Torproject's Response Mechanism on Controversial Incidents

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Siyang Sun

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

Torproject's Response Mechanism on Controversial Incidents

Introduction

With the internet boom of the 21st century, nowadays there are 4.9 billion active internet users worldwide (Flynn, 2023). Many people treat the internet as private a private space, similar to the idea of their writing letters. A lot of the internet's features model private space in the physical world, such as email modelling sending letters.. Physical mail is definitely a private space where senders and recipients assume that this conversation is private.

However, the modern internet is not a private space, there is a lot of surveillance from employers, government, and service providers. Also, users in the heavily censored country cannot access certain websites that have been blacklisted by the government. This lack of privacy and freedom on the internet prompted users to find tools to protect and free themselves. The Onion Router (TOR) appears as one of the tools among VPNs and web proxies that provide anonymous free browsing to users. My research will focus on how Tor is affected by its user group by looking into past incidents. I will also investigate how Tor as an organization treats its goal settings and development when affected by such public events.

The Onion Router

The Onion Router (Tor) - is a technology used by censored netizens, such as those in China, and privacy seekers to bypass censorship and access the web anonymously. Tor chooses three servers from over 6000 volunteers who ran servers (*Servers* 2022). It routes data securely using secure & private tunnels through these three chosen servers to the destination web server (About tor browser, n.d.). Tor is developed by a non-profit organization called Tor Project that handles the development and maintenance of Tor as software. Developers worldwide could contribute to this project since it is an open-source project.

Tor, in this heavy surveillance age, provided journalists and whistle-blowers the tools to expose questionable and often unconstitutional acts by governments or large corporations. Tor gives back their user's digital rights, "right to privacy and freedom of expression, in the context of digital technologies" (Chen et al., 2022). One of the most famous Tor users, Edward Snowden, said Tor "allowed him to fulfill his oath to the constitution of the United States and release information of public interest to the media about the abuses committed by the government through its mass surveillance program" (Thank you, Edward Snowden: Tor project, 2019). Snowden's act brought much-needed attention to online privacy and citizens' rights on the web. This incident built a positive public image and gained more support for Tor. This positive image could attract more developers, thus perfecting the tool.

Tor, on the other hand, has provided cybercriminals, including drug dealers, with the ease of anonymity at no cost. Silk road, a well know drug market hosted on Tor, has close to a million user accounts (Fung, 2021). Ironically, a government organization, the U.S. Naval Research Lab, initiated the Tor Project (The Tor Project: Privacy & Freedom Online, n.d.). When it comes to

enforcing laws online, this government-initiated endeavor could cause the government greater problems. Many organizations have decided to forbid connections to Tor relays as a result of criminal instances, including the shutdown of Silk Road, which has placed a negative light on Tor as a tool used by criminals. However, these crackdowns on cyber drug markets do not significantly affect the general operation of these online drug dealers (Décary-Hétu, Der, 2016). This is another important factor to think about since the negative effects of Tor cannot be easily countered with increased law enforcement. So further development of Tor might cause an exponential growth in the need for law enforcement personnel to keep the negative effect the same or lower than the current level.

Another use of Tor is that it allows users to escape the bubble and content personalization created by internet services that allow users to only see what they want to see (Garcia-Rivadulla, 2016). Modern internet services keep track of user information and preferences on their server. For example, if a client uses YouTube on their phone without logging in, YouTube will still keep track of what videos this client likes to watch. From this client's past selection, YouTube will push similar videos to this client's main page. Over time, this client will only see contents that he likes to see. This will create more biases over time in society.

This bubble effect is especially apparent when one gets a new phone and the browser has not yet learned the user's preference. Under this circumstance, the user will likely encounter news stories that they could never see in their previously biased browser. Since Tor sends the client's data through three different servers and the client could also request a new identity, this will enable the user to surf the web using a blank identity. Thus, service providers have no historical data to look to when displaying content, creating more neutral content for the user to see. So using Tor to browse the web is like using a new phone every day to browse the web so there is no content personalization.

