

# On the liability of TOR Exit Relay operators

Alessio Trivisonno

University of Trento

**Abstract.** Tor is a network providing anonymous access to the Internet to users all over the world. It relies on the efforts of volunteers who share their personal internet access point with other users of the network. This service is extremely valuable in countries where the censorship is much stronger but it is sometime used for bad purposes. Many where the abuses of the Tor network to commit cyber-crimes or to visit websites hosting child pornography or drug selling platforms. The Tor Exit Relays operators are the ones that put themselves in the higher risk of being held accountable for committing such crimes because of the technological architecture of Tor. The purpose of this paper is to investigate on the problem of the legal liability of Tor Exit Relays operators in case of law infringement. We will compare the role of these people with the figure of the Internet Service Providers and we will see if the shields that ISP benefit are still valid in the context of Tor. The paper seeks to answer the research questions: 1) Are Tor Exit Relays operators ISPs? 2) Are they liable for the actions of their users? 3) Are they forced to inspect the traffic to inhibit their users to commit crimes?

**Keywords:** Tor, Exit Node, ISP, Internet Service Provider, Liability, Privacy, eCommerce directive, mere conduit

## Introduction

In this paper we will investigate on the Liability of Tor Exit Relay operators. We will present in section 1 what is Tor and how it works from the technological prospective. Then in section 2 we will present some of the use cases of the Tor network explaining the advantages and the disadvantages that this technology carries with it. In section 3 we will discuss the problem of the liability and its root causes. We will analyze from this point on the actions of the Tor operators with respect to the category of Internet Service Providers. In section 4 we will present a case of a Tor operator that was sentenced for helping the distribution of child pornography and we will discuss the motivation of the ruling. And lastly in section 5 we will present a similar case of an ISP that was sued for defamation and privacy infringement.

## 1 Background

### 1.1 What is TOR

Tor is a free and open source software aimed to enable anonymous communication on the web. It is the most used and secure *Privacy Enhancing Technology*

that is available now. Tor belongs to the same class as VPNs, Proxies and DNS Bypass. However it is the only technique that has been proved truly ensure your anonymity on the web. For this reason Tor has become more and more popular during these years, especially in countries where censorship is most suffered. Like China and Saudi Arabia. Today Tor is used on average by 2 Million users every day.

The name Tor stands for “The Onion Router“ which is the technology at the core of this software. The Onion Routing is a networking mechanism that ensures encryption and anonymity in a communication between two endpoints. Such endpoints might be two users (in a P2P communication) or a user and a web service (like a website). The connection between endpoints is routed along an encrypted channel that jumps multiple times all over the world inside the Tor Network. Each relay has the knowledge of only the previous and the following nodes in the chain of jumps and this makes the complete picture of the communication hidden from anyone.<sup>1</sup> [1]

## 1.2 How It Works

Tor achieves such anonymity with a very simple architecture that relies on cryptography. It is composed of basically three entities:

- The Directory Servers
- Middle Relays
- Exit Relays

The Directory Servers advertise the entry points of the Tor Network to the client. The network itself is made of components called Relays. Those are of two different types: one is called Middle Relay and another one Exit Relay. Tor creates a circuit starting from the end user to the destination that jumps on different hops (Relays) during its path. At each jump the intermediate packet is encapsulated into an additional layer of encryption, achieving the fact that each node knows only its previous and following hop. From the moment that the request of the end user enters the network it jumps randomly on a set of Middle Relays before reaching the Exit Relays. Those Exit Relays are the points in which the request of the end user makes the last step towards the final destination. See Fig 2

Another fundamental function of Tor are the so called Hidden Services. A Hidden Service is a functionality of Tor used to keep the physical location of a server anonymous and uses a mechanism called rendezvous. When using Hidden Services the client’s request and the server’s response meet in a designated random point in the Tor Network. In this way the anonymity is preserved from both the user and the server side. See Fig 1

---

<sup>1</sup> Although the technology is very strong and secure there are still many attacks that can undermine the anonymity of the Tor users

