University of Washington School of Law
UW Law Digital Commons

Technology Law and Public Policy Clinic

Centers and Programs

9-13-2013

Tor Exit Nodes: Legal and Policy Considerations

Sarah Campbell Eagle

Abigail St. Hilaire

Kelly Sherwood

**The Technology Law and Public Policy Clinic at
the University of Washington School of Law**

TOR EXIT NODES
LEGAL AND POLICY CONSIDERATIONS

Student Authors:

Sarah Campbell Eagle, Abigail St. Hilaire and Kelly Sherwood

Clinic Director
William Covington covinw@uw.edu

Section 1-Introduction

Anonymity Networks

The Internet is a constant companion to people the world over and as technology improves it is becoming more accessible every day. With the amount of communication that occurs online, it was only a matter of time before anonymity became an important topic of discussion. Several so-called "anonymity networks" have been developed to facilitate anonymous communication by the citizens of the web. Because the use of these networks is already so widespread, the time is ripe for a discussion of their merits and potential government responses to this phenomenon.

An anonymity network "enables users to access the Web while blocking any tracking or tracing of their identity on the Internet."[1] Anonymity networks generally use some combination of encryption and peer-to-peer networks to allow people to use the Web anonymously. Electronic encryption functions much like the codes that have been used by governments and militaries for centuries. Put simply, one computer will translate a message into a secret code and only computers that have the key to the code will be able to decrypt it. Encryption contributes to anonymity for the obvious reason that if a message is sent over the Internet and someone intercepts it, they won't be able to decode it unless they have the key (or a very powerful computer depending on the level of encryption). The shortcoming of encryption is that is doesn't protect the source or the destination of the communication, only the content of the message. Peer-to-peer networks are networks like Napster. When a person would download music on Napster, they were downloading it from another user's machine. There was no central database where all the information was stored. These networks can contribute to anonymity in the sense that there isn't a central server that is monitoring and recording all of the traffic in the network.

Anonymity networks are most effective when they are more widely used. They rely on volume of communications to cloak individual communications. A good network will also require minimal computing power and consume few network resources, as all the encryption in the world won't do any good if it makes the network too slow to be useable.

Most Common Types of Anonymity Networks

Tor

The Onion Relay ("Tor") enables individuals to access sites and services available on the Internet in ways that are, at once, secure and anonymous. It does so by employing a decentralized, volunteer-run network of servers throughout the world. To use the Tor network, individuals operate through Tor clients, which cipher and decipher information and in turn make use of Tor servers, which relay information from a point of entry (or "node"), to other Tor nodes, to an exit node that delivers the user to a publicly accessible Internet location. Accordingly, when a user transmits and receives information vis-à-vis the Tor network, that information is both encrypted and encapsulated: encryption hides the user's content, and encapsulation hides the user's identity.[2]

[1] Techopedia, *Anonymity Network*, at http://www.techopedia.com/definition/25187/anonymity-network (last visited June 2013).

[2] The Tor Project, *Tor: Overview*, at https://www.torproject.org/about/overview.html.en (last visited June 2013).

Tor's system architecture attempts to provide a high degree of anonymity and strict performance standards simultaneously. Tor provides anonymity for its users by constructing a multi-hop circuit through the network of Tor routers, using a layered encryption strategy known as *onion routing*. As information travels from one Tor operator's tunnel to another, the software adds a new "layer" of encryption (hence the onion metaphor). This process means that no operator in the circuit can ever trace the transmission back more than one layer, which protects the anonymity of the Tor user who initiated the request. [3]

Tor operators called "relay nodes" pass information along the circuit, and an "exit node" operator hands off the transmission to the user's intended destination. That destination might be a website, an instant messaging server, or any other online services that Tor users wish to access without revealing their true IP addresses. The transmission bears only the exit node operator's IP address, which means that the transmission appears to come directly from the exit node. [4]

Due to the way Tor encrypts data, "each node in the circuit can only know the IP addresses of the nodes immediately adjacent to it."[5] The list of nodes is publicly available, but it doesn't do potential trackers any good to know who runs the nodes because trackers can't find out who is using a given node at a particular time. A potential tracker would probably be able to find out that someone was using Tor. A person would also be able to look at traffic from an exit node to sites on the Internet, but that person can't connect traffic from exit nodes to traffic entering the Tor network (unless they already knew where the traffic was coming from and where it was going, which would eliminate the need for tracking).

