Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law

Tomáš Minárik, Anna-Maria Osula *

NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Keywords:
Tor
Anonymity
Human rights
Privacy
Freedom of expression
Content liability
Criminal investigation
Evidence
Personal data
Tor exit node

A B S T R A C T

Tor is one of the most popular technical means of anonymising one's identity and location online. While it has been around for more than a decade, it is only in recent years that Tor has begun appearing in mainstream media and openly catching the attention of governments and private citizens alike. The conflicting interests related to the use and abuse of Tor also raise a number of legal issues that are yet to be analysed in depth in academic literature. This article focuses on a number of relevant legal issues pertaining to Tor and reflects our initial legal comments, while noting that all of the identified legal questions merit further research.

After introducing the technical side of Tor and the attitudes of governments towards it, we (1) explore the human rights connotations of the anonymity provided by Tor, coming to the conclusion that this anonymity is an integral part of certain human rights, particularly the right to privacy and the right to freedom of expression. Government activities with respect to Tor should thus not be unlimited. In relation to this, we (2) provide a closer look at the problem of content liability of the Tor exit node operators. Finally, we (3) point out several legal problems in conducting criminal investigations with the need to obtain the evidence from the Tor network.

We conduct this legal analysis in the context of international and European law, paying a particular attention to the case law of the European Court of Human Rights and the Court of Justice of the European Union.

1. Introduction

Tor is one of the most popular technical means of anonymising one's identity and location online. It is one of several options available to defend against traffic analysis that 'threatens personal freedom and privacy, confidential business activities and relationships, and state security'.[1]

Such anonymity is desirable for actors with different motivations. For example, in July 2013, the FBI took control of Freedom Hosting servers, a provider of 'Tor hidden service' sites that were a major source of child pornography. The FBI replaced the original Freedom Hosting sites with pages that sent an error message containing malicious code. This code was then used to locate the sites' visitors.[2]

A similar fate befell Silk Road, a Tor hidden service marketplace for illegal drugs, prohibited weapons, and even for

* *Corresponding authors*. NATO CCD COE Law & Policy, Branch, Filtri tee 12, Tallinn 10132, Estonia.
E-mail addresses: anna-maria.osula@ccdcoe.org (A.-M. Osula); tomas.minarik@ccdcoe.org (T. Minárik).

[1] 'Tor Project' <https://www.torproject.org/>. An alternative to Tor is e.g. 'The Invisible Internet Project', <https://geti2p.net/en/>.

[2] Kevin Poulsen, 'FBI Admits It Controlled Tor Servers behind Mass Malware Attack', <http://www.wired.com/2013/09/freedom-hosting-fbi/>.

http://dx.doi.org/10.1016/j.clsr.2015.12.002

hiring assassins.[3] Despite shutting down the site in October 2013, only a month later, Silk Road 2.0 was online, along with a multitude of other marketplaces.[4] Hours after Silk Road 2.0 was seized in November 2014, Silk Road 3.0 was up and running.[5]

At the same time, Tor is viewed by prominent human rights advocate groups as an important tool in bypassing censorship and protecting privacy.[6] This dual use of Tor poses challenges for policy-makers. Governments are interested in enforcing law and providing citizens with security, while citizens are interested in the free flow of information and respect for privacy. As one commentator has put it, 'sympathising with the challenges of law enforcement, after all, has never required us to forgo access to any instrument that can be used by bad actors. Should we have banned pagers, cell phones, or laptop computers in light of their utility to drug lords?'[7] These conflicting interests also bring along a number of legal challenges that have not yet been analysed in great depth in the academic literature.

Our article is a modest attempt at filling this gap.[8] We have selected a number of relevant legal issues related to Tor and offer our initial legal comments, while noting that all of the identified legal questions merit further research. First, we introduce Tor and the varying approaches of different governments. We then turn to human rights and contend that anonymity is an integral part of certain human rights, and that governments adhering to the idea of human rights should not ban or suppress Tor or other anonymity networks on the basis of expediency for security and law enforcement.

Second, we look at the issue of content liability of Tor exit node operators as a particular example of the limits of anonymity.

