Winter 2022

Public Libraries and the Implementation of The Onion Route (Tor)

Ronique Gillis

Public Libraries and the Implementation of The Onion Route (Tor)

Ronique Gillis

GRADLIS 9704: Librarianship & Evolving Technologies

December 12, 2022

The world wide web is divided is into three layers; the surface web, the deep web, and the dark web. The surface web is where the everyday browser can easily peruse through information indexed by common search engines such as Google or Bing. It is estimated that the surface web only contains a limited amount of free content, approximately 0.3% of the internet, that can be accessed (Islam & Ozkaya, 2019, p. 18). The deep web is approximately “4,000-5,000 times larger than the surface web” (p. 18). This part of the internet dives down further and contains more sensitive information such as medical records, legal documents, scientific reports, financial records, etc. all of which takes considerably more effort for someone to get their hands on, especially if the data does not belong to them. Lastly, the dark web consists of the deepest layers of the internet where certain browsers are needed to access it since it contains information that is intentionally hidden.

The Onion Router (Tor) is one of those browsers that can access the dark web as it is a browser that operates with the optimization of privacy and security of its users as one of its main reasons for operation. For this reason, some libraries have taken to advocating for the implementation of Tor into the library space. I, on the other hand, will argue against the implementation of Tor in public libraries because it can be used by to commit harmful and/or dangerous acts and there is a gap in the policies provided by the American Library Association that addresses patrons’ access to such browsers. Prior to the arguments, a brief description of Tor and its relationship with the dark web will be provided.

The Onion Router (Tor)

To begin, the development of “onion routing,” the principal function of Tor software, started in the 1990s with the intention to protect U.S. intelligence communications and saw its official launch in 2006 (Tindle, 2019, p. 64). The software is free for public use and it is defined as “a network of digital relays that allows users to browse the Internet anonymously” akin to an intricate game of leap frog (p. 64). We leave behind digital footprints, a digital representative of our movement, in the online world. This software gives individuals who use it the opportunity to keep their web searches and communication private, be free of most forms of surveillance, avoid censorship of information shared on the internet. Tor software hides the users information while they browse on the Internet, however, it does not mask the fact that the user is using Tor. When the user performs a search via this software, it adds numerous layers of encryption to the searcher's data and then sends the user's data through a series of digital relays that are randomly selected (p. 64). According to the Tor Project (n.d.), running their relay can aid in the network running “faster (and therefore more usable), more robust against attacks, more stable in case of outages, safer for users (spying on more relays is harder than on a few).”

The reason the software is called Tor is because the (onion) layers of encryption that are decoded through each relay in order to determine where to send the next layer of information (p. 64). As reported by the Tor Project (n.d.), there were 6,600 public relays in 2021 alone. Within the Tor circuit, there are three types of relays, the first being the guard relay, followed by the middle relay (has the ability to become a guard relay depending on its stability and speed), and ending with the exit relay where the

information is sent to its destination (Tor Project, n.d.). On one hand, there is no traceable data pertaining to the origin (the sender/user) and path the data has travelled through when it reaches the final relay (p. 64). On the other hand, the exit relay can be deemed as the most vulnerable relay as it is the most vulnerable to legal exposure meaning that the information leaving the relay can be intercepted, monitored, and susceptible to malware attacks. (Tor Project, n.d.). With its ability to provide its users with anonymity, any browsing activity and communications this software is then a suitable conduit for accessing the dark web. Jardine et al. (2020) introduce an interesting concept via their collection of statistical data regarding the distribution of illegal content and its intricate relationship with the political in the form of “free” countries and “not free” countries (p. 31716). The authors reported that their:

> …data also show that the distribution of potentially harmful and beneficial uses is uneven, clustering predominantly in politically free regimes. In particular, the average rate of likely malicious use of Tor in our data for countries coded by Freedom House as “not free” is just 4.8%. in countries coded as “free,” the percentage of users visiting Onion/Hidden Services as a proportion of total daily Tor use is nearly twice as much or ~7.8%. (p. 31716)

The data indicates that the utilization of Tor in first-world countries is significantly higher than those in the Global South. Simply put, Tor became a double-edged sword where the same anonymity is a shelter for those seeking to commit crimes both in the cyber world and reality.

The Dark Web

This part of the World Wide Web is stereotyped as the digital hub for criminal activity and interactions in popular fiction whether that may be books, television shows, or movies. It may come as a shock to the generic internet user that the dark web is easier to access than they thought and that not every piece of data solely contains dangerous and/or harmful information. There are many presumptions that it is an inaccessible space for the everyday internet user, however, Tor is one of the networks through which those browsing can enter the depths of the internet. An example of the commendable use of Tor is demonstrated by whistleblowers and/or people who do not want to disclose their identities when expressing opinions that may be dangerous if stated openly. Contrary to this, illegal activities include human trafficking, illicit drug trading, assassinations, terrorism, identity theft, unauthorized weapons dealing, etc. can all be located on the dark web via Tor (Tindle, 2019, p. 65).