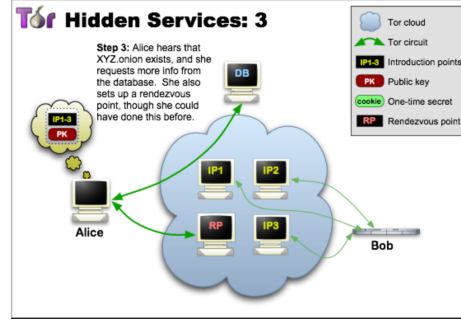


Fig. 1. Tor Hidden Service Architecture

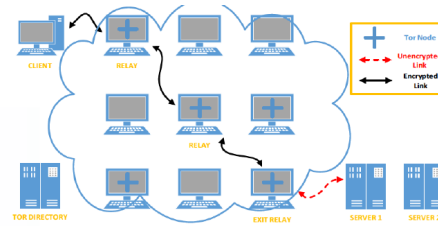


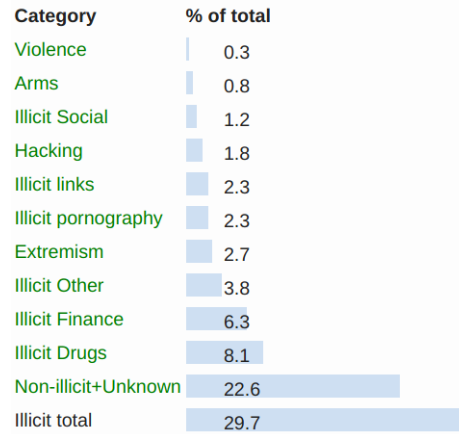
Fig. 2. Tor architecture

The whole Tor technology relies solely on the efforts of volunteers (individuals or organizations) all over the world who run the relays and provide the access to the internet using their own internet access point.

## 2 For what Tor is used for

Tor has been developed with the idea that anyone should be able to surf the internet and express their belief without being monitored by others, not even by governments. Among its main usage we can find privacy protection for individual unwilling to give away their navigation data to ISPs. In the business filed Tor is used to ensure confidentiality and for conducting research on competitors without leaving traces. Similarly Tor can be used for intelligence gathering by government's body like the U.S. Navy, in fact they were the ones who developed this very idea of the Onion Routing. It can also be used to protect the identity of sources for journalists, like whistle-blowers. And It can also help activists to report abuse or organize meetings, as it happened during the Egyptian Revolution of 2011. [2]

Beside that good things, Tor has been accused to be a safe harbor for criminal activity, especially regarding child pornography and drug dealing. As shown in figure 3 the amount of illicit activity percentage on the overall onion services is



**Fig. 3.** Web-Based Onion Services in February 2016 (Source Wikipedia.org)

high (almost 30%). For example famous were the cases of the sites PlayPen <sup>2</sup> and SilkRoad which led to the incarceration of many users and maintainer of those sites.

### 3 The problem: Liability of Tor Exit Relays Operators

Since the Tor Exit Relay Operators are the one that carry on the *last mile communication* they are the one that are most exposed in terms of legal actions. In this paper we investigate the position of the Tor Relay operators and we compare them to the figure of the Internet Service Provider.

As shown in Fig 2 the connection between client to relay and relay to relay is encrypted and does not cause any liability issues to the Middle Relay operator, just because it is not possible to know anything about the traffic that is flowing through the node. The Exit Relays instead, are the most exposed part of the network, since the communication between the client and the server is, at this stage, unencrypted. From the technological prospective, if from their server transit a request from a generic Tor user for a site that hosts illicit content, such request cannot be distinguished from the normal traffic of the person who is operating the Exit Relay. The request will look like as it is the Exit Relay which is originating that traffic. This is because Exit Relays behave in the same way as normal relay does, except for a major difference. They remove the source IP address of any incoming internet packet, and replaces that with its own IP address as a source, lastly they forward the request to the next hop. What is

<sup>2</sup> The PlayPen investigation the American National Security Agency identified thousands of computers around the globe that used Tor to visit the Playpen site. This led to court 137 American citizens for possession of video depicting images with child pornography.

different from the other relays is that in this case the last hop is the final destination and as shown in Fig. 2 the communication between the Exit Relay and the destination server is no longer secured by the Tor protocol<sup>3</sup>. In this case the source address of the machine originating the request to the final destination is the source address of the operator's machine.