The primary actors involved in Tor contains Tor developers, whistler blowers and freedom seekers, cybercriminals, censoring government, and cybercrime investigators. Whistle-blowers and freedom seekers use Tor to achieve their basic human rights of freedom of speech and access to knowledge, while the censoring government tries to stop freedom seekers and whistle-blowers from posting or reading from websites they disapprove of. In this scenario, Tor has helped to promote basic human rights and protect citizens from brutal state violence. On the other hand, cybercriminals use Tor to hide their identity and conduct illegal activities online. In this case, Tor has made cybercrime investigators' jobs hard by providing a protective mask to criminals. Under these two common use cases, Tor as an organization will be affected by both groups of users, bringing in positive publicity from whistle-blowers such as Snowden and negative publicity from exposed cyber crime ran on the Tor network.

Methods

To understand Tor's basic inner workings, I will look into Tor's organization's constitution. To explore how its user groups affect Tor's decision-making and goal settings, I will look into Tor's Forums during important censorship events, such as the Snowden incidents and

the Silk Road crackdown. These will be my primary sources extracted from Tor Project's official channels.

On the other hand, I will look for client feedback and information on Tor usage during censorship incidents to talk about how Tor has influenced society in digital rights. I will use Tor's official metrics website to gain access to these data. This evidence will enable me to conclude the conversation about Tor's impact on society and vice versa. I will use these debates to enlighten my readers about how society and the torproject deal with the trade-off that Tor introduces between digital rights and cybercrime.

Finally, I interviewed students from the UVA body to gauge public sentiment on Tor among college students to compile first-hand data. These interviews were conducted online through Zoom or offline in a one-on-one meeting format with precompiled questions. I have selected the interviewees using a convenient sample since I did not have every student's email at UVA to conduct a simple random simple. But I did take into account the academic background of the interviewees to gain a more well-rounded student opinion.

Results

Tor has helped many individuals gain freedom on the internet world, ranging from high-profile whistleblower Snowden or just ordinary curious citizens in China. These events have led the online community to recognize Tor as a symbol of freedom. Unsurprisingly, Tor's mission as a group is to promote freedom and privacy on the world wide web.

In Tor Projects Social Contract, it states the organization "make tools that help promote and protect the essential human rights of people everywhere. (*The Tor Project Social Contract*) This is the first line in the social contract, a document stating the shared value of the organization, which exhibits the importance of this value inside Tor Projects. This contract defines the community standard within Tor Project and it is also a "promise from our internal community to the rest of the world, affirming our commitment to our beliefs" (*The Tor Social Contract: Tor project* 2016). Thus, we can see that the Social Contract is an important part of Tor Project.

Further down the document, the social contract explained in detail the essence of promoting human rights in the Tor Project's sense. "We advance human rights by creating and deploying usable anonymity and privacy technologies. We believe that privacy, the free exchange of ideas, and access to information are essential to free societies. Through our community standards and the code we write, we provide tools that help all people protect and advance these rights." (*The Tor Project Social Contract, n.d.*) We could see pretty clearly that Tor, as an organization, believe that human rights on the web are essential to a free society and that they are committed to creating software that would enable everyone around the world to achieve these basic human rights.

This deep belief in freedom of speech on the internet is what guides decision-making and product development inside the Tor organization. Under this primary doctrine, Tor also promise that they would never intentionally harm their user, specifically in the social contract. "We take

seriously the trust our users have placed in us. Not only will we always do our best to write good code, but it is imperative that we resist any pressure from adversaries who want to harm our users. We will never implement front doors or back doors into our projects. In our commitment to transparency, we are honest when we make errors, and we communicate with our users about our plans to improve." (*The Tor Project Social Contract, n.d.*) This commitment is rare in this age of the internet where almost all software providers are trying to max out on the profit from their users. Creating backdoors on software could help companies gain more insight into useful information and also collect more data from users which could ultimately turn into profit. According to Github's octoverse report, close to one-fifth of all vulnerabilities are intentionally planted. (*Octo--verse, 2020*) Therefore, Tor's commitment to its user really shows its mission in privacy when most of the industry heads in the opposite direction.