Public Libraries and Tor

Protection, spying, national security, rule compliance, administration/social welfare, documentation, social control, entertainment (i.e., reality tv shows), etc. are all reasons for surveillance. In this case, electronic interface surveillance is quickly becoming an issue among the general population as they interact with various technological devices and their software. The library is a space that is dedicated to providing not only visual and audio material for loan, but also computer terminals, as a service to its patrons. Public libraries in particular tend to supply the population(s) they serve with these terminals for the purposes of creating documents, printing/scanning, completing tasks (school- or work-related), or just general browsing. Even though this

service is provided, patrons are restricted from various functions and sites while browsing and monitored while using these services. Depending on the funding allotted to a public library system like the Mississauga Library System, the library may offer Chromebooks as an option for patrons to leave the library space as a loan. With Tor software installed on library computers, the surveillance of patrons' usage to ensure that they abide by the library policies would plummet. In fact, when accessed, the software could be used to commit dangerous acts such as establishing and/or distributing illegal content within the library space without the library worker's knowledge. To add to this, there is also the issue of children and youth potentially accessing the dark web or being targets of those with ill intent due to the lack of digital literacy required to safely browse the internet using the software on computers at a terminal or in a computer lab.

Although Tor is free to install, there are two concerns that can be raised as they have the potential to be costly. The first is the requirements for the acquisition and installation of Tor relays. The computers terminals inhabiting the library space will need to have the ability to have at least "16 Mbit/s (Mbps) upload and download bandwidth" for Tor to run efficiently though Tor Project (n.d.) also asserts that more than the stated amount is preferable. Some service providers may only permit non-exit relays, guard or middle relays, meaning that acquiring the software may lead to the library needing to change its service provider which in itself is an expensive decision to make. To this end, the relay itself ranges in cost from anywhere to a few dollars to hundreds of dollars per month (Tor Project, n.d.). The second concern revolves around the educational aspect to using Tor and the dangers of the dark web, essentially teaching both staff and patrons alike how to make use of the software. As it is the public library space, the likely

route is to hold informational workshops whereby capable personnel external to the library are paid to facilitate informative sessions that they are knowledgeable in. These workshops would ideally discuss the lack of censorship while browsing that Tor gives a user, the typical do's and don'ts of the software, and how the library plans on managing the browsing activity of its patrons, e.g., patrons who violate the code of conduct and other policies the library has in place regarding the services they offer.

The Gap in Library Policy

Based on the ALA's Core Values and policy manual, there are numerous references to the advocation of privacy yet no policies and/or values that currently reflect the other side of the 'sword' that Tor presents to patrons—the involvement in illegal within the public library space. The Core Values lean towards assuring that users of various demographics are permitted and/or unrestricted, to a certain extent, while in the library space and using the services; there is no statement pointing towards exceptions regarding browsers such as Tor.

The gap here points out the lack of accountability in ALA's policy manual pertaining to browsers such as Tor and its functions as well as no references to the browser, and its connection to the dark web, concerning the following Core Values: Access, Confidentiality/Privacy, and Social Responsibility. For example, ALA's Core Values asserts that libraries have a social responsibility to solve "the critical problems of society; support for efforts to help inform and educate the people of the United States on these problems and to encourage them to examine the many views on and the facts regarding each problem" (American Library Association, 2020). As for Confidentiality/Privacy, section dictates the following concerning the library's role in

safeguarding the privacy of their patrons. Section B.2.1.17 Privacy (Old Number 53.1.16) of ALA's policy manual dictates that:

> In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf. Protecting user privacy and confidentiality is necessary for intellectual freedom and fundamental to the ethics and practice of librarianship. (American Library Association, 2022)

As displayed here, there is no specification of privacy as it interacts with the browsing services offered by services. This begs the question of how public libraries will respond to the implementation of Tor as their primary browser when there is no existing policy or legislation established by the ALA surrounding it. Writing policies that directly respond to the incorporation of the software will be time-consuming for Library and Information Science (LIS) professionals working in public libraries who are already deficient in time and resources based on the funding allotted to them. That being said, there are trace notions of censorship that can be seen due to the fact that this kind of software is not addressed straightforwardly.

Conclusion

When utilized with its initial purpose(s), the added privacy of browsing the internet and the anonymity of the user, Tor is advantageous in the public library where internet connectivity is particularly weak to harmful cyber attacks when not monitored.

Tor is not an emerging technology in the sense that it was recently created. It was discussed throughout this paper as emerging technology due to the software being a relatively new addition to library spaces. For instance, Toronto Public Library (TPL) offers the Tor browser on all of their Learning Centre computers across the city (Toronto Public Library, n.d.). TPL assert that public libraries carried the role of defenders of intellectual freedom and view Tor as the technological answer to mass surveillance technology guarding intellectual freedom (Toronto Public Library, n.d.). The library system also states that:

> Criminals already have many options better than Tor Browser for being anonymous online since they are willing to break the law….The current landscape is that criminals have good anonymity options online and law-abiding citizens do not: this is the worst of all possible worlds. (Toronto Public Library, n.d.)