Third, we show the principal legal challenges in law enforcement's use of Tor, such as collecting evidence and monitoring Tor traffic as an exit node operator.

Our analysis has been conducted in the context of EU and international law, with a particular focus on the case law of the European Court of Human Rights and the Court of Justice of the European Union.

2. What is Tor?

Tor is free software that allows its users to conceal their location and browsing habits by redirecting their traffic through a distributed network (the 'Tor network'[9]) of relays acting as proxy servers[10] provided by volunteers (also known as node operators). Due to its ability to protect against a common form of Internet surveillance known as 'traffic analysis', Tor is popular among a variety of people and groups[11] and boasts over 2 million users daily.[12] It is used by individuals who wish to avoid websites tracking them, or to connect to websites that may otherwise be blocked by their local Internet providers; by journalists or anyone who needs to secure their communication or bypass censorship; by organisations which want to safeguard their members' privacy or to maintain civil liberties online; and by government entities such as the military and law enforcement.[13] In addition to re-directing traffic, Tor also offers its users 'hidden services' which allow websites to be published and other services to be offered without needing to reveal the location of the site.[14]

How does Tor work? Let us imagine that Alice wants to connect to a webpage on Bob's server, but that site is forbidden in the country where she is located. Moreover, Alice does not know whether Bob's server has been compromised by an adversary who collects the IP addresses of the users.

Alice can use Tor to connect to Bob's server. Tor downloads a list of nodes available in the Tor network, and it randomly selects three of these nodes (entry, relay and exit). It encrypts Alice's HTTP request in three layers of encryption and then sends it to the entry node. The entry node establishes a connection with Alice, exchanges keys with her, decrypts the first layer of the request, and establishes a connection with the relay node. The same process is repeated recursively at the relay node and the HTTP request reaches the exit node. The exit node similarly decrypts the last layer and sends the HTTP request to the destination, Bob's server. The reply from Bob follows the same path in reverse. Each node only knows about the immediate nodes to which it connects and so the decrypted HTTP request and Alice's IP address will never be available at the same node. Consequently, in order for anyone to prove that it was Alice who made that particular HTTP request, this person would have to be in control of each of the three nodes selected at random. In reality, due to the distributed nature of the Tor network, being in charge of all three nodes would be very unlikely.

---

[3] Andy Greenberg, 'End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Black Market', <http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/>.

[4] Graham Templeton, 'The Silk Road 2.0 is Now Bigger and Better than Ever Before: What's the FBI to Do?', <http://www.extremetech.com/extreme/182083-the-silk-road-2-0-is-now-bigger-and-better-than-ever-before-whats-the-fbi-to-do>.

[5] James Cook, 'There's Already a Silk Road 3.0', <http://www.businessinsider.com/theres-already-a-silk-road-30-2014-11>.

[6] For example, the Electronic Frontier Foundation, <https://www.eff.org/torchallenge/>; see also the list of sponsors of the Tor Project: <https://www.torproject.org/about/sponsors.html.en>.

[7] Craig A Newman, 'After the Silk Road Conviction, Tor Must Be Protected', *The Guardian* (19 February 2015), <http://www.theguardian.com/media-network/2015/feb/19/after-the-silk-road-conviction-tor-must-be-protected>.

[8] This article is an expanded and updated version of our contribution to Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula, 'Technical and Legal Overview of the Tor Anonymity Network', NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015, <https://ccdcoe.org/multimedia/technical-and-legal-overview-tor-anonymity-network.html>.

[9] Where it is clear from the context, the term 'Tor' is used interchangeably for the terms 'Tor software' and the 'Tor network' throughout this article.

[10] 'Tor Metrics – Relays and Bridges in the Network' (*Tor Project*), <https://metrics.torproject.org/networksize.html>.

[11] 'Tor: Overview', <https://www.torproject.org/about/overview>.

[12] 'Tor Metrics – Direct users by country', <https://metrics.torproject.org/userstats-relay-country.html>.

[13] 'Tor: Overview' (n 11).

[14] ibid.