OPEN ACCESS
Freely Available Online

JOURNAL OF ADVANCED FORENSIC SCIENCES

ISSN NO: 2692-5915

Review

DOI: 10.14302/issn.2692-5915.jafs-20-3366

Is the Onion Router a Secure Network?

Donald L. Buresh, Ph.D., J.D.[1,*]

[1]Touro University Worldwide

Abstract

This paper attempts to answer the question of how government agencies use The Onion Router, or Tor, in conducting investigations. The essay observes that Tor is free open-source software that can be used by anyone who desires to communicate with others in a secure manner. In surveying the literature, it is found that Tor can be employed for both legal and illegal purposes. As the major financial contributor, Tor is used by government to secure its communications. Because Tor by bad actors, and because many of the Tor relays are operated by government agencies, Tor has been successfully employed in catching unsuspecting criminals. The conclusion of this exposition is that if one wants to communicate securely with someone else, and not be visible to government agencies, Tor should not be the vehicle of choice. There are alternative modes of communication that can thwart the risk of government surveillance.

Corresponding author: Donald L. Buresh, Ph.D., J.D., 3115 Enoch Avenue, Zion, Illinois 60099 Telephone: 847-872-1659.

Keywords: GCHQ, NSA, The Onion Router, TOR

Received: May 06, 2020 **Accepted:** Jun 05, 2020 **Published:** Jun 05, 2020

Editor: Dipanwita Thakur, Banasthali University, Banasthali, Rajasthan, India

The Onion Router, or Tor as it is more commonly known, is free software that supports anonymous communication on the Internet.[1] Tor guides Internet traffic through a global network that is both free and administered by volunteers.[2] It consists of over seven thousand relays that hide an individual's whereabouts and usage from others that are attempting to analyze the flow of data on the Internet.[3] By employing Tor, it may be difficult, and sometimes impossible, to associate Internet activity with a particular person, including when one displays a specific website, posts a message online, sends an email message, etc.[4] Tor does not preclude an online service provider from figuring out when one is employing Tor to access the facility, and it does not disguise itself so that an Internet service provider does not know when a person is using Tor.[5] Some websites limit the ability of a user to use the full capability of a site.[6]

Onion routing is accomplished by creating by encrypting the data in the application layer of its communication protocol.[7] When processing a packet using onion routing, it is as if the Internet communication protocol is peeling the layers of an onion.[8] Tor not only encrypts the data but also the IP address of the next destination node.[9] This encryption is accomplished many times, where each relay or server in the Tor network decrypts the outermost layer so that it can send the remaining encrypted packet along to the next relay.[10] When a packet arrives at the relay just before the destination, the final encrypted layer is decoded, and the packet is sent to its destination.[11] The advantage of employing the onion methodology is that network surveillance cannot trace a packet backward to its source.[12] In the past, the National Security Agency ("NSA") attempted to de-anonymize a user using its XKeyscore ("XKS") system (codenamed "EgotisticalGiraffe"), where an email message, a telephone call, or web traffic can be monitored anywhere in the world without first obtaining a warrant.[13] A variety of organizations have funded Tor, but the majority of the monies originates from the United States federal government via the Office of Naval Research ("ONR") and the Defense Advanced Research Projects Agency ("DARPA").[14]

The purpose of this paper is to briefly review its history, describe how it works, discuss how it is currently employed, and then highlight its strengths and weaknesses in an attempt to answer how Tor is used by government agencies in conducting investigations. Tor seems to be a viable alternative to the Internet in its current form for individuals and organization, legal or otherwise, that desire to remain anonymous.[15] The advertised primary advantage of Tor is that personal anonymity is preserved while providing users with an efficient and effective alternative to the current state of Internet surveillance.[16]

A Review of Tor

This section reviews the historical literature of how Tor evolved into its current state. The literature seems to indicate that Tor has been billed as a secure network, where users can safely send and receive messages anonymously. However, the research demonstrates that Tor is anything but safe. Individuals that blithely employ Tor for legal or illegal purposes do so at their own risk. The section observes that there are some legitimate uses for Tor, but the fact that Tor is government funded and that the NSA and the GCHQ run many of the relays establishes the existence of a significant flaw its implementation.

