Colin Quinn

Professor Huggins

CS 300

29 August 2019

The History of Tor and its Uses

The Tor browser is one of the most renowned of its kind. The goal of Tor browser is to supply their users with free access to anonymity as technology continues to threaten individual privacy, according to their mission statement (“The Tor Project Elects…”). With its alpha release in 2002, Tor was first released to the public on August 13, 2004. Tor is very similar to Mozilla’s Firefox browser in looks, feel, and they share many features. The main code behind the Tor browser is almost directly based off of Firefox, but with some additional features that enable Tor to function the way it has been intended to do so. One of these features is the main draw of Tor, which is its anonymous browsing capabilities. This will be explained more later, but in addition to allowing the user to hide their trail through the network, they also offer Tor’s hidden sites as extra incentive to use their browser. It is the combination of these two additions that give the Tor browser and network that solidify its place as one of the better browsing options.

The Tor network functions quite similarly to the rest of the internet, with a few additions to make it stand out from the rest of the networks and browsers. Tor, which is short for “The Onion Router”, gets its name from the type of packet routing it performs. Onion routing works with layers of protection, much like an onion’s layers, in that once a request is made to a server, the request is then encrypted and sent through a handful of relays before arriving at the intended server. These relays each encrypt the packet before sending it off to the next relay, where it is encrypted again, and ultimately decrypted just before arriving to the server. Once at the server, the information requested is sent back to the user through the same process of layering encryption at each relay that the packet passes through, then is again decrypted at the user’s computer. This layering of encryption ensures that the only data available is the current location and next location while making sure that the other relay points do not know where entire path leads to. While Tor does not give true anonymity over networks, it keeps almost all vital information hidden behind layers of encryption. Mixing these layers with over a million users provides the network with enough traffic and encryption to make it very difficult to get a useful amount of information from.

Tor originally started in the mid 1990’s as a project through the United States’ government, more specifically for the Office of Naval Research and then the Defense Advanced Research Projects Agency. This project was originally assigned to Michael Reed and Paul Syverson, a computer scientist and mathematician respectively. Prior to the alpha release in 2002, computer scientist Roger Dingledine was added to the team working on Tor. Shortly after the public release in 2004, the financial support for development was shifted to the Electronic Frontier Foundation. As development continues, December 2006 marks the start of The Tor Project. This team of five people is ran by Dingledine and Syverson to develop and support Tor through the means of a research-based non-profit organization. In going to a non-profit model, Tor relies on a myriad of sponsors to remain functional, such as Google, Mozilla, National Science Foundations through University of Minnesota, Georgetown, and Rochester Institute of Technology, Fastly, Reddit, and still government agencies such as Defense Advanced Research Projects Agency as well as the U.S. Department of State Bureau of Democracy, Human Rights, and Labor (“The Tor Project: Privacy…”). Most of the financial support however comes from the government, while other parties tend to offer more research and idea-based support. In late 2015, Shari Steele joined The Tor Project after leading the Electronic Frontier Foundation for fifteen years, with the goal of making Tor a more widely accessible tool. Not long after sexual harassment allegations toward one of Tor’s developers, Jason Appelbaum were found to be true, not only did he step down from his position, but shortly after the entire board of directors at The Tor Project all step down and are replaced with the new executive director as Isabela Bagueros.

Since The Tor Project originally began as a government research topic, it is quite evident that they continue to not just fund the project, but also use the current state of it. While there are not many records of in which ways and where the government uses this type of technology, Roger Dingledine in 2004 goes on record stating that “They (the government) need these technologies so that they can research people they’re interested in, so that they can have anonymous tip lines, so that they can buy things from people without other countries figuring out what they are buying, how much they are buying and where it is going, that sort of thing” (Taylor). In order for the government to have such a reliable anonymity network however, they also rely on many individual’s network traffic to mask over their activity. In doing so, they accept that there will be many people that use this network for numerous reasons, some positive and many negative.