There is not much research in the field of liability of Tor operators and people have tried over the years to relate the activity of such people to the activity of the Internet Service Providers. But can Tor Operators be considered as ISP? As it was explained in the section 2 the activity of such people is just to forward internet packets from one node to another. Middle Relays can by no means know nor the content of the packet nor the destination,<sup>4</sup> which makes any surveillance of the traffic technologically impossible. Exit relays instead do know the final destination of the user request and have the technological power to do at least controls to enact censorship. However because of the way they handle the data, they fall in the "mere conduit" safe harbor, which we will see shields them from any liability, given that some conditions are met.

#### 4 The case Austrian Regional Crime Court vs William Weber

In this section I will present the case of Austrian Regional Criminal Court in Graz vs. W. Weber. This case sees W. Weber, a tor exit node operator being sentenced by the court for aiding the distribution of child pornography. I will discuss the case and talk about the reason why he was held accountable and what where the court motivation for that.

**The facts** On June 30th 2014 William Weber a Tor Exit Node Operator was arrested with the charge of helping the distribution of child pornography through his servers. During the investigations he was found talking with an anonymous user of the Tor network about hosting the material on his servers. He said:

*"You can host 20TB child porn with us on some encrypted HDD"[...]  
"You can host child porn on our servers" [...] "If you want to host child  
porn ... I would use Tor."*

After his arrest the authority seized his computer and the Forensic experts have reconstructed some images depicting pornographic acts of children.

At the end of this first litigation he decided to do not go in further trials and accept the court ruling.

**The Court Ruling** W. Weber was sentenced to 3 months of jail and 3 years of probation for helping the distribution of child pornography on through his server.

<sup>3</sup> The communication can still be encrypted at application level with HTTPS but the source and destination IP address are no longer anonymised

<sup>4</sup> Because they know just the previous and the following hop

**Considerations** Regarding the fact that some illicit material was found on his computer he could not be found guilty since there was no evidence that these picture were effectively downloaded by him or by the the automatic caching mechanism. And he was by far protected by the article 12 section 2 of the eCommerce Directive for these evidence:

*2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.*

But, since he was intercepted having that conversation with the anonymous user, he was actively collaborating with the intent of doing illegal activities with that person. That invalidated the liability exemption from "mere conduit" considering the Recital 44 of the Directive:

*(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.*

So the main reason why the court judged W.Weber liable of aiding the distribution of child pornography was not because he hosted a Tor Exit Relay, but because he was intercepted while talking with the user about the possiblith of hosting the illicit material in his website. Although he declared on his blog that this conversation was used out of context and that he was just talking hypothetically that showed to the Court that not only was he at least aware that his Tor node could have been used to do distribute child pornography, but also that he does not disapprove that.

As stated by Hufko [4] *"the Austrian Court found that this activity may lead to criminal liability for aiding and abetting of a crime of distribution of child pornography when coupled with other circumstances."* And the other circumstances that invalidated the *mere conduit* safe harbour were these very transcript acquired during the investigation. In fact the "mere conduit" is valid only if the condition (a),(b), and (c) of the article 12 of the eCommerce directive are met:

- 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:*
  - (a) does not initiate the transmission;*
  - (b) does not select the receiver of the transmission; and*
  - (c) does not select or modify the information contained in the transmission.*

This decision demonstrates that Tor Exit Node Operators should be very cautious when operating their activity not only from the technology prospective, but also from the legal prospective. However as cited in Hut'ko's blog [4] *we should be really careful in keeping the standard of "deliberate collaboration" very high, otherwise it might be easy to criminalize Tor Exit Nodes operators.* Criminalizing the Tor operators would be very easy in countries *with less legitimate criminal offences such as anti-state propaganda crimes* [4]. Without their valuable work the whole anonymity network phenomena would not exist. They in fact operate in one of the most crucial point of the architecture, they connect the anonymous world with the real world, without that connection the anonymity world has no point to exist.