The History of Tor

The principle of onion routing was created by the United States Naval Research Laboratory ("USNRL") on May 31, 1996, at the first Information Hiding Workshop held in Cambridge, UK.[17] Tor was invented Paul F. Syverson a mathematician, and by Michael G. Reed and David M. Goldschlag, both computer scientists.[18] The first generation of the open source code was made available in July 1996.[19] Although several proofs of concept models were developed, in 2002 the alpha version of Tor was produced by Syverson along with Roger Dingledine and Nick Mathewson, again both computer scientists.[20] The project was affectionately known as the Tor Project.[21] In 2004, the USNRL freely released the source code of Tor.[22] Also in 2004, the Electronic Frontier Foundation ("EFF") started funding Dingledine and Mathewson to ensure the survival of the project. [23]

In December 2006, Dingledine, Mathewson, and a host of others officially founded The Tor Project, a 501

(c)(3) organization located in Massachusetts.[24] The project itself is a research-oriented nonprofit organization that not only supports Tor, but also develops additional functionality to further ensure user anonymity.[25] The EEF was the first sponsor of the Tor Project, but funding has also come from such organizations as the National Science Foundation ("NSF"), US Department of State Bureau of Democracy, Human Rights, and Labor ("DSBD"), DARPA through the University of Pennsylvania, Google, the SRI International, etc. (Sponsors, n.d.).[26] After 2006, the United States government has been the major funding source for Tor.[27]

In 2013, the NSA discovered how to penetrate the Tor network, unmasking its users.[28] The Washington Post published the notes of the meeting in 2007 between Dingledine and the NSA.[29] In these notes it was revealed that Dingledine not only described to the NSA how Tor worked, but also disclosed the categories of users that employ Tor or a regular basis.[30] In 2011, the Tor staff admitted that Tor was not as safe as it had been advertised.[31] Mike Perry, a Tor developer admitted that "[e]xtremely well funded adversaries that are able to observe large portions of the Internet can probably break aspects of Tor and may be able to deanonymize users."[32] One year later, Syverson confirmed Perry's assertion when he stated that Tor is insecure against an adversary that can analyze correlated traffic at different relays by exploiting traffic patterns, thereby subverting Tor security.[33]

Although Tor has been advertised as a secure network that preserves anonymity, the future of Tor is uncertain. If it becomes generally known that Tor is insecure, its usefulness diminishes rapidly. The question that the Tor Project must answer is what additional security measures can be effectively implemented in the future, particularly because Edward Snowden recently revealed that the NSA and the British Government Communications Headquarters ("GCHQ") run a substantial number of Tor relays and desire to run even more relays.[34]

How Tor is used

Tor permits its users to access the Internet as well as chat and send messages, just like many other Internet applications. However, has been used in the past for a variety of legal and illegal purposes, including gambling pornography, hacking, counterfeiting, whistleblowing, fraud, and selling illicit drugs.[35] The Economist has labeled Tor "a dark corner of the web" because of its relationship with Bitcoin and Silk Road.[36] Even so, Tor has been targeted by the NSA and the GCHQ, although these actions appear to be either software quality assurance efforts or a desire to track illegal Tor usage.[37] For example, GCHQ used a tool called Shadowcat to monitor encrypted access to virtual private servers ("VPS") over secure shells ("SSH") using Tor to capture illegal activity.[38] Other illegal uses of Tor include selling controlled drugs, weapons, stolen credit card numbers, money laundering, identity theft, and exchanging counterfeit currency.[39]

In the complaint regarding United States v. Ross William Ulbricht, the federal government admitted in court that Tor could be employed legitimately even though the document listed a plethora of illegal usages.[40] Even so, Tor is increasingly used by domestic violence victims and their social workers to communicate anonymously.[41] One legal advantage of using Tor is that it prevents stalking by private actors, but according to the information above, Tor in no way assures anonymity from government actors.[42] Nonetheless, Tor has been legally employed by The Guardian, The New Yorker, ProPublica, The Intercept_, etc.[43]

Discussion of Tor's Weaknesses

From a naïve technological perspective, Tor seems to be an impenetrable network. Onion routing is attained by encrypting data in the application layer, and then when processing a packet, a relay peels off one layer of the encryption, sending the packet onto the next relay until a packet reaches its destination.[44] The reality of the situation is something entirely different. Tor is freely available to anyone who wants to use it, the majority of the funding for Tor comes from the federal government, and the NSA and GCHQ operate many of the relays in the network.[45] However, for all of the assurances by the Tor Project that employing the software enables Internet communications to be secure, the fact is that many of the Tor relays are owned and operated by the federal government.[46] This fact begs the question of whether Tor is as secure as its advertising purports it to be. After all, Perry and Syverson have

publically admitted that Tor is susceptible to surveillance when an adversary can monitor large portions of its network.[47] What better organization is there to scrutinize Internet traffic than the federal government with their virtually unlimited budget?[48] The answer is that the federal government is the best candidate to engage in extensive Internet surveillance.

