Internet Anonymity Systems: A Tool for Negotiating Privacy in the United States

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

Justin Fabrizio

Spring 2022

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

Sean M. Ferguson, Department of Engineering and Society

Internet Anonymity Systems: A Tool for Negotiating Privacy in the United States

While data collection can be seen as financially beneficial for many private companies and can improve user experience, data breaches have become an increasingly common occurrence in the United States and expose users to identity theft and other forms of fraud. Additionally, data breaches can be financially destructive to the companies storing data; in 2015 it was estimated that data breaches cost a total of $10 billion annually in the U.S. (Romanosky, 2016). Internet data mining has also produced fears about government surveillance; federal wiretapping laws were once thought to protect citizens from online government surveillance, but evidence exists that federal entities including the NSA have partnered with major tech companies to obtain data on their users. In recent years, these and many other concerns have put a spotlight on internet anonymity systems as a way to limit the amount of data collected by websites and internet service providers. An internet anonymity system is any piece of infrastructure that provides internet communication without leaking enough information to identify the communicating parties(Oujani, 2011). This paper will explore how internet anonymity systems have become a tool for negotiating power and privacy in the United States.

Literature Review

This topic will be studied through the theoretical framework of sociotechnical imaginaries. Sociotechnical imaginaries are collective assumptions and representations that facilitate, envision, or contest a sociotechnical order (Hess & Sovacool, 2020). Sociotechnical imaginaries are oftentimes manifested in the design of new technologies. While examining sociotechnical imaginaries regarding public security, Lars Gerhold (2021) aptly summarizes this notion: “Technologies condition social change, yet social change also conditions technological

development" further stating "technologies are inseparable from the broader social contexts in which they arise (p. 1)."

Geoffrey Gimse looks at the evolution of computer networking architecture through the lens of sociotechnical imaginaries, particularly those at the public scale. Gimse analyzes the imaginaries of three "publics" in particular: those of the implementers, vendors, and users of computer networking systems. He defines publics as the groups of people who are a key audience of the technology he is studying. When examining the imaginaries of each public, Gimse draws conclusions based on both the origins and technological results of each imaginary as well as the conflicts and interactions between them throughout their histories (Gimse, 2019, pp. 2-5). A similar strategy can be adopted to research internet anonymity systems. Despite the varying uses of internet anonymity systems, the stakeholders in these systems can be easily divided into two publics: implementers and users. The vendor public defined by Gimse can be omitted for this research as anonymity software is typically open source. This research will establish how the imaginaries of these two publics have formed, how they interact, and how they have resulted in the modern status quo of internet anonymity systems.

First it is necessary to assess the conclusions reached by other scholars in regards to similar topics. After taking a closer look at a 2013 government surveillance leak, Florek (2014) attempted to define a "modern expectation of privacy for a modern society." In the context of the article, this question can be rephrased as "what level of privacy should be expected in a society where the internet is a part of everyday life?". Florek concludes that data privacy is now too broad of an area to be adequately addressed by isolated judicial rulings and that, moving forward, third party data collectors and the government alike should better acknowledge that a voluntary disclosure of specific information on the internet does not mean that an individual has

abandoned all privacy interests. Furthermore, Florek states that people "have a default expectation of privacy in their affairs and personal information (p. 36)." This expectation suggests an American value at play behind the current data-privacy sociotechnical imaginary and, likewise, provides a good starting point for further research into this imaginary. Another scholar, John N. Gathegi, addresses primarily the legal aspects behind internet anonymity in the United States, but also brings up some important points with respect to how anonymity is valued in the United States. Gathegi views internet communications as an extension of speech, and likewise draws parallels between anonymous speech and internet anonymity (Gathegi, 2016, pp. 1-2). Looking at internet anonymity as a form of free speech can help explain why it is so valued by the American public. More specifically, the cultural importance of free speech in the United States (particularly in political discourse) could be a major contributing factor to the current user imaginary that values data-privacy and internet anonymity and it will be important to consider this when further analyzing the user imaginary.