This ruling has not to be considered as against Tor. Tor is still perceived as an important tool to ensure privacy and secrecy, as stated by Shubert in the Constitutional Court who said that *"privacy and especially the secrecy of communication on the Internet have to be protected"* and that the legality of Tor should not be challenged. [5]

## 5 The situation of ISP in Italy

In Italy rules the Art 2043 of the Civil Code which says *"Whatever malicious or negligent misconduct, or negligence, which causes an unfair damage to another person, obliges who committed the fact to pay the compensation"*. However in the 2003 the European Directive commonly known as eCommerce regulation was introduced in the corpus of the law with the D.L. 70 of 2003.<sup>5</sup>

Since there is no case in Italy that sees a Tor Operator on trial and since we demonstrated in the previous sections that the activity of such is similar to the one of the ISPs, we now present a case of an ISP (Google) sued by an organization for defamation and privacy infringement.

### 5.1 The case Google vs Vivi Down

In this section I will present the case Google vs. Vivi Down. Vivi Down is an organization that aims to aid people affected by autism. Google is an American company specialized in internet services. They were sued in the scope of their platform Google Video, which is an online platform where registered users can upload their videos and share them among the community.

**The facts** On May 2006 some highschool students from Turin uploaded on the platform Google Video a video depicting them in the act of insulting and hitting a boy affected by autism. Furthermore the bullies said to be part of the organization Vivi Down. After 2 months the video gained a lot of success for the

<sup>5</sup> Decreto legislativo 9 aprile 2003, n. 70 Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; pubblicato in G. U. n. 61 del 14.04.2003.

time, scoring more than 5000 views before it was taken down by Google. Vivi Down sued not only the boys who commit the crime but also Google bringing as support the art 40 of the Italian Criminal Code. The accuses that Vivi Down addressed to Google were defamation and privacy infringement, because of the disclosure of the extremely personal data about the health of the autistic boy in the video. <sup>6</sup>

**The first level ruling** The trial was carried out by the public prosecutor's office of Milan, being Milan the legal residence of Google Italy[6]. In 2010 the Court found the Google managers not guilty of the accuses of defamation since the activity of Google and his platform Google Video falls into the shield of the European eCommerce regulation 2000/31/CE. In particular they applied the concept discussed above regarding the *mere conduit safe harbor* for which Google Video acting as a simple hosting is not responsible for any illegal acts performed by his users, until he became aware of such infringement. But the Court also said that although the 2000/31/CE forbids the obligation of surveillance of the content that people upload on a service provider's platform In particular they applied the recital 47 which says

*Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; [...]*

With respect to that they should have informed in a clean and explicit way the boys who uploaded the video on the requirement of collecting the explicit consent of the autistic boy for the disclosure of such private information. They correlated this to the Art 13 of the Italian Privacy Code. <sup>7</sup>

Furthermore the Court pointed out that there might have been a malicious intent in the act of Google of sharing the video containing such information because they turned a profit through the platform Google AdWord. <sup>8</sup> And since the platform AdWord was able to track the users behaviour and suggest video raccomandation the Court changed the scope of Google Video from Hosting to Content Provider, which does not benefit from the exemption of the 2000/31/CE. <sup>9</sup>.

<sup>6</sup> "Non impedire un evento, che si ha l'obbligo giuridico di impedire equivale a cagionarlo" - Art 40 of the Italian Criminal Code

<sup>7</sup> *The interested party, or the person whose personal data has been collected, is informed beforehand either orally or in writing*

<sup>8</sup> AdWord is a service given by Google to target user with personalized advertisement based on their browser history

<sup>9</sup> Cfr. M. De Cata, *La responsabilità civile dell'Internet service provider, Milano, 2010, pp. 70-71*, he defines the host provider as someones who gives some memory space of his server for the hosting of a web service, whereas the content provider is someone who gives on its own content to the public as has therefore more responsibility on the content he delivers.



**The Second level ruling** The case was then appealed to the Corte D'Appello of Milan <sup>10</sup> where the Court, respectful the Privacy Code violation of the article 13, ruled that the Google Managers were not guilty since the art 167 says that the violation occurs only if the author acted not conforming the regulation. And that none of the part of this article force the ISP to educate the user concerning the content of the Privacy Code. [6] They also refused the ruling of the first level ruling about the malicious intent of Google in sharing the video with the justification that there were no specific links pointing to the video. Furthermore the Court stated the non-involvement of Google as they acted as only a hosting refusing the scope change in Content Provider and gave all the responsibility of the illegal act to the "uploaders".