A question that remains to be answered is: Why would the federal government fund Tor development in the first place? Two responses are readily apparent. First, federal agencies such as the NSA and its British counterpart the GCHQ need a secure network where they can communicate with individuals both in the field and at headquarters.[49] Almost as a corollary, Tor has value to the NSA and the GCHQ because it is advertised as providing secure communication, and private individuals who have something to hide are more than likely to use Tor for legal or illegal purposes.[50] In advertising that Tor is a secure network, it is as if there is a big red flashing neon arrow pointing at Tor attempting to discourage private individuals from using the network, while at the same time, individuals ignore the flashing indicator because the advertising is so enticing and hypnotic. These people forget or are unaware that the federal government developed Tor, and that the government is interested in its communications, but not necessarily the interactions of its citizenry.

It is well established that Tor is employed for legal and illegal purposes, such as selling controlled drugs, weapons, stolen credit card numbers, money laundering, identity theft, and exchanging counterfeit currency.[51] From a common sense perspective, the surveillance of illegal actives on the Tor network could be construed to be entrapment.[52] However, when dealing with entrapment, it is not an affirmative defense if an individual has a predisposition to commit a crime.[53] If a person is employing Tor for illegal purposes, then it is legally impossible to invoke entrapment as a defense because the person has the appropriate mental state or mens rea to commit the particular crimes. [54] Thus, the secondary purpose of Tor can be stated in the vernacular to be to catch the bad guys.

One problem with Tor that can defeat secret government communications is when adversaries such as the China and Russia governments covertly own and operate Tor relays. Both countries are adamantly against private citizens operating Tor relays, sometimes prosecuting its citizens on charges of terrorism.[55,56] Even so, a more critical is issue occurs when foreign governments, whether or not the governments are American allies, use Tor relays to spy on U.S. government activities.[57] Given that this negative consequence can be effectively mitigated, Tor has many economic, legal, and political advantages and few disadvantages.

Conclusions

In conclusion, if this author were to suggest to a third party whether to use Tor, the recommendation would be negative. Although Tor seems to be a mechanism for secure communication, first looks are deceiving. The federal government has too much influence in the use and results of Tor for the simple reason that it is its primary funding source. The adage at play here is that the person who pays the piper calls the tune. The paper followed the money that funded The Tor Project and discovered that the major contributor was the federal government. The government is not necessarily interested in altruistically protecting the privacy of individuals. It pursues its interests. Thus, if the Tor Project puffing transfixes a person, one uses the network at one's own risk. In the opinion of this author, it is just not worth the risk. There are alternative forms of communication that do not employ the Internet and are probably much safer, such as Federal Express. Why expose oneself to government surveillance when it is not necessary? It should always be remembered that not all that glitters is gold.

References

1. Tor, *Tor Project*, n.d., https://www.torproject.org.
2. Id.
3. Tor Network Status, *Tor Status*, n.d., http://torstatus.blutmagie.de.
4. P. Kingsley, Turks click away, but Wikipedia is gone, *The New York Times*, June 17, 2017, https://www.nytimes.com/2017/06/10/world/europe/turkey-wikipedia-ban-recep-tayyip-erdogan.html.
5. Id.
6. Id.
7. R. TERMANINI, THE NANO AGE OF DIGITAL IMMUNITY

