Is TOR Browser a Viable and Ethical Solution for Libraries?

Anna Arenas

University of South Florida

Is TOR Browser a Viable and Ethical Solution for Libraries?

In the past, advances in science and technology were considerably slower than they are today. Inevitably, the more we know, the more humanity is capable of keep researching. To this, we have to add the fact that, in this globalized world of ours, knowledge is shared at the pace of light thanks to the Internet. This is a marvelous situation, but as with everything, it has also another face. It is the dizzying speed at which intellectuals, legislators, and public in general should analyze, discuss, and argue ethical issues. In previous centuries, since the times of Plato, morals and ethics were discussed, even before any civilization had to deal -technically- with the issues in question. In a sense, morals came before science. Instead, our twenty-first century has to deal with ethical problems as they rise, since they weren't considered beforehand, simply because the factors and variables involved are so big and their appearances so fast, that understanding and evaluating the risks and benefits of any new technical advancement has to be done in parallel to the events per se, which not necessarily provides the most unbiased, balanced approach.

One of the most critical situations we have to deal as a society consists in the balancing of three main concepts that nowadays seem to be in conflict with each other, even though all of them constitute an integral part of America. Those are freedom, privacy, and security.

If there is something this modern world has taught us is that there is no such thing as total freedom, total privacy, or total security. We have to keep balancing. Continuously, we have to sacrifice one for the benefit of the other two. That sacrifice is also fluctuating, though. Depending on the circumstances, it has been necessary to switch between them. It becomes a

matter of priorities. Again, the main word here is balance. Here is where it resides the core of our society, the continual balancing act. In time, perhaps philosophers and intellectuals may find a coherent solution, but for the rest of us, we have to keep making decisions day in and day out on our current situations.

For a whistleblower, a press confidante, or a dissident under a dictatorship, privacy is crucial, more than that, it is vital. For individuals living under attack and victims of hate, security is indispensable. For people that want to live their lives in their own way, there is nothing more precious than freedom. Some of our values are now being played by circumstances which inherently can not provide a unique solution. That's why solutions can only be partial. The core of the matter hinges then, not on **which** decision, but on **how** and **when** we take any decision. What are the parameters, the expectations, and the risks.

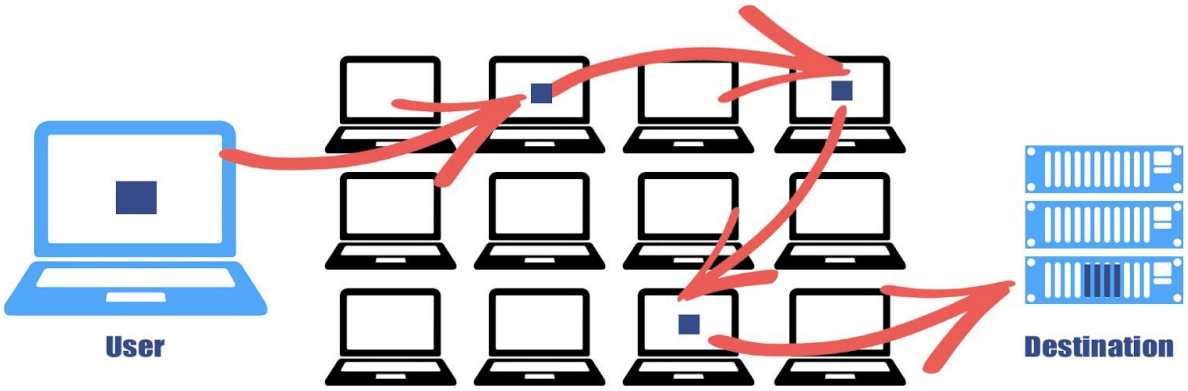
Since Ortega and Gasset wrote *The Rebellion of the Masses*, a lot has been said in regards to the importance of experts (or lack thereof). Nonetheless, the rise of the Internet has created a dangerous concept that, because everybody can talk (and post), all opinions carry the same weight. This can produce horrible mistakes and misguided decisions. It doesn't mean, however, that experts know all the answers, or that they haven't made mistakes in the past, but they have to be heard and their positions on topics should be taken seriously before making final decisions. They know more variables that the public at large. Critical decisions should be made with critical approaches **and** expertise. This is a pivotal point where librarians find themselves when they are considering the use of TOR browser in their institutions.