The User's Imaginary

Tor Browser is the most popular internet anonymity system to date. As of 2022, Tor Project, the non-profit creator of Tor Browser, states that Americans account for the largest percentage of Tor Browser users at over 20%, followed by numerous European countries (Tor Project, 2022). From this statistic, it can be inferred that opinions held by the American public likely align with those of Tor Browser's users. Recent surveys show that a majority of Americans are concerned about how their internet data is being collected and used. In a 2019 survey, 84% of U.S. adults stated that they felt they had very little to no control over government-collected data. Furthermore, 66% stated that the risks of government-collected data outweigh the benefits and 64% stated that they were concerned about how that data was being

used (Auxier et al., 2020). It should also be noted that 78% of those surveyed expressed a lack of understanding about data use; it is possible that this lack of understanding may contribute to increased skepticism regarding government data collection. Regardless, this survey still indicates that widespread feelings of concern and lack of control regarding data privacy exist amongst the American public who are the most prominent users of Tor Browser. In the context of the user imaginary, this provides strong evidence for the existence of pro-anonymity and pro-data privacy values in the user public's vision for the future of internet anonymity systems.

Due to the nature of internet anonymity systems, it can be hard to pin down the demographics of Tor users outside of broad metrics; however, several isolated incidents can provide information about the user imaginary. One such incident that received national attention was the arrest of Ross Ulbricht in 2013 for his involvement in the operation of the "Silk Road", a Tor hidden service (The United States Department of Justice, 2015). Tor hidden services are servers that are only accessible through the Tor network. Ulbricht's "Silk Road" service acted as an online black market in which it is estimated over 70% of the products offered were illegal drugs (Zajacz, 2016, pp. 1-2). Ulbricht's arrest led to increased attention on Tor and internet anonymity systems from both the public and politicians alike. More importantly, this incident showed the American people the criminal uses of anonymity systems; in particular, how they could be used to channel illicit goods and services throughout the country. Furthermore, the investigation and arrests were conducted by an entity of the federal government, the FBI, likely showing policy makers that pursuing criminals hiding behind internet anonymity systems was not futile. With that being said, a 2019 study found that 93% of Tor users only used the system to access clearnet sites, meaning that these users were most likely using Tor as a privacy tool rather than a platform for illicit activity. This distinction is important when considering the user

imaginary as it indicates that underlying values of data privacy are more prevalent than criminal intention when a person decides to use Tor Browser (Jardine, 2020).

Tor Browser is a popular anonymity tool for corporations, not just individuals, and, as such, their visions should be taken into account when considering the imaginary of the user public. Multiple news organizations such as BBC News, Radio Free Europe, New York Times, and ProPublica host Tor hidden services as a means of censorship circumvention. More specifically, these sites are hosted on Tor to ensure that non-state media is accessible in regions under authoritarian rule and as a safe outlet for whistleblowers or reporters to deliver information to the media (Ellis, 2014). These particular uses of Tor Browser suggest that this technology has enabled values of free speech to become more prevalent in the user imaginary by providing more avenues for decentralized media to reach their audiences.

While the imaginary of the user public might be seen primarily as one that is shaped by the technology (as opposed to one that shapes it), the introduction of internet anonymity systems outside of Tor Browser have shown how the user imaginary has had an impact on the development of the technology as a whole. A multitude of internet anonymity systems that use onion routing, the pivotal technology behind Tor Browser, have been developed in Tor Browser's wake. Two of the most popular of these systems are Invisible Internet Project (I2P) which uses its own network to replicate Tor's onion routing system and Brave, a browser which interfaces with Tor Browser's network (Brave Software, 2020). I2P and Brave both offer new innovations on top of Tor Browser's functionality, perhaps the most significant of which being mobile functionality (Invisible Internet Project, 2022). Allowing users to access onion-routing via a mobile application greatly increases the number of potential users, broadening the user public. The fact that the Invisible Internet Project and Brave Software Inc. are for-profit

organizations implies that the development of these new features is a result of a pre-existing user imaginary that was shaped by Tor Browser. The values of free-speech, pro-data privacy, and pro-internet anonymity all contribute to the increased accessibility available in newer internet anonymity systems like I2P and Brave.

Implementer's Imaginary and the Creation of Onion Routing

As opposed to the imaginary of the user public, the imaginary of the implementer public should have a much more discernible impact on the development of internet anonymity systems. Examining the history of onion routing can help explain who the implementers of internet anonymity systems are and what makes up their imaginary. The U.S. Naval Research Laboratory in Washington D.C. began researching secure encryption and routing methods in the early 1990's and had revealed a publicly accessible onion routing system in 1996. One of the computer scientists at that lab, Paul Syverson, would go on to co-found the Tor Project and subsequently help develop Tor Browser (Tor Project, 2021). From this information, it can be ascertained that the U.S. federal government accounted for a large portion of the implementer public during the late 1990's and early 2000's until the Tor Project was founded. At first glance, it would seem that Tor Project developers would henceforth be the sole party active in Tor Browser's implementation; however, Tor Project financial statements indicate that government funding continued throughout 2010's indicating that, at a minimum, the federal government either shared or continued to have influence over the social values at Tor Project and likewise, contributed to the implementer imaginary (Tor Project, 2013).