Some of the more positive uses of the Tor network is to those from countries that regulate their population’s internet traffic in order to censor information. This includes those who use Tor to gain accurate information around the Great Firewall of China or to avoid the censorship that North Korea puts upon their people. This also then extends to whistleblowers, which are people that contact media personnel with information or tips about something that is happening that they feel should be public knowledge but is being hidden. Some of the most recent and well-known examples of whistleblowers are Edward Snowden and Julian Assange. Snowden is known for leaking classified information he received while working for the National Security Agency. During an interview between Snowden and some of the staff on the Tor Project, Snowden explains that “Tor is a critical technology, not just in terms of privacy protection, but in defense of our publication right, our ability to route around censorship and ensure that when people speak their voices can be heard. The design of the Tor system is structured in such a s way that even if the US Government wanted to subvert it, it couldn’t because it’s a decentralized authority. It’s a volunteer based network” (Perry). Based on this quote, it seems rather evident that without the access to the Tor browser, Snowden would have most likely not felt safe enough to reveal the information he did. In addition to Snowden, Julian Assange, the man responsible for WikiLeaks which grew to fame around 2010 also used Tor to keep his identity hidden for a majority of his information leaks. While it can be debated that this information helps or harms a given situation, due to the nature of sensitive information, it does not negate Tor’s influence in opening the internet to new opportunities.

Tor is also closely associated to those who participate in the dark web due to its anonymity features. As a result of this, Tor is typically used by hacktivist groups, such as Anonymous. Anonymous is a worldwide group of hackers, also known as anons, that is very polarizing in their hacks that they organize. Some of their hacks are done as pranks that push their agenda of free and open information, such as in 2010 they performed Operation Smalltits. This distributed denial of service attack (DDoS) was in response to the Australian government supposedly censoring small-breasted women in pornography (“Timeline of Events…”). While most of their attacks are on more serious matters, like in 2013 they performed a hack on Nigeria’s national website shortly after their government passed a law-making homosexuality a crime punishable by fourteen years in prison (“Timeline of Events...”). This hacking group is very hidden and the only solid information that can be found is the things they release to the public such as their threats, but some mistakes are made by their group. Such as Brecht, who was only connected to Anonymous in 2014 due to him dropping a flash drive while committing another crime, where the flash drive had sensitive data about his DDoS attacks on Crelan banking services and assistance in targeting the 2014 FIFA World Cup. This hacktivist group is the highest profile among the general public, famous for their use of the Guy Fawkes Mask. Despite being rather high profile, it is very rare to arrest any of the members due to their skill and care with protecting their identities. Tor assists in this by giving them a network that also assists in hiding their identities while still having their voices heard by masses. Of course, this group takes it to the extreme and it is heavily debatable whether they are acting ethically or not in some cases, but without the access to Tor, their voices would not be heard at all.

As a result of easy access to anonymity thanks to Tor, internet black markets begin to form and start to thrive. The release of Tor in 2002, and the introduction of Bitcoin in 2008 allowed the Tor browser found its niche among the population. Unlike online payments through a bank, a Bitcoin transaction simply requires an amount of Bitcoin and an address to send it to. This enables the option for users to make it relatively anonymous by not requiring any personal information attached to their Bitcoin wallet and by changing the address after a transaction is completed. The combination of Tor’s hidden websites features and Bitcoin is what brought Ross Ulbricht’s Silk Road marketplace into the limelight. Prior to Ulbricht’s sentencing, he states in a document that “I created Silk Road because I thought the idea for the website itself had value, and that bringing Silk Road into being was the right thing to do. I believed at the time that people should have the right to buy and sell whatever they wanted so long as they weren’t hurting anyone else… Silk Road turned out to be a very naive and costly idea that I deeply Regret” (Ulbricht). Despite Ulbricht’s stated intentions, it does not negate the effects of his website. Silk Road acted as the go-to marketplace for many illegal items such as illicit drugs of any kind, and faulty driver’s licenses. This particular black market prohibited the sale of items that could harm anyone, such as stolen credit card information, guns or knives, and child pornography, although other markets were not so friendly in this regard. Silk Road was also used for the sale of legal items like clothes, jewelry, and books. At the time that Silk Road was shut down, the FBI estimates that “from February 6, 2011 to July 23, 2013 there were approximately 1,229,465 transactions completed on the site. The total revenue generated from these sales was 9,519,664 Bitcoins, and the total commissions collected by Silk Road from the sales amounted to 614,305 Bitcoins. These figures are equivalent to roughly $1.2 billion in revenue and $79.8 million in commissions” (“Silk Road (Marketplace)”). This marketplace’s success inspired others to follow like its immediate predecessor Silk Road 2.0 and later AlphaBay and Hansa. Advocates for these markets used the reasoning that it would be safer to buy these illicit products from home compared to having to physically meet the seller with cash, and this sentiment seemed to be true by the amount of traffic that these markets see. This reasoning does not excuse the acts of breaking the law however, and legal action is still taken when the situation requires it.