To talk about The Onion Router (TOR) it is important to understand certain terms. The way the web is currently visualized is by dividing it in three layers. The surface web, the

deep web, and the dark web. The surface web refers to what we commonly use. Those are the pages we visit through http, https, or other protocols. The pages are indexed by standard search engines (e.g. Google and Bing) and may reached by anyone. The deep web are pages that have been prevented to be indexed by search engines because they contain critical information. Here we find bank statements, court records, private companies' documents, or in the case of libraries, special collections that can be reached only by having login access. The content in the deep web may be inaccessible but it is locatable. By locatable, it means that it has an IP clearly assigned and identified, so it is clear where the resource is, even if the content can not be seen. It is traceable for law enforcement purposes. Finally, we have the dark web which was conceived to be accessible through anonymity using special software, being TOR browser the most common. Dark web means its resources not only are invisible for most people, but most importantly are not locatable. The latter means the IP address and the location of a particular resource is completely hidden. Additionally, by using TOR, the user accessing the resource is hidden as well.

In simple words, browsers like TOR used in the dark web work in special ways. A computer connecting to the web through TOR creates anonymity by creating a different mechanism to the currently used DNS routing. The traffic is not driven by known traceable servers but by computers in the same TOR network. In other words, the request for a web document generates a random path to get to the destination computer where the file requested lies.

Fig 1. Schematic of How TOR Browser Works



However, it is not only the random path that provides the anonymity or the fact that every connection, at every computer that forms part of the system, is encrypted (meaning the message can not be read if intercepted), it is mainly the fact that the headers (indicators of IP addresses for every computer) are visible only by the adjacent computer, not the one of the source or of the destination. This way, it appears that the traffic arriving to the destination came from the last computer, hiding completely the computer where the original request was sent.

Much has been written about “Big Brother” and the spying by government agencies on private citizens. Much has been discussed about the revocation of restrictions laws on ISPs to gather and sell customers behaviors on the web for marketing purposes. Much has been said by conspiracy theorists and libertarians about the future of the nation and the need to speak freely what they think about their political views. So much, that for the common person it is hard to make an informed decision. The comments about the risks to our liberties are so noisy and loud that people are migrating to TOR fearing that they are being watched by government

and private entities all the time. It is interesting to note that, even though libertarians insist on the freedom of speech as their argument for supporting TOR, the fact remains that, according to Guitton (2013), there is almost non-existing political discussion in the dark net. In reality, it is *not* being used, at least by Americans, to air political views. Our own open political system already allows it without the need to go underground. The real problem is, however, much more complicated. Opting for anonymity on the web is not a choice taken only by laymen, or perhaps dissidents living in oppressive nations. Anonymity is also the breeding ground for criminality because it minimizes accountability. TOR is being used, not only by people annoyed with ads and marketing. It is being used heavily by drug dealers, child pornographers, gun sellers, and terrorists. The fear of losing privacy is placing our society on a serious risk of terrorist attacks, which may manifest not only by bombs or shootings, but by cyber attacks that could cripple our most basic institutions.

When talking about the dark web and its main browser TOR, it is important to understand a couple of things. The first one, TOR can be used simply as a browser (the way Internet Explorer or Chrome works) with the advantage for the user that it hides the individual behind the computer. Used like that may seem innocuous. It means that customers can, for example, purchase something on the web and not keep seeing ads of the same product, or related ones, on their screen. It could also mean that the user is blocking NSA, for instance, to watch their browsing history. We have to remind ourselves, though, that just because the government has an infrastructure capable to do it doesn't mean it is really doing it all the time to everybody. It is about patterns, but let's not digress... Additionally, anonymity can mean that TOR users would be able to post anything, anywhere. In the past, anonymity has been the tool for the most

atrocious crimes. There is no reason to believe it won't continue to be. It has been reported that when we are not watched, our behaviours in some instances become outrageous and completely off-the-rails. Hate-speech and bullying flourish in the dark. Some supporters of TOR may say that it is their right, under the first amendment, to say what they think. Which is true, as long as it doesn't incite crime. However, that blurry line gets erased when there is no fear of prosecution because nobody knows who spoke such dangerous words.

The second aspect of TOR is that it allows the user to visit "hidden services". Those are specific web pages that sell any type of services, reportedly in vast majority illegal ones, varying from arms and drugs to child pornography. For obvious reasons, illegal enterprise prefers to live in the dark, hidden from law enforcement agencies. Though TOR users are a relatively small community, it is gaining popularity and this is a conversation that needs to be taken seriously by librarians.