When evaluating the implementer imaginary behind the creation of Tor Browser, two key features of the system come to mind. The first main feature of Tor Browser, like most internet anonymity systems, is onion-routing through an overlay network. Onion-routing, a form of

layered encryption, is the core technique responsible for keeping the user's traffic secure when communicating over the Tor network (Goldschlag, 1999). Secondly, the software for Tor Browser, notably, is open source, meaning that anyone with sufficient hardware can communicate over the Tor network or participate in the Tor network by hosting Tor relays themselves. Both of these features indicate that values of pro-data privacy and pro-anonymity existed within the federal government during the late 1990's and early 2000's and were key aspects of the implementer imaginary at that time.

During the 2010's, several government data leaks would expose data surveillance programs which would contradict this pro-data privacy implementer imaginary. Perhaps the most prominent leak regarding government data surveillance reached the public eye in 2013 and indicated that the National Security Agency (NSA) had been conducting data surveillance in partnership with major tech companies under a program codenamed "PRISM" (FTC, 2013). The leak revealed a set of training presentation slides briefing the audience about this relationship. Important details included a slide claiming that their data collections had begun mid-2007 starting with Microsoft and another slide listing what forms of media they collected, which included emails, photos, VoIP, and metadata. Additionally, several slides detailed how the NSA had attempted to deanonymize users by hosting malicious sites on the Tor network that would install tracking software onto the users' machines through a JavaScript plug-in (NSA, 2013). By nature, this type of attack would deanonymize anyone who accessed their site, meaning that the surveillance being performed by the NSA was not targeting specific users. This insinuates that any pro-surveillance values present within the implementer imaginary were targeted towards a broader public rather than specific, criminal, Tor users. The American public appeared to suffer a knee-jerk reaction to this revelation; over 25 lawsuits were filed against the federal government

in some capacity within a year of the leak. While the majority of these cases were dismissed, they provide an example of direct conflict between the user and implementer imaginaries (Nelson, 2013).

The existence of pro-surveillance values within the implementer imaginary was further confirmed by a series of classified documents leaked in 2017, collectively known as "Vault 7", which revealed that the Central Intelligence Agency (CIA) maintained a comprehensive collection of tools and techniques to collect data from a variety of devices used by the general public such as smartphones, smart TVs, cars, and web browsers. Vault 7 also revelead that the CIA coordinated data collection with other agencies including the NSA, FBI, and DHS (WikiLeaks, 2017).

Together, these leaks show that as early as 2013, government agencies had attempted to deanonymize the users of internet anonymity systems on a broad scale. One explanation for these values being incorporated into the implementer imaginary could be the presence of a pre-existing societal vision that relies heavily on data surveillance and lack of internet privacy. In addition to new technologies, the visions of governing bodies are also frequently manifested in new laws; a shift in surveillance laws in the United States appears to mirror the addition of surveillance values into the implementer imaginary during the 2000's. More specifically, closely regulated wiretapping at the federal level has been permitted for criminal investigations since 1968 with the passage of the Omnibus Crime Control and Safe Streets Act (Hibbard, 2012); however, much broader internet surveillance was authorized with the passage of the USA PATRIOT Act in October of 2001. This act allowed Internet Service Providers to disclose customer information and traffic content to law enforcement agencies simply if the provider believed that death or serious injury would result without law enforcement intervention (Birnhack & Elkin-Koren,

2003). This marked a significant relaxation of wiretapping restrictions as the former bill required that a court order first be obtained before the wiretapping could take place. The passage of this law was preceded by the September 11th terrorist attacks by only a month; it is not unreasonable to assume that heightened fears of terrorism sparked the formation of new values within the federal government that were later manifested into new laws and activities, and likewise, into the implementer imaginary of internet anonymity systems.

