may not represent all user perspectives on Tor. It may have missing components in the full spectrum of user experiences and concerns. Also, although small, the possibility of Twitter users representing a demographic that is less concerned about privacy cannot be ruled out. Hence, there is a possible risk of bias in this study. Additionally, to manage the complexity and enhance clarity, visualizations were created using a subset of the network (50 out of 300 tweets) in this study. Hence, it is possible to miss certain characteristics or patterns in the tweets.

8 CONCLUSION

Tor faces significant challenges related to trust, privacy failures, low compatibility with applications, and a suboptimal user interface. By focusing on these areas and developing a comprehensive technology acceptance model, Tor can enhance its appeal and effectiveness as an anonymization tool. This approach aligns with the insights from previous studies emphasizing that achieving usability is as crucial as meeting security goals to ensure a larger and more anonymous user base. The most significant issue identified in this study was a lack of trust in Tor's ability to provide robust privacy and anonymity, followed by its limited compatibility with various applications. Through targeted improvements focused on these issues along with a user-centric approach, Tor can overcome its current barriers and foster wider adoption. Also, undertaking secondary measures like improving transparency with regards to users' data usage and explaining necessity for regular upgrades (such as to improve speed, reduce latency, and make interface more user friendly) can improve Tor acceptance among users. Besides, although the biggest challenge, addressing the negative image due to its association with illegal activities is the most crucial element in popularizing Tor. Progress in this context can be made through partnerships and collaborations with various groups and organizations that endorse and promote Tor. Educational outreach programs and media engagement can also be useful while regular security audits by developers can positively impact the users' acceptance to Tor.

REFERENCES

1. David L. Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 2 (Feb. 1981), 84–90. <https://doi.org/10.1145/358549.358563>
2. George Danezis, Roger Dingledine, and Nick Mathewson. 2003. Mixminion: Design of a Type III Anonymous Remailer Protocol. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP '03)*. IEEE Computer Society, USA, 2.

3. Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. 2001. Freenet: a distributed anonymous information storage and retrieval system. In International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability. Springer-Verlag, Berlin, Heidelberg, 46–66. https://doi.org/10.1007/3-540-44702-4_4
4. Roger Dingledine, Michael J. Freedman, and David Molnar. 2001. The Free Haven Project: distributed anonymous storage service. In: Federrath, H. (eds) Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol 2009. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44702-4_5
5. Ian Goldberg, David Wagner, and Eric Brewer. 1997. Privacy-enhancing technologies for the Internet. Retrieved July 29, 2024 from <https://people.eecs.berkeley.edu/~daw/papers/privacy-compon97-www/privacy-html.html>
6. De Moor GJ, Claerhout B, and De Meyer F. 2003. Privacy enhancing techniques - the key to secure communication and management of clinical and genomic data. *Methods Inf. Med.* 42, 2 (2003), 148-153.
7. Zhong Sheng, Yang Zhiqiang, and Wright Rebecca N. 2005. Privacy-enhancing k-anonymization of customer data. In Proceedings of the 2005 ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS, Baltimore, MD, United States.
8. N. K. Ratha, J. H. Connell, and R. M. Bolle. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* 40, 3 (March 2001), 614–634. <https://doi.org/10.1147/sj.403.0614>
9. Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-Generation Onion Router. In Proceedings of the 2004 Usenix security symposium on Advanced computing systems, San Diego, CA, USA.
10. Justin Boyan. 1997. The anonymizer. *Computer Mediated Communication Magazine*. Retrieved July 29, 2024 from <http://www.december.com/cmc/mag/1997/sep/boyan.html>
11. Spiekermann Sarah. 2007. User Control in Ubiquitous Computing: Design Alternatives and User Acceptance. Habilitation Humboldt Universität Berlin.
12. Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith. 2013. On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In: De Cristofaro, E., Wright, M. (eds) Privacy Enhancing Technologies. PETS 2013. Lecture Notes in Computer Science, vol 7981. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39077-7_13
13. Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur, and H. Raghav Rao. 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Inf. Sys. J.* 24, 1 (Jan. 2014), 61-84.