Tor's commitment to privacy and freedom has also been put to test in the real world. According to CBS news, Silk road's debut on the clear web around 2011 through blog posts describing this new black market on the Onion router network and the increased international shipment of drugs caught the police's attention later on, which triggered a years-long investigation on Tor. The police were "able to actually — find vulnerabilities in the website, where they saw it actually leaking its IP address" (Batson & Chenetz, 2020). This vulnerability led to the shutdown of the silk road. If Tor had a backdoor for such purposes, it will most likely be pressured by the police and FBI to use it to catch the silk road administrators. The years-long investigation by the police and the tedious road of finding vulnerabilities further supported the claim by Tor that no backdoor exists in their program. We could see that Tor is very firm on its mission statement and that during periods of the public spotlight, Tor, as an organization, still upholds its mission of promoting freedom and privacy on the web. This mission is the foundation of Tor Projects' inner workings.

From Tor's forum posts and discussions, we could see that Tor users' experience indeed affects the decision of Tor Projects. According to Meduza, a Russia-focused independent new source, Russian has tightened its internet censorship in December 2021 and Tor users in Russia could not connect to the Tor network which they previously could. (Meduza, *2021*) Russian Tor users are one of the top ten users groups of the Tor network, who make up around 15 percent of all Tor users worldwide in late 2021. (*Users, 2021*) This ban on Tor in Russia will leave many Russian users blocked from the free internet and also leave them vulnerable to government surveillance.

Tor Project responded to this censorship incident by raising awareness in their developer community by sending out blog posts to encourage the increase of Tor Bridges. "We are calling on everyone to spin up a Tor bridge! ", stated one of the Blog posts on the official Tor forum. (*Responding to tor censorship in Russia, 2021*) Tor bridges are used when a client cannot directly connect to the entry Tor relay successfully, so they use Tor bridges as another stop on Tor's routing path. These bridges are not publicly listed, so it has less of a chance of being blocked by censorship (*What is a bridge?, n.d.*). Bridges hide the fact that the user is connected

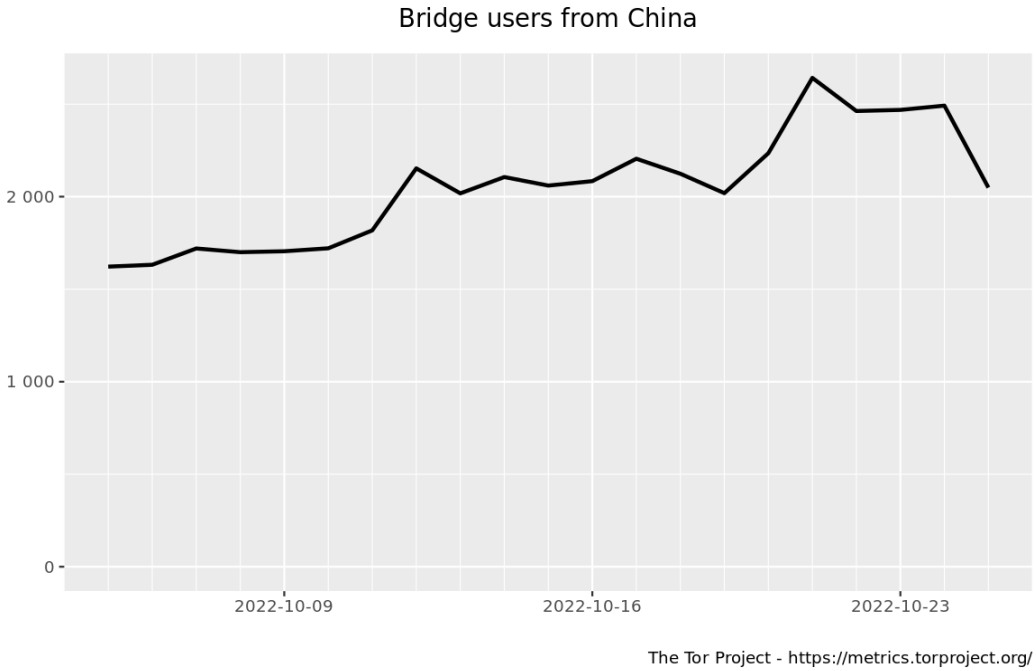
to a Tor network, so these connections will not be blocked by network operators due to being suspicious (*Tor relays and Bridges, n.d.*).