Understanding what is a DNS, what is an IP, PGP, botnets, worms and trojan horses, how encryption works, http vs https pages, decentralized networks, DDoS attacks, password management, browser history, metadata of online activity, exit nodes, all these topics, and more, should already be mastered by librarians. If those are not completely understood, jumping into TOR could be not only irresponsible but dangerous, for both librarians and patrons. Installing TOR without proper understanding and intensively educating the public might lead to a false sense of security not only to marginalized communities, but to the public in general, with possibly grave consequences. Before installing TOR libraries should raise "awareness of cybersecurity issues" (West 2016, p.25)

As stated before, there is no such thing as complete privacy, anyways. Because illegal activity is being carried out in the dark web, law enforcement is continuously trying to track it down. It is not an easy task to track down these users, as a matter of fact it is extremely hard, but not impossible. The very nature of the web, as Pekala affirms "diminished the library's ability to control patron privacy" (Pekala 2017, p.48) In other words, even with TOR, libraries won't be able guarantee absolute privacy. As a token, we have to remind ourselves that Ross William Ulbricht, the owner of Silk Road, a website that black market vendors used to sell illicit products and services, and one of the big players in TOR, was captured and brought to justice. Ironically, he was captured at the Glen Park Branch Library in San Francisco. This is an idea for librarians to consider if they are thinking the possibility to use TOR in patrons' computers. TOR availability could also alter the demographics of the people visiting the library. Obviously, everybody has the right to use libraries, but librarians will have to take the necessary precautions to protect their patrons. Even if protecting users' privacy is an obligation for librarians, their safety is not, and should not be, second priority. TOR could possibly attract more criminals to the libraries putting in danger the rest of the library users.

Some may think that, because TOR can be used to browse the surface web in order to keep the user's anonymity, anything illegal in the dark web is not related with them. Nonetheless, the truth of the matter is that, because they are using TOR, users' computers are the relay of the content and purchases being done in the dark web. Under these circumstances, even though nobody is considered responsible, nobody is morally exempt. This is a serious ethical issue. When librarians decide to use TOR on their premises to guarantee privacy to their patrons, they have to understand also that they are, under their blind eyes, allowing criminal activity to

take place because the same computer that it is protecting a user's privacy right now while she is browsing the web, is the one that might be relaying the request for a killer to commit an assassination or a terrorist act, and there is no way of knowing when it happens. How can we expect to live in a reasonably safe world if we are willing to let criminals brew in the dark?

Additionally, it is important not to lose focus. Yes, libraries have an ethical obligation to provide privacy to their patrons, but it can not be at the expense of their own "*raison d'etre*". The main purpose of a library is to provide information. It is to help people find the content they are looking for. This is what freedom of information is all about. Artificial intelligence, the motor behind the most amazing advances in our times, is what lies behind any search on Google or any relevant search engine for that matter. It is a complex process to understand needs, lexicon, grammar, location, and history to offer the best solution possible. It is what allows users navigate an overwhelming ocean of information while being able to find what they are searching. When a user hides behind a browser like TOR to search in the surface web, it is denying the search engines to provide the most adequate results in an easy list. It is denying computational intelligence to offer the best possible relevant solutions. This is contrary to the idea of finding information. It clutters the results and it makes it more difficult to find what the user is looking for when browsing the Internet. In this scenario, the library is limiting, instead of helping the research on the web. It is, at its most basic, a contradiction to library functions. Additionally, is placing the library at a disadvantage place against Google. As if that wasn't enough, latency is an issue in the dark web, which means that patrons would also be losing speed to reach the content they are searching by hiding themselves.

Few years back, it was extensively studied and reported that the apparent anonymity of the surface web unleashed horrific situations, like bullying, abuse, and scams, simply because individuals thought they were invisible. Anonymity brings disinhibition and disinhibition is the first step to aggression. The perspective has changed and nowadays a different picture is being developed. As it was learned that anything in the surface web is traceable, two important reactions have occurred. One is running for hide, which explains the increase use of TOR bulletin boards related with racism, misogyny, and prejudiced comments posted in the dark web. The other route has been the radicalization of the conversations developed on the surface web since the majority of users tend to talk and relate with people similar to them, instead of learning from others. The result has been the creation of subcultures that in isolation tend to radicalise. In some instances, the Internet, instead of creating a global community embracing diversity, it has been the substrate for division and social tension. If libraries want to think themselves as the new community centers and offer the vastest possibilities of diversity, personal growth, equality, and creativity, they have to look for solutions to help people connect in better ways, not to divide. They have to provide expertise, mainly in information literacy. Libraries need to guide patrons on how to learn to discriminate news from opinion, relevant sources to fake ones, help recognize deception and distortion. The library as a community center should promote healthy, productive dialogues. It is imperative for libraries support patrons to be Internet savvy without sacrificing safety. In short, libraries should create connections not barriers, open doors instead of closing drapes.