INFRASTRUCTURE FUNDAMENTALS AND APPLICATIONS: THE INTELLIGENT CYBER SHIELD FOR SMART CITIES (CRC Press March 05, 2018).
8. Id.
9. Overview, *Tor Project*, n.d., https://www.torproject.org/about/overview.html.en.
10. Id.
11. Id.
12. Id.
13. Peeling back the layers of Tor with Egotistical Giraffe, *The Guardia*, October 04, 2013, https://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.
14. Y. Levine, Almost everyone involved in developing Tor was (or is) funded by the US government, *Pando*, July 16, 2014, https://pando.com/2014/07/16/tor-spooks/.
15. See supra, note 9.
16. Id.
17. P. F. Syverson, Brief selected history, *Onion Routing*, n.d., https://www.onion-router.net/History.html.
18. P. F. Syverson, M. G. Reed, & D. M. Goldschlag, Hiding routing information, *International Workshop on Information Hiding*, 1996, https://link.springer.com/chapter/10.1007/3-540-61996-8_37.
19. See supra, note 17.
20. R. Dingledine, N. Mathewson, & P. Syverson, Tor: The second-generation onion router, *Proceedings of the 13th USENIX Security Symposium*, 2004, https://www.usenix.org/legacy/events/sec04/tech/dingledine.html.
21. Id.
22. See supra, note 14.
23. See supra, note 20.
24. Core People, *Tor Project*, n.d., https://www.torproject.org/about/corepeople.
25. Id.
26. Sponsors, *Tor Project*, n.d., https://www.torproject.org/about/sponsors.html.en.
27. See supra, note 14.
28. B. Gellman, C. Timberg, & S. Rich, Secret NSA documents show campaign against Tor encrypted network, *The Washington Post*, October 04, 2013, https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html.
29. Id.
30. See supra, note 14.
31. Id.
32. M. Perry, Iran cracks down on web dissident technology, *Tor-Talk*, March 22, 2011, https://lists.torproject.org/pipermail/tor-talk/2011-March/019898.html.
33. See supra, note 14.
34. Phobos, On being targeted by the NSA, *Tor Blog*, July 03, 2014, https://blog.torproject.org/being-targeted-nsa?page=4.
35. D. Lawrence, The inside story of tor, the best internet anonymity tool the government ever built, *Bloomberg BusinessWeek*, January 23, 2014, https://www.bloomberg.com/news/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency.
36. Monetarists Anonymous, *The Economist*, September 29, 2012, https://www.economist.com/finance-and-economics/2012/09/29/monetarists-anonymous.
37. J. Ball, B. Schneier, & G. Greenwald, NSA and GCHQ target Tor network that protects anonymity of web users, *The Guardian*, October 04, 2013, https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.
38. JTRIG Tools and Techniques, *The Intercept*, July 14, 2014, https://theintercept.com/document/2014/07/14/jtrig-tools-techniques/.
39. J-M. Bond, How to buy drugs (or anything else) on the deep web, *The Daily Dot*, January 16, 2017, https://www.dailydot.com/layer8/how-to-buy-drugs-deep-web/.
40. See *United States v. Ross William Ulbricht*, 13 MAG 2328 (S. Dist. N.Y. 2013), https://web.archive.org/web/20131002221530/http://ww1.icsi.berkeley.edu~nweaver/UlbrichtCriminalComplaint.pdf.
41. J. Teveten, Where domestic violence and cybersecurity intersect, *Rewire News*, April 12, 2017, https://rewire.news/article/2017/04/12/domestic-violence-cybersecurity-intersect/.
42. G. LeVines, As domestic abuse goes digital, shelters turn to counter-surveillance with Tor, *The Boston Globe*, May 07, 2014, http://www.betaboston.com/

news/2014/05/07/as-domestic-abuse-goes-digital-shelters-turn-to-counter-surveillance-with-tor/.
43. J. Ellis, The Guardian introduces SecureDrop for document leaks, *Nieman Lab*, June 05, 2014, http://www.niemanlab.org/2014/06/the-guardian-introduces-securedrop-for-document-leaks/ http://www.niemanlab.org/2014/06/the-guardian-introduces-securedrop-for-document-leaks/.
44. See supra, note 13.
45. See supra, note 1; see supra, note 14; and see supra note 34.
46. See supra, note 14.
47. See supra, note 32 and see supra note 14.
48. See supra, note 14.
49. T. Lee, Everything you need to know about the NSA and Tor in one FAQ, *The Washington Post*, October 04, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.
50. See supra, note 35.
51. See supra, note 39.
52. W. R. LAFAVE, MODERN CRIMINAL LAW: CASES, COMMENTS, AND QUESTIONS 4th ed. (Thompson/West Publishing 2001).
53. Id.
54. Id.
55. P. Winter, & S. Lindskog, How the Great Firewall of China is Blocking Tor, *UseNix*, n.d., https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf.
56. T. Hatmaker, Tor node operator arrested in Russia will be held on terrorism charges until June trial, *Tech Crunch*, 2017, https://techcrunch.com/2017/04/24/dmitry-bogatov-tor-russia/.
57. K. Poulsen, Russian spy nodes caught snooping on Facebook users, *Wired*, January 21, 2014, https://www.wired.com/2014/01/russia-tor-attack/.