The Tor developer community has responded to this call and according to Gus, a user in the Tor forum, 200 new bridges were deployed after only 48 hours of the call build new Tor bridges (gus, 2021). We could see that Tor Project is affected by its user group on a day-to-day basis. When a user group is having trouble using their service, the developer community rushes to support this group and changes Tor accordingly. In 2023, although Russian Tor users have dropped percentage-wise, but they still have a mean daily user of around 90,000. (*Users, 2023*) This significant daily Russian user proves that the Tor community's mission to build new Tor bridges helped Russian users to stay connected and anonymous on the world wide web. Russian users' difficulty with increased censorship led Tor to improve its Tor Bridge program. This is one way how Tor's user group affects Tor Project's decision as an organization. However, this relationship goes in both directions. Not only does Tor's user group affects Tor, but also Tor would affect its users' worldwide changing their perspective on the world.

Triggered by tight Covid restrictions and general frustration towards the government, one man in Beijing, China decided to hang anti-government posters in October 2022 on a busy highway bridge in urban Beijing to vent out anger towards the current regime and also call for change in China. This is a rare scene in mainland China since it is under heavy state surveillance and there are special police forces that are used to put out uprises and protests. Because of the Great Fire Wall in China, most people could not even learn about this event inside China's censored internet environment, despite hearing different perspectives of this event.

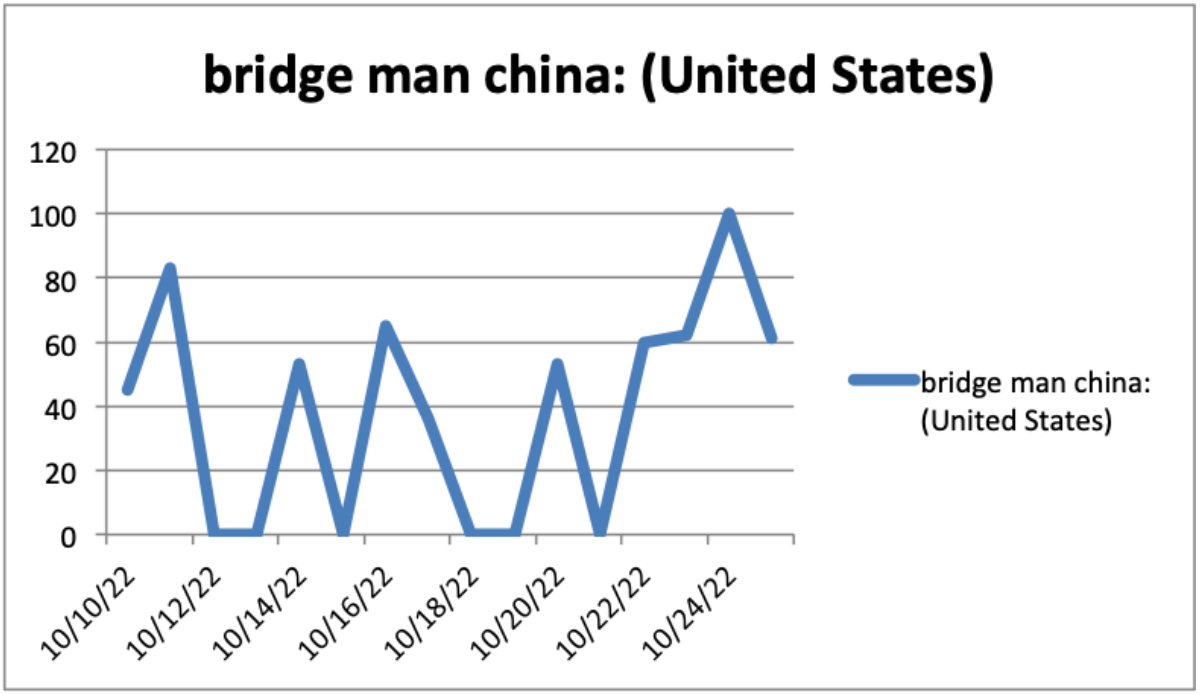
Tor, following through with its mission statement about the free exchange of ideas, helps people in China to learn about this latest protest. Figure 1 is the amount of Chinese Tor users that access the Tor network through bridges, the primary method to use Tor in China due to censorship. We can see that there is a local maximum from October 21st to 24th. This means that there are more Tor users from China than previously in this time range. Most exit relays are hosted inside the United States (*Tor exit nodes mapped and located* 2020). From the Google trends chart in the US, we learned that there is also a peak in the keyword "China Bridge Man" searched in roughly the same time period. We could, thus, infer that Tor has helped Chinese netizens to access the free internet to exchange ideas freely that would otherwise be banned in China. This will definitely change how these Chinese netizens view their government since Tor allowed them to access news sources that offer events on current China that are not available through Chinese media. This might gradually change the national consciousness of China on their government through peaceful evolution.