The existence of such an implementer imaginary seems contradictory to one that would produce an open source internet anonymity system for the general public in the first place. A deeper understanding of the user of internet anonymity systems suggests that the implementer imaginary at the time was not as generous to the users as it may have seemed. An internet anonymity system is clearly not anonymous if only one party is communicating over it, meaning that it could also be argued that the onion-routing technique developed by the U.S. Naval Research Laboratory was only made available to the public to further protect state entities using the system. Evidence for this notion comes from a statement made by Runa Sandvik, a security researcher who helped develop Tor: "if you have this anonymity system and [all] traffic going into the system is the U.S. Navy and everything popping out is the U.S. Navy, then you're not that anonymous … by opening up this system to everyone, different groups of people can hide in a big crowd of anonymous Tor users" (Chertoff, 2017). With this logic, the values of Tor Project and the federal government seem much more aligned within the pro-surveillance implementer imaginary.

Discussion

Considering this evidence, it appears that the implementer and user imaginaries for internet anonymity systems are at odds. Values and visions within the user imaginary appear to

be well-aligned in support of a data private and digitally anonymous future. Intuitively, this makes sense due to the very nature of Tor Browser as an internet anonymity system; however, pro-internet anonymity visions are also evidenced by growing concern regarding data privacy by the broader American public, Tor usage by large media corporations, and the development of new and more widely accessible internet anonymity systems like I2P and Brave. This observation also aligns with Gathegi's conclusion that free speech values within the American public translate to online interactions. On the other hand, the imaginary of the implementer public appears to contain visions and values supportive of large-scale surveillance and data collection as evidenced by the relaxation of federal wiretapping restrictions, government data surveillance leaks like PRISM and Vault 7, and government investigations of illicit Tor activity. Even actions that appear to be supportive of a pro-data privacy future, such as the development of onion-routing and the funding of Tor Project, are overshadowed by the government's need for a large user base to conceal their own actions on the Tor network. In this particular aspect, similarities can be drawn between the implementer and user imaginaries as both are seeking to preserve internet anonymity to some degree, yet the notable difference is that the implementer public seemingly desires to constrict this privacy to a much smaller group of people.

This difference in visions emerges as an ongoing struggle between the implementer and user imaginaries over how broad the accessibility of internet anonymity should be in the United States. This relationship shows how Tor Browser and other internet anonymity systems have become a means for negotiating privacy in the United States as both the implementer and user publics rely on one another's existence in order to maintain a usable internet anonymity system. In the future, it may be valuable to expand this research to include a heavier focus on private and

for-profit internet anonymity systems to analyze the degree to which monetary assets influence the relationship between the user and implementer publics.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center: Internet, Science & Tech. Retrieved March 10, 2022, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Florek, A. (2014). *The problems with prism: How a modern definition of Privacy Necessarily Protects Privacy Interests in Digital Communications*. Retrieved March 10, 2022, from https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1744&context=jitpl

Gathegi, J. N. (2016, July 17). *Internet anonymity, reputation, and freedom of speech: The US Legal Landscape*. Retrieved March 10, 2022, from https://deliverypdf.ssrn.com/delivery.php?ID=599110006119023017103104030096106117063092005021001065087073072018066031125127103005050023002057007036006022108024102089112074037018087036085027117084008084116077075027005032002081113020115000110114117000117083074069102101123097082070025104083095071073&EXT=pdf&INDEX=TRUE

Lim, D., Zo, H., & Lee, D. (2014, January 13). *The Value of Anonymity on the Internet*. Retrieved March 10, 2022, from https://www.researchgate.net/profile/Hangjung-Zo/publication/221581285_The_Value_of_Anonymity_on_the_Internet/links/00b4952d361e380947000000/The-Value-of-Anonymity-on-the-Internet.pdf

Bureau, U. S. C. (2021, April 19). *Computer and internet use in the United States: 2018*. The United States Census Bureau. Retrieved October 4, 2021, from https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html.

Romanosky, S. (2016, December). *Examining the costs and causes of cyber incidents*. Federal Trade Commission. Retrieved October 17, 2021, from https://academic.oup.com/cybersecurity/article/2/2/121/2525524.

Federal Trade Commission. *Government surveillance and the internet*. (2015, October). Retrieved October 4, 2021, from https://www.ftc.gov/system/files/documents/public_comments/2015/10/00023-97629.pdf.

The Tor Project: Privacy & Freedom Online. *Tor Project History*. (2021, October). Retrieved October 4, 2021, from https://www.torproject.org/about/history/.

Tor Project. (2022, April 25). *Users*. Tor Metrics. Retrieved April 25, 2022, from https://metrics.torproject.org/userstats-relay-table.html

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017, January 1). *Understanding the Mirai botnet*. Google Research. Retrieved October 17, 2021, from https://research.google/pubs/pub46301/.