In the cases of someone being caught performing illegal actions through Tor, it is almost always the fault of the user, rather than the network. This however does not negate that one of the most common question for Tor users is why people would trust a product of the government to hide their personal information. When Michael Reed, one of the original team members was asked about this potential fault, his answer seems to satisfy those curious. Reed claims that they knew it would be an issue going into the project for government, as well as the repercussions of releasing their best technology for anonymity to the public, but it was all by design. He mentions that the main purpose for the project was to allow the government to anonymously gain intelligence or keep their paths hidden, and that the other uses of onion routing are merely side effects of them doing their job correctly (Smith). This interestingly makes all users of Tor more safe as traffic increases, as it can be described as if one of two people were doing something suspicious, it would stand out much more than if one out of ten-thousand people, making the network trails harder to trace for all users. The government was aware that civilians would use the anonymity produced by Tor for illegal things like the forming of the Silk Road, but it was the only way they would produce a product that achieves their goal of intelligence gathering (Smith). By creating more traffic through onion routing, the government can more effectively hide their investigations in the constant communications through the network. It is essentially never worth the effort to track down the average Tor user, and instead the only investigations held are the high-profile cases such as Silk Road or other government related hacks. This results in a safe environment for a large majority of users, while also giving enhanced protection to those who push the limits of their anonymity.

Tor’s very wide variety of users yields the users better results when it comes to anonymity. Since Tor is free to download and use, it is also heavily crowdsourced, in that many average people operate their own relays in order to give other Tor users a faster and better overall experience on the network. Allowing anyone to run these relays opens the question of whether or not they can see what comes in and out of their router, and in short, it is possible. In 2007, Dan Ergstad configured his local network to include five Tor exit relays, which is the layer that decrypts the packet to be configured back to the normal internet traffic rather than through the Tor network. In doing so, Ergstad gained access to numerous private email accounts, message threads, and usernames and passwords. His most notable information came from the embassies of Australia, Japan, Iran, India, and Russia, as well as the Dalai Lama’s liaison and Iranian Foreign Ministry (Stockley). Using this information, it is theorized by not only Snowden but also Ergstad that multiple governments run these sorts of spying exit relays in order to peek at what the network is transmitting. While this data is readable at these exit relays, the origin of the data is still unknown, so unless the information within the packet contains some sort of identity linking information then it is still anonymous but is far less hidden once passing through a spying exit relay. This means that the only information that can be intercepted from a Tor relay is the contents of the packet, which requires special care to keep from containing any sort of personally linking information. In order to keep this information safe from these man-in-the-middle style attacks, it is important to remind users that the Tor network still needs to send and receive information from the regular internet and to do so requires identifiable packets. So in short, Tor alone will not keep your login credentials or email safe, but it does add an extra layer of protection on top of practices that should already be in practice through the user such as not giving out passwords and making them complex enough to not be easily guessed.

Since a Tor relay can receive sensitive information, a controversial question is whether Tor is truly anonymous or not. In short, the answer is no, however it is much more complicated than that. A more accurate answer would be that it can be if proper precautions are taken. The Tor network does its job very well and is also very resilient to attacks on the network. In 2014, Carnegie Mellon’s Software Engineering Institute was able to tamper with Tor network traffic for a short period of time before being patched by the Tor Project team (Inc, Arma). It is then up to the users to put their best practices forward in order to maintain their anonymity online. For most users, Tor’s features along with general online safety practices are enough to keep them safe, while also implementing additional features for those who prefer more security. Within the Tor browser, there are presets for low, medium, and high security, where low mainly gives the benefits of the network, through high which fully disables JavaScript and disables showing certain image formats and fonts.