Figure 1



Number of Bridge users from China, sourced from Tor Metrics

Figure 2



Interest Level on “bridge man china” search sourced from Google Trends

This channel for exchanging information, provided by Tor, changed and shaped their user group in censored countries. The information they received through Tor will add a new perspective to how they see current events as well as those around them, such as their family and friends. Thus, we could see that Tor could affect its user group as well as vice versa. So this is a mutual shaping relationship between Tor Project and its user group.

So far we have looked at Tor on a macro level, by analyzing user data and policies. When exploring a topic, it is also important to study the micro level of the problem to provide some concrete arguments. To study Tor on a personal level, I have conducted interviews with UVA students to ask them about their opinions on Tor.

One of the students expressed the opinion that Tor should develop freely as an organization to promote freedom of speech on the internet. Each country should have its policy regarding Tor depending on its tolerance of the trade-off between digital rights and cyber crimes. This student is majoring in Computer Science and Media Studies, so his opinion represents someone with both technical and humanity backgrounds. This insight will be more well-rounded since the student has an interdisciplinary background.

Another student believed that Tor should be banned outright since there are illegal activities conducted on the network. This is a perspective that is not always discussed in past literary reviews. This student comes from a non-technical background. This non-technical background will likely cause the student to focus on a more easily understood Tor topic that is available on mainstream media. A lot of the time, these mainstream media only focus on the bad aspects of Tor that involve the drug trade to capture more attention. So this negative view of Tor might come from a lack of education on Tor. These interviews could give us a glimpse into what UVA students think about Tor. Also, it gives future Tor developers a possible understanding of some of the negative image the public has on Tor. Building based on this understanding, Tor developers could create activities that will try to change the public perception of Tor.

Conclusion

From the above analysis, we have seen that Tor is affected by its user group through the experience of the user and also through its official forum channels. This is important to note because Tor is usually discussed as an organization that develops anonymous browsing software. However, the general public often fails to ignore that the direction of Tor development is not only dictated by leaders within the organization but is also heavily influenced by its users. This is important to note when analyzing the negative effects of Tor on society since Tor Project did not make all of the development decisions and some are made by Tor users through feedback and forum posts.

Tor, on the other hand, also affects its users through its technology and service. Users worldwide are affected by Tor's ability to circumvent censorship and gain new perspectives on the world. This will change the consciousness of a user group and gain awareness of certain events in heavily surveillance states. This could change the political situation of a country

through peaceful evolution using Tor as a medium. This possibility of transforming a nation's consciousness through Tor has not been studied extensively and could be an area to be further discussed through academic research. It is also vital to study the outlook of Tor on younger generations. This might predict Tor's direction of development in the long run.