The only thing about Tor that looks like a peer-to-peer network is the fact that people who download the Tor client software can be used as nodes. Tor is mostly used to communicate with people outside the Tor network, however.

Freenet

Downloaded over 2 million times since its launch in 1999, Freenet is the most widely used anonymity-protecting peer-to-peer network.[6] Freenet is software available for free download that allows users to anonymously share files, browse the Internet, and publish information on "freesites" (websites accessible only through Freenet). It has five primary objectives: (1) to prevent censorship; (2) to provide anonymity for users; (3) to remove any single point of failure or control; (4) to store and distribute files efficiently; (5) and to enable peers, which it terms "nodes," plausibly to deny knowledge of the files stored on their computers.[7] Freenet employs an absolutist philosophy of anonymity based on the central premise that the free flow of information is essential to the maintenance of a democratic society.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Free Network Project, *What is Freenet?*, at http://freenet.sourceforge.net (last visited June 2013).

[7] Adam Langley, Peer-to-Peer: Harnessing the benefits of a Disruptive Technology. *NEED TO GET THIS CITATION.

Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what the content of the message is. Users contribute to the network by giving bandwidth and a portion of their hard drive (called the ‘data store’) for storing files. Files are automatically kept or deleted depending on how popular they are. Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can’t be held accountable for it. Chat forums, websites, and search functionality, are all built on top of this distributed data store.[8]

I2P Anonymous Network

I2P is an anonymity network with functionality that lands somewhere in between Tor and Freenet. It is less peer-oriented than Freenet because it doesn’t actually require people to use I2P directly. Most users will only use it through “I2P enabled applications.”[9] This means that many users won’t even know that they are using I2P, but their communications will be sent through the I2P network when using one of these applications. It is more peer-oriented than Tor because all of the communication actually takes place inside the network. There are websites within the I2P network, but the network itself isn’t designed for communication outside the network. It is meant to make both the sender and the recipient anonymous to each other and to third parties. This leads us to Tor, which requires a peer network to function, but doesn’t limit communication to peers.

Section 2-Why Be Anonymous?

The Reality of Privacy Online

A strong desire for online anonymity is often met with suspicion and skepticism. Many people have trouble imagining why someone would want to be anonymous online, unless that person was planning on undertaking some illicit activity.

The simplest response is that people want to be anonymous online for the same reason citizens don’t want security cameras on every street corner. Of course, not everyone is opposed to security cameras on every corner, but when someone is opposed to it they aren’t immediately suspected of questionable behavior. Many people generally prefer privacy, and privacy online is just as important to some people as privacy in the street.

Part of the suspicion of online anonymity is likely due to a misconception about how the Internet works and how private it actually is. Many people assume that because they don’t voluntarily give out information online, or because they are never the victim of identity theft, that their online conduct is already private. In reality, data is constantly being gathered by various parties. Web traffic is monitored by private companies and the government. Personal data is collected without Internet users ever knowing it happened.

[8] Freenet, *What is Freenet?,* at https://freenetproject.org/whatis.html (last visited June 2013).

[9] *A Gentle Introduction to How I2P Works*, at http://www.i2p2.de/how_intro (last visited June 2013).

A quick look at Google's privacy policy reveals just how much information can be gathered from relatively menial online tasks. Google seems to be fairly transparent in the sense that they make it easy for users to learn what kinds of information is being gathered, but every website that a person uses could theoretically gather much of the same information and not be nearly as straightforward about it as Google.

Google gathers basic user information, which is information that is requested by Google and input by the user when setting up accounts and the like. Google also collects "device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number)."[10] Google also says that it "may associate your device identifiers or phone number with your Google Account."[11] This means that even if you chose not to give your phone number to Google when signing up for an account, they might gather that information anyway from your mobile phone when you use it to access their services.