14. Younghwa Lee and Kenneth A. Kozar. 2005. Investigating factors affecting the adoption of anti-spyware systems. *Commun. ACM* 48, 8 (August 2005), 72–77.
<https://doi.org/10.1145/1076211.1076243>
15. Younghwa Lee and Kenneth A. Kozar. 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Inf. Manage.* 45, 2 (March, 2008), 109–119.
<https://doi.org/10.1016/j.im.2008.01.002>
16. San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2011. What makes users refuse web single sign-on? an empirical investigation of OpenID. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 4, 1–20.
<https://doi.org/10.1145/2078827.2078833>
17. Alma Whitten and J. D. Tygar. 1999. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 (SSYM'99)*. USENIX Association, USA, 14.
18. Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. 2006. Why Johnny still can't encrypt: evaluating the usability of email encryption software. In *SOUPS*. ACM, 3–4.
19. Philip G. Inglesant and M. Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery, New York, NY, USA, 383–392.
<https://doi.org/10.1145/1753326.1753384>
20. Sacha Brostoff, Philip Inglesant, and M. Angela Sasse. 2010. Evaluating the usability and security of a graphical one-time PIN system. In *Proceedings of the 24th BCS Interaction Specialist Group Conference (BCS '10)*. BCS Learning & Development Ltd., Swindon, GBR, 88–97.
21. Serge Egelman, David Molnar, Nicolas Christin, Alessandro Acquisti, Cormac Herley, and Shriram Krishnamurthi. 2010. Please continue to hold an empirical study on user tolerance of security delays. Retrieved July 29, 2024 from <https://cs.brown.edu/~sk/Publications/Papers/Published/emcahk-pl-cont-hold-sec-delay/paper.pdf>
22. Greg Norcie, Jim Blythe, Kelly Caine, and L. Jean Camp. 2014. Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. In *Proceedings of the Network and Distributed System Security (NDSS) Symposium, San Diego, CA, USA*.
<http://dx.doi.org/10.14722/usec.2014.23022>
23. Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* 13, 3 (September 1989), 319–340. <https://doi.org/10.2307/249008>
24. Fred D. Davis. 1993. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *Int. J. Man Machine Studies* 38, 3 (March 1993), 475–487.

<https://doi.org/10.1006/imms.1993.1022>

25. Viswanath Venkatesh and Fred D. Davis. 2000. A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Manage. Sci.* 46, 2 (February 2000), 186–204. <https://doi.org/10.1287/MNSC.46.2.186.11926>
26. Viswanath Venkatesh and Hillol Bala. 2008. Technology Acceptance Model 3 and a research agenda on interventions. *Decision Sciences* 39, 2 (May 2008), 273–315. <https://doi.org/10.1111/j.1540-5915.2008.00192.x>
27. Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User acceptance of information technology: toward a unified view. *MIS Q.* 27, 3 (September 2003), 425–478.
28. Viswanath Venkatesh, James Y. L. Thong, and Xin Xu. 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Q.* 36, 1 (March 2012), 157–178.
29. D. Harrison Mcknight, Michelle Carter, Jason Bennett Thatcher, and Paul F. Clay. 2011. Trust in a specific technology: An investigation of its components and measures. *ACM Trans. Manage. Inf. Syst.* 2, 2, Article 12 (June 2011), 25 pages. <https://doi.org/10.1145/1985347.1985353>
30. Tamara Dinev and Paul Hart. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Info. Sys. Research* 17, 1 (March 2006), 61–80. <https://doi.org/10.1287/isre.1060.0080>
31. Paul A. Pavlou. 2003. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *Int. J. Electron. Commerce* 7, 3 (Number 3/Spring 2003), 101–134.
32. Jian Mou, Dong-Hee Shin, and Jason F. Cohen. 2017. Trust and risk in consumer acceptance of e-services. *Electronic Commerce Research* 17, 2 (June 2017), 255–288. <https://doi.org/10.1007/s10660-015-9205-4>
33. Greg Norcie, Kelly Caine, and L Jean Camp. 2012. Eliminating Stop-points in the Installation and Use of Anonymity Systems: A Usability Evaluation of the Tor Browser Bundle. In *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS 2012)*.
34. Borgatti, S.P., Everett, M.G. and Freeman, L.C. 2002. *Ucinet for Windows: Software for Social Network Analysis*. Harvard, MA: Analytic Technologies.
35. Jiang Yinhao, Mir Ali Rezazadeh Bae, Leonie Ruth Simpson, Praveen Gauravaram, Josef Pieprzyk, Tanveer Zia, Zhen Zhao, and Zung Le. 2024. Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures. *Cryptography* 8, 1 (Jan. 2024), 5. <https://doi.org/10.3390/cryptography8010005>
36. Sean Oesch, Ruba Abu-Salma, Oumar Diallo, Juliane Krämer, James Simmons, Justin Wu, and Scott Ruoti. 2022. User Perceptions of Security and Privacy for Group Chat. *Digital Threats* 3, 2, Article 15 (June 2022), 29 pages. <https://doi.org/10.1145/3491265>

37. Nandita Pattnaik, Shujun Li, Jason R.C. Nurse. 2023. Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter. *Computers & Security* 125 (Feb. 2023), 103008. <https://doi.org/10.1016/j.cose.2022.103008>
38. Ildiko Pete, Jack Hughes, Yi Ting Chua, and Maria Bada. 2020. A Social Network Analysis and Comparison of Six Dark Web Forums. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Genoa, Italy, 484-493. <https://doi.org/10.1109/EuroSPW51379.2020.00071>.