**The Third level ruling** The case was finally brought to the Corte di Cassazione who ultimately absolved Google confirming their non-involvement with respect to the European eCommerce Directive 2000/31/CE. As confirmation of non-involvement in the illicit activity was brought as an exaple the fact that Google immediately removed the video from his platform once they became aware of the privacy violation from the authorities. Thus Google acted in full compliance with the recital 46 of the 2000/31/CE

*In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned;*

## 6 Conclusions

We saw in section 3 that the Exit Relay operator are the ones that put themselves in the most risky position because they share their personal internet access point with anonymous users of the Tor Network. But as seen also in the section 4 they limit themselves to only forward the internet traffic to the final destination without any interference with it.

The case presented in the section 4 was very interesting since is the only case available in that field but the fact that Mr. Weber decided to do not go into further level of trials does not allow a complete analysis of the case. From what we have we can say that the court found W.Weber liable not because he was operating the node, but because he was actively collaborating in the act of helping the distribution of child pornography suggesting the anonymous user the optimal way to deliver such content with the help of his server and through the Tor network. We can say that the legitimacy of operating a Tor Exit Relay remains untouched if the operators follow the guidelines of the 2000/31/CE eCommerce directive.

The case in section 5 demonstrated that an ISP in Italy is not liable for the content that the users of its services put on the network. Again this was

<sup>10</sup> Corte d'Appello di Milano, I sezione penale, sentenza n. 8611/12, 21 dicembre 2012.

possible because of the 2000/31/CE eCommerce directive which states the non-involvement of the ISP and more importantly forbids the states to claim any surveillance by an ISP on the user activity. The ISP however should be careful in removing the illicit content to benefit the shield.

In this paper we investigated in a relatively new field which as not been well regulated yet, because the technology that is involved is too borderline to define explicitly what is black and what is white. It was seen that besides the case at section 4 there were no legal actions against Tor Exit Relays operators. Maybe because they generate kind of traffic that is highly recognizable and that makes clear the non-involvement of the operators in the content of the communication. Even the NSA has demonstrated no interest in prosecuting the exit operators, aiming instead to the users as it was done with the PlayPen case. Also it is to say that the majority of sites that host illicit activity, if not all of them, use the technology of Hidden Services which makes the detection of the illicit activity even harder to investigate. That may explain why there has been no other cases that touched this matter. As stated in section 4 Tor is still perceived as a crucial technology to safeguard the freedom of expression of all the people around the globe for the reason we explained in section 2. We can say that the legitimacy of running a Tor Exit Relay remains untouched and this is confirmed also by the fact that some of them are hosted in institutional places like universities.

## References

1. Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula (2015). *Technical and Legal Overview of the Tor Anonymity Network*. NATO Cooperative Cyber Defence Center of Excellence, Tallin, Estonia
2. Keith D. Watson. (2012) *THE TOR NETWORK: A GLOBAL INQUIRY INTO THE LEGAL STATUS OF ANONYMITY NETWORKS*. Washington University Global Studies Law Review
3. Electronic Frontier Foundation  
*The Playpen Cases: Frequently Asked Questions* link:  
<https://www.eff.org/it/pages/playpen-cases-frequently-asked-questions>  
 date of last visit: "03/04/2019"
4. Hutko's Technology Law Blog  
*Austrian Court Sentenced a Tor Exit Node Operator* link:  
<http://www.husovec.eu/2014/07/austrian-court-sentenced-tor-exit-node.html>  
 date of last visit: "12/04/2019"
5. Loek Essers, PC WORLD  
*Tor exit node operator convicted of abetting spread of child porn* link:  
<https://www.pcworld.com/article/2452320/tor-exit-node-operator-convicted-of-abetting-spread-of-child-porn.html> date of last visit: "12/04/2019"
6. Federica Notari, Amministrazione In Cammino  
*La controversa responsabilità dell'Internet Service Provider in materia di privacy nella giurisprudenza europea e interna: il caso Google*