Google also gathers details about the use of their services, like search queries. Google can also collect information about a person's actual location when that person uses a location-enabled Google service like Google Maps. [12] Google also gathers information about how a user interacts with ads and content. The way that Google gathers information may not seem particularly invasive, but if every website anyone uses gathers similar information and every service anyone signs up for monitors behavior patterns, there is an enormous amount of information being gathered about every single Internet user all the time. That information can be stored indefinitely so there is potentially a years-long record of online activity following around every person who has used the Internet that long.

Tor would prevent Google or any other company from gathering information like this by preventing the companies from linking online actions to specific people. The companies would see that the exit node was taking certain actions, but they would have no way of tracing those actions back to the user, assuming the user was properly employing Tor. Although companies gather information for profit-seeking purposes, governments can use much of the same information to monitor and censor their citizens.

Social Benefits to Anonymity

The major social benefit of Tor is as an anti-censorship tool. Around the world, dictatorial regimes monitor the web traffic of their citizens. By disallowing access to websites that have anything to do with furthering freedom of thought or expression these regimes prevent their citizens from engaging in meaningful political discourse. When citizens do manage to engage in a conversation that questions the ruling party or the methods of the government, those citizens are often persecuted as traitors or seditionists.

[10] Google, *Privacy Policy*, at http://www.google.com/policies/privacy/ (last visited June 2013).

[11] Ibid.

[12] Ibid.

The Tor Project reports that "human rights activists use Tor to anonymously report abuses from danger zones."[13] The organization Human Rights Watch also recommends Tor for use by people attempting to counteract state censorship particularly in China, but also in the rest of the world to facilitate safer communication about human rights abuses.[14]

Business Uses

Tor also has some practical uses for businesses. Companies that gather information on the Internet for proprietary purposes can use Tor to hide their tracks. If a company could monitor the Internet usage of its competitor's employees, it could gain a serious competitive advantage.

Some companies also get more devious and attempt to reroute their competitors' IP addresses in an effort to prevent their competitors' from having access to basic information that even customers have access to. It is common for companies to simply browse the websites of their competitors to gather information, but some companies will redirect that traffic to counterfeit sites. Companies can use Tor to disguise their identities and view the Internet as it is viewed by every day customers.

Large corporations that are concerned about dishonest behavior inside the organization can use Tor to allow their employees to blow the whistle on their superiors anonymously and without fear of reprisal. In that way, Tor can be a tool to achieve accountability throughout an organization.[15]

Journalistic Uses

Journalists can get tremendous utility out of Tor. In many instances it is vital for journalists to be able to conduct their work anonymously, even in countries with a cultural proclivity for free speech. People who aren't journalists can use Tor to report on events in countries where the traditional media is suppressed or co-opted by the government. It is also important for the sources journalists come in contact with to be able to remain anonymous, especially if they are whistleblowers.[16]

Law Enforcement Uses

Law enforcement can benefit from Tor just as easily as dissidents and criminals. Undercover operations happen constantly and many criminals possess the computer savvy to check the IP addresses of the people they communicate with. If criminals saw that the IP

[13] The Tor Project, *Activists & Whistleblowers use Tor*, at https://www.torproject.org/about/torusers.html.en#normalusers (last visited June 2013).

[14] See generally, Human Rights Watch, *Race to the Bottom: Corporate Complicity in Chinese InternetInternet Censorship* (2006), at http://www.hrw.org/sites/default/files/reports/china0806webwcover.pdf (last visited June 2013).

[15] The Tor Project, *Inception: Businesses use Tor*, at https://www.torproject.org/about/torusers.html.en#normalusers (last visited June 2013).

[16] The Tor Project, *Inception: Journalists and their audiences use Tor*, at https://www.torproject.org/about/torusers.html.en#normalusers (last visited June 2013).

addresses of their supposed coconspirators were located inside a law enforcement office, the undercover operation would no longer be undercover.

As with businesses and journalists, people can use Tor to anonymously tip off law enforcement about illegal behavior, so it serves a whistleblower function in this context as well.[17]

Section 3-Liability and the Tor Network

Introduction

Internet anonymity serves many legitimate ends, but is also subject to potential abuse. Internet anonymity can contribute significant social value by providing a platform for individuals to preserve privacy, enable free speech, and facilitate political reform. Recently, dissidents in Egypt used the Tor network extensively during the Arab spring to get around the Internet shutdown, and it has been used by bloggers in Syria to communicate with the outside world. But the same anonymity that enables the spread of democracy can be used to shield those who choose to use Tor to access or publish offensive and illegal material to the Internet.