The Tor browser and network are very polarizing pieces of the internet. Some people cannot imagine a world without anonymous access to the internet, while others believe that everything should be censored or hidden accordingly. It is not easy to say which side is in the right as both have their merits, but the common theme of Tor is that information should be accessible by anyone and everyone that wants to find it. Tor is a product that has shown its effectiveness over many years through some of the best computer hackers, serving many governments and those who look to expose the governments, and even down to the average person that simply wants to keep themselves and their information online safe and protected. Tor addresses their goal of an ever-growing need for access to an unadulterated and unfiltered internet. It takes an old concept and continues to release new ideas upon improving their ideal version of the internet. While Tor is almost synonymous with the dark web in some people’s views, many positives come out of the network that are less heard of. The Electronic Frontier Foundation’s Eva Galperin stated in 2014 that “Tor’s biggest problem is the press. No one hears about that time someone wasn’t stalked by their abuser. They hear how somebody got away with downloading child porn” (Harris). It is always possible that someone with malicious intent will find a way to act maliciously, and while Tor does enable those acts, it also enables others to be more safe than they would be otherwise.

Works Cited

Brown, Jennings. “Anonymous Hacker Sentenced After Dropping USB While Throwing Molotov Cocktail.” *Gizmodo*, Gizmodo, 24 June 2019, gizmodo.com/anonymous-hacker-sentenced-after-dropping-usb-while-thr-1835810645.

Chandler, Nathan. “How Anonymous Works.” *HowStuffWorks*, HowStuffWorks, 12 Mar. 2013, computer.howstuffworks.com/anonymous.htm.

Harris, Shane, and John Hudson. “Not Even the NSA Can Crack the State Dept's Favorite Anonymous Network.” Foreign Policy, Foreign Policy, 4 Oct. 2013, foreignpolicy.com/2013/10/04/not-even-the-nsa-can-crack-the-state-depts-favorite-anonymous-network/.

Inc, Arma. “Tor.” Tor Project: FAQ, 24 Feb. 2016, 2019.www.torproject.org/docs/faq.html.en.

Inc. “Tor.” *Tor Project: FAQ*, 2019.www.torproject.org/docs/faq.html.en.

Perry, Mike. “This Is What a Tor Supporter Looks Like: Edward Snowden.” *Tor Blog*, 30 Dec. 2015, blog.torproject.org/what-tor-supporter-looks-edward-snowden.

“Silk Road (Marketplace).” Wikipedia, Wikimedia Foundation, 2 Aug. 2019, en.wikipedia.org/wiki/Silk\_Road\_(marketplace)#Products.

Smith. “No Conspiracy Theory Needed: Tor Created for U.S. Gov't Spying.” *CSO Online*, CSO, 28 Mar. 2011, [www.csoonline.com/article/2228873/no-conspiracy-theory-needed-tor-created-for-u-s-gov-t-spying.html](http://www.csoonline.com/article/2228873/no-conspiracy-theory-needed-tor-created-for-u-s-gov-t-spying.html).

Stockley, Mark. “Can You Trust Tor's Exit Nodes?” Naked Security, 26 June 2015, nakedsecurity.sophos.com/2015/06/25/can-you-trust-tors-exit-nodes/.

Taylor, Sven. “Tor Browser - What You Really Need to Know (Read This First).” *Restore Privacy*, 4 July 2019, restoreprivacy.com/tor/.

“Timeline of Events Associated with Anonymous.” *Wikipedia*, Wikimedia Foundation, 18 July 2019, en.wikipedia.org/wiki/Timeline\_of\_events\_associated\_with\_Anonymous.

“The Tor Project Elects New Board of Directors.” *Tor Blog*, 13 July 2016, blog.torproject.org/tor-project-elects-new-board-directors.

“The Tor Project: Privacy & Freedom Online.” Torproject.org, [www.torproject.org/about/](http://www.torproject.org/about/).

Ulbricht, Ross. Letter to Judge Forrest. 22 May 2015, freeross.org/wp-content/uploads/2015/05/Ross\_Letter\_to\_Judge\_05-22-2015.pdf#page=2.