Birnhack, M., & Elkin-Koren, N. (2003, April 10). *The invisible handshake: The reemergence of the state in the digital environment*. SSRN. Retrieved October 17, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=381020.

Hibbard, C. M. (2012). *Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance*. Retrieved October 17, 2021, from https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1617&context=fclj.

Oujani, A. (2011, December 6). *Tools and protocols for anonymity on the internet*. Retrieved October 17, 2021, from https://www.cse.wustl.edu/~jain/cse571-11/ftp/anonym/index.html#Anonymity.

Tor Project. *Servers*. Tor Metrics. (2021, October). Retrieved October 17, 2021, from https://metrics.torproject.org/networksize.html.

Tor Project. *CONSOLIDATED FINANCIAL STATEMENTS AND REPORTS REQUIRED FOR AUDITS IN ACCORDANCE WITH GOVERNMENT AUDITING STANDARDS AND OMB CIRCULAR A-13* (2013, December 31). Retrieved October 17, 2021, from https://www.torproject.org/static/findoc/2013-TorProject-FinancialStatements.pdf.

Zajacz, R. (2016, April 17). *Silk road: The market beyond the reach of the State*. Retrieved November 1, 2021, from https://clas.uiowa.edu/commstudies/sites/clas.uiowa.edu.commstudies/files/Zajacz_SR16_proofs.pdf.

Cochrane, N. (2011, February 2). *Egyptians turn to Tor to organize dissent online*. SC Magazine. Retrieved November 1, 2021, from https://web.archive.org/web/20111213154629/http://www.scmagazine.com.au/News/246707,egyptians-turn-to-tor-to-organise-dissent-online.aspx.

Hess, D. J., & Sovacool, B. K. (2020, February 18). *Sociotechnical matters: Reviewing and Integrating Science and Technology Studies with energy social science*. Retrieved March 10, 2022.

Chertoff, M. (2017, March 13). *A public policy perspective of the dark web*. Retrieved March 11, 2022, from https://doi.org/10.1080/23738871.2017.1298643

Gerhold, L. (2021, June 20). *Sociotechnical imaginaries of a secure future*. National Library of Medicine. Retrieved April 11, 2022, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8215639/

Gimse, G. (2019, May). *Culture and Code: The Evolution of Digital Architecture and the Formation of Networked Publics*. Retrieved April 21, 2022, from https://dc.uwm.edu/cgi/viewcontent.cgi?article=3075&context=etd

Nelson, S. (2013, June 12). *PRISM Class-Action Lawsuit Filed: $20B, Injunction Sought Against 'Complicit' Companies and Officials*. Retrieved April 24, 2022, from https://www.usnews.com/news/newsgram/articles/2013/06/12/prism-class-action-lawsuit-filed-20b-injunction-sought-against-complicit-companies-and-officials

Jardine, E. (2020, November 30). *The potential harms of the Tor anonymity network cluster disproportionately in free countries*. Retrieved April 25, 2022, from https://www.pnas.org/doi/10.1073/pnas.2011893117

Invisible Internet Project. (2022, April). *I2P: A scalable framework for anonymous communication*. Retrieved April 25, 2022, from https://geti2p.net/en/docs/how/tech-intro

Brave Software. (2020, October 5). *Brave.com now has its own Tor Onion Service, providing more users with secure access to brave*. Brave Browser. Retrieved April 25, 2022, from https://brave.com/new-onion-service/

Goldschlag, D. (1999, January 28). *Onion Routing for anonymous and private internet connections*. Retrieved April 25, 2022, from https://www.onion-router.net/Publications/CACM-1999.pdf

WikiLeaks. (2017, March 7). *Vault 7: CIA Hacking Tools Revealed*. Retrieved April 25, 2022, from https://wikileaks.org/ciav7p1/

NSA - IC off the record. (2013). *NSA PRISM slides*. Retrieved April 26, 2022, from https://nsa.gov1.info/dni/prism.html

The United States Department of Justice. (2015, May 29). *Ross Ulbricht, a/k/a "Dread pirate roberts," sentenced in Manhattan Federal Court to life in prison*. U.S. Attorney's Office Southern District of New York. Retrieved April 10, 2022, from https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison

Ellis, J. (2014, June 5). *The Guardian introduces SecureDrop for document leaks*. Nieman Lab. Retrieved April 26, 2022, from https://www.niemanlab.org/2014/06/the-guardian-introduces-securedrop-for-document-leaks/