References

Flynn, J. (2023). *How many people use the internet? [2023]: 35 facts about internet usage in America and the world*. Zippia Retrieved March 31, 2023, from https://www.zippia.com/advice/how-many-people-use-the-internet/

torproject. *(2022). Servers. Tor Metrics. Retrieved May 2, 2023, from https://metrics.torproject.org/networksize.html*

About tor browser. ABOUT TOR BROWSER | Tor Project | Tor Browser Manual. (n.d.). Retrieved October 25, 2022, from https://tb-manual.torproject.org/about/

Chen, Z., Jardine, E., Fan Liu, X., & Zhu, J. J. (2022). Seeking anonymity on the internet: The knowledge accumulation process and global usage of the Tor Network. *New Media & Society*, 146144482110722. https://doi.org/10.1177/14614448211072201

Thank you, Edward Snowden: Tor project. The Tor Project. (2019, December 25). Retrieved October 25, 2022, from https://blog.torproject.org/thank-you-edward-snowden-tor/

The Tor Project: Privacy & Freedom Online. Tor Project | History. (n.d.). Retrieved October 25, 2022, from https://www.torproject.org/about/history/

Décary-Hétu, D., & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law and Social Change, 67(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

Garcia-Rivadulla, S. (2016). Personalization vs. privacy. *IFLA Journal*, *42*(3), 227–238. https://doi.org/10.1177/0340035216662890

Fung, B. (2021, December 6). *7 revealing numbers about silk road, the internet's darkest drug market*. The Washington Post. Retrieved March 31, 2023, from https://www.washingtonpost.com/news/the-switch/wp/2013/10/02/7-revealing-numbers-about-silk-road-the-internets-darkest-drug-market/

torproject. (n.d.). *The Tor Project Social Contract*. SOCIAL_CONTRACT.TXT - community/policies - proposed and adopted community policies, etc. Retrieved March 31, 2023, from https://gitweb.torproject.org/community/policies.git/tree/social_contract.txt

Octo--verse. Octoverse 2020 Report. (2020). Retrieved March 31, 2023, from https://octoverse.github.com/2020/

Batson, A., & Chenetz, R. (2020). Inside the FBI takedown of the mastermind behind website offering drugs, guns and murders for Hire. CBS News. Retrieved May 2, 2023, from https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/

Meduza. (2021). *В России начали блокировать tor с помощью оборудования для изоляции рунета*. Meduza. Retrieved March 31, 2023, from https://meduza.io/news/2021/12/03/zhiteli-rossii-pozhalovalis-na-blokirovku-tor

torproject. (2021). *Users*. Tor Metrics. Retrieved March 31, 2023, from https://metrics.torproject.org/userstats-relay-table.html?start=2021-10-12&end=2021-11-10

gus. (2021, December). Responding to Tor censorship in Russia. torproject forum. https://forum.torproject.net/t/responding-to-tor-censorship-in-russia/1057

torproject. (2023). *Users*. Tor Metrics. Retrieved May 2, 2023, from https://metrics.torproject.org/userstats-relay-table.html?start=2023-01-12&end=2023-02-10

Google trends. (2022). bridge man china, Retrieved April 1, 2023, from https://trends.google.com/trends/explore?hl=en-US

torproject. (2022). *Bridge users from China*. Tor Metrics. Retrieved March 31, 2023, from https://metrics.torproject.org/userstats-bridge-country.html

Tor relays and Bridges. Tails. (n.d.). Retrieved May 2, 2023, from https://tails.boum.org/doc/anonymous_internet/tor/index.en.html#:~:text=Tor%20bridges%20are%20secret%20Tor,who%20monitors%20your%20Internet%20connection.

torproject. (n.d.). *What is a bridge?* Support. Retrieved May 2, 2023, from https://support.torproject.org/censorship/censorship-7/

torproject. (2016, August 10). *The Tor Social Contract: Tor project*. The Tor Project. Retrieved May 2, 2023, from https://blog.torproject.org/tor-social-contract/#:~:text=At%20The%20Tor%20Project%2C%20we,were%20more%20or%20less%20unspoken.

Tor exit nodes mapped and located. HackerTarget.com. (2020, March 2). Retrieved May 2, 2023, from https://hackertarget.com/tor-exit-node-visualization/