Solutions are not easy. Then again, there are no unequivocal solutions. There are, though, educated ideas and prospects. Awareness, understanding, and above all expertise are the

keys. Issues related with privacy and security can not be solved by amateurs. They have to be done by experts. As stated above, it doesn't mean that experts can not be wrong, but at least, they manage and know more variables than the rest of us. They have to have the final word. It is imperative that librarians learn as much as they can about these issues before deciding about TOR or any similar browser. The dark net should not be taken lightly. Different libraries may find different solutions, but it has to be evaluated with care and it has to involve knowledgeable individuals in different areas, from law enforcement to civil rights defenders.

It is not possible to finish this paper without mentioning the Lebanon NH library. 2 years ago, librarians decided to install TOR in the patrons' computers, Homeland Security and the Police expressed their concern about the situation and the library agreed with officials by deciding to drop the idea. The community reacted and expressed its disappointment and the library went back again with their TOR original plan. This is precisely the type of problems that libraries should avoid. Just because the community cries in favor of something doesn't mean it is necessarily a good idea. Maybe yes, maybe not. It is not the majority, but the people who understand what is at stake who should be involved in the decision. Clear leadership and knowledge are crucial.

The dark net exists, it is there, and we need to know as much as we can about it. Libraries have an enormous responsibility of being on top of cyber issues to make informed decisions for the benefit of their patrons. In this new era, some may think that, by turning our heads or closing our eyes, we are not responsible for what we do not see, but in an ethical world, we should, or at least make an effort, to understand, be aware of, and prepare for the consequences of our decisions.

References

Bayle, E., Compoe, S., Ehrick, R., Hubbell, D., Lowe, B., & Ridge, J. (2017). Patron privacy: is the Tor Browser right for library use?. *Computers in Libraries,* (6). 10.

Berghel, H. (2017). Which is more dangerous-the dark web or the deep state?. *Computer*, (7), 86.

Bradbury, D. (2014). Unveiling the dark web. *Network Security,* (4), 14. doi:10.1016/S1353-4858(14)70042-X

Clemmitt, M. (2016). The Dark Web: Does identity-masking technology increase cybercrime?. *CQ Researcher*, 26(3), 49-72.

Everett, C. (2009). Feature: Moving across to the dark side. *Network Security,* 200910-12. doi:10.1016/S1353-4858(09)70099-6

(2015). Full Disclosure; The portal to the dark Web. *Star Tribune (Minneapolis, MN).*

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society,* 18(7), 1219. doi:10.1177/1461444814554900

Guitton, C. (2013). A review of the available content on Tor hidden services: The case against further development. *Computers In Human Behavior,* (6), 2805. doi:10.1016/j.chb.2013.07.031

Hurlburt, G. (2017). Shining light on the dark web. *Computer,* (4), 100.

Jardine, E. (2016). The Dark Web Dilemma. (cover story). *Australasian Science,* 37(5), 12.

Ling, Z., Luo, J., Yu, W., Fu, X., Jia, W., & Zhao, W. (2013). Protocol-level attacks against Tor. *Computer Networks,* 57869-886. doi:10.1016/j.comnet.2012.11.005

Macrina, A. (2015). The Tor browser and intellectual freedom in the digital age. Reference & User Services Quarterly, (4), 17.

Pekala, S. (2017). Privacy and User Experience in 21st Century Library Discovery. *Information Technology And Libraries*, (2), 48.

Romeo, A. D. (2016). Hidden threat: the dark web surrounding cyber security. *Northern Kentucky Law Review,* (1), 73.

Stevens, T. (2009). Regulating the 'Dark Web': How a Two-Fold Approach can Tackle Peer-to-Peer Radicalisation. *RUSI Journal: Royal United Services Institute For Defence Studies,* 154(2), 28. doi:10.1080/03071840902965687

West, J. (2016). Cybersecurity as an extension of privacy in libraries. *Computers in Libraries,* (5). 24.

Wolf, B. B. (2016). Decentral, unbreakable and anonymous?. *Ischannel,* 11(1), 24-29.