While this may be correct, TPL would have then implemented this browser under the assumption that their patrons are all law-abiding citizens and not the very criminals that they mentioned. The library system's reasoning then lies with the presumption that the software does not commit the crime, the people do. This is faulty logic due to the fact that the library is unable to distinguish between law-abiding citizens and criminals, therefore, providing access to the tool that has the ability to create the harm is no different than being perpetuating the illegal acts that stem from the dark web. As Islam and Ozkaya (2019) have stated "The threat landscape is still growing with new black markets rising from the ashes of the ones taken down by legal enforcement agencies" (p. 25).

To conclude, I wanted to note that most of the funding for Tor originated from the U.S. government for the duration of the software's conception and inception into the digital landscape though they ceased their funding in 2012, a decade later (Islam & Ozkaya, 2019, p. 49). This factor is intriguing to bring forth as it highlights the U.S. government's crucial role in developing technology that bases itself in anonymity and privacy. This factor will not be discussed in this paper so as not to take away from its focus. On a final note, while it is not overall beneficial to have Tor implemented in public libraries, I will acknowledge that there are some benefits to incorporating this kind of technology into public library institutions.

Reflection

It was difficult to choose a topic for this project as there was so much that I wanted to discuss and found that narrowing down into a specific area brought forward many issues. Originally, this project started off as an essay that would have discussed the implementation of digital interfaces that interacted solely with patrons and printed books into the library space, specifically public libraries. The mode of delivery then shifted from essay writing to building a website that would have displayed a digital interface, FingerLink, that was selected, comparisons of the tool, along with comparisons to two other digital interfaces that featured similar functions. The website would have taken the form of a technology blog site built using Wix templates. Once I begun the process of searching for the appropriate site template, I became cognizant of the fact that I was not knowledgeable enough in the area of digital interfaces and their relationship with LIS studies to efficiently write about them and generate responses to the studies conducted on digital interfaces. This then led to a downward spiral of various ways I could approach this final assignment with ideas that were suitable as well as my comfortability writing about it. The decision to settle on discussing Tor as an emerging technology in libraries and its relationship with ALA's Core Values, despite its age, brought me right back to writing an essay mostly because of final exam season, but also because I think the ideas/arguments that I have written about would translate better in an essay format.

As to why I chose Tor, I wanted to learn more about the browser and how it functioned inside and outside of LIS spaces. The scholarly articles were mostly, interestingly enough, for the implementation of the browser in library spaces as it

enhances library patron's safety while browsing on the internet and provides them access to another part of the internet that is typically restricted to a select few. These articles also advocated for Tor as it grants the user with a higher level of privacy while browsing all while supposedly supporting intellectual freedom as libraries are positioned to do. I chose to argue against the implementation of the software simply because not enough is known about how it would impact the library space and its patrons. I argued within this viewpoint as I am of the opinion that Tor's intertwinement with the public library space without proper policies and control will inevitably introduce an onslaught of issues concerning the very factors the software aims to protect—privacy and security.

Most of the challenges I had with this paper centered on the limited sources arguing that Tor should stay out of the public library space. Articles tended to focus on Tor and its deep connections with the dark web, an element that I discussed, or Tor's potential to uplift intellectual freedom by opening new doors for access to more information. I would have preferred to provide more examples of the detrimental impacts of Tor as it is employed as the library's main browser, however, time constraints and other assignments prevented this research from occurring. Although I did mention the U.S. government's close relationship to the software in the conclusion as a passing thought, I would have also preferred to expand on this aspect a bit more.

References (APA)

American Library Association. (2022). *B.2 intellectual freedom (old number 53)*. About ALA. https://www.ala.org/aboutala/governance/policymanual/updatedpolicymanual/section2/53intellfreedom#B.2.1.17

American Library Association. (2020). *Core values of librarianship*. Advocacy, Legislation & Issues. https://www.ala.org/advocacy/intfreedom/corevalues

Islam, R. & Ozkaya, E. (2019). *Inside the dark web*. CRC Press/Taylor & Francis Group.

Jardine, E., Lindner, A. M., & Owenson, G. (2020). The potential harms of the Tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences of the United States of America*, *117*(50), 31716–31721. https://doi.org/10.1073/pnas.2011893117

Tindle, J. (2019). The Onion Router (TOR). *In Conflict in the 21st Century : The Impact of Cyber Warfare, Social Media, and Technology* (pp. 64–65).

Tor Project. (n.d.). *Tor Project: The Tor Network*. https://community.torproject.org/training/resources/tor-relay-workshop/#/0/4

Toronto Public Library. (n.d.). *Tor browser pilot*. https://www.torontopubliclibrary.ca/using-the-library/computer-services/tor-browser-pilot/#why