Generally courts have interpreted the freedom of speech and right to anonymity on the Internet to be limited by or withheld from three primary types of content: obscenity (specifically child pornography),[18] defamation and libel,[19] and copyright infringement.[20] In those areas, speakers cannot escape liability simply by publishing anonymously.[21] The difficulty with anonymous speech over networks like Tor is that the network is designed to prevent node operators from knowing the content and origination point of data passing through the network.

This may be particularly frustrating for law enforcement, because there is neither a statutory basis granting law enforcement access to encrypted data, nor is there any way to access that data from the network itself. The decentralized design and multilayered encryption of the Tor network renders operators incapable of identifying the sources of transmissions that travel through their nodes.

Further, if the Tor network were to be found liable for copyright infringement or child pornography distribution, it is not clear that there is any way to disable the network. Tor is decentralized in the sense that the software itself routes all user activity through a series of volunteer operators, and no single entity monitors or controls the process. In essence, the software does everything short of funding itself and updating its own code – functions that are currently performed by TorProject.org. This decentralized design allows the Tor service to

[17] The Tor Project, *Inception: Law enforcement officers use Tor*, at https://www.torproject.org/about/torusers.html.en#normalusers (last visited June 2013).

[18] *See United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996), cert denied, 519 U.S. 820 (1996) (finding couple guilty of knowingly transporting obscene files in interstate commerce under a federal obscenity statute because of a computer bulletin board service).

[19] *See Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (noting a “legitimate and valuable right to participate in online forums anonymously or pseudonymously” that must be weighed against “the need to provide injured parties with an forum in which they may seek redress for grievances”).

[20] Ar*ista Records LLC v. John Does 1-19*, 551 F. Supp. 2d 1, 8 (S.D.N.Y. 2008) (holding that where the speech in question is copyright infringement the privacy interests are “exceedingly small”).

[21] *See AutoAdmit.com*, 561 F. Supp. 2d at 254; *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999); *Doe No. 1 v. Cahill*, 884 A.2d 451, 456 (Del. 2005).

operate in the absence of an overseeing entity. This means that the network could remain operational even after a complete shut down of the Tor Project, Inc. the entity that presently funds and develops Tor software.

Reduced Exit Policies for Exit Node Operators

The fact that all Tor users take on the IP addresses of their exit node operators exposes those exit node operators to liability for any Tor user's wrongdoing. This is a particular concern because it is statistically likely that an exit node will be used at some point for illegal purposes. For exit node operators in the US, the Tor network allows the operators to adopt a reduced exit policy. A reduced exit policy is simply a configuration of the exit node whereby it will only deliver data to specified ports in the Internet, and the ports are selected as those that will not deliver to sites that allow illegal file sharing.[22]

Tor and Child Pornography Laws

The structure of Tor allows users to access sites that would be blocked in the user's home country by connecting to the network and routing their request through an exit node in a country that does not restrict Internet usage. This has contributed to Tor's reputation as a safe haven for criminal activity, especially child pornography.[23]

The Protection of Children Against Sexual Exploitation Act prohibits the interstate transportation, distribution and receipt of visual images of child pornography.[24] This law attaches criminal liability to those who knowingly receive or distribute child pornography "by any means including by computer."[25] On its face, this seems to indicate that a Tor operator could be held liable if they knowingly facilitated the downloading of child pornography. But the whole design of Tor is to keep node operators from knowing what is being routed through their computers. Further, in *United States v. X-Citement Video, Inc.*,[26] the Supreme Court held that distribution entities must have specific knowledge of the pornographic images for the entity to be held liable under this statute.

There is a case currently being litigated in Kentucky that may settle the question of whether Tor operators will face liability in child pornography cases.[27]

[22] https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment (last visited June 5, 2013).

[23] Jennifer B. McKim, *Privacy Software, Criminal Use*,
BOSTON.COM (Mar. 8, 2012), http://articles.boston.com/2012-03-08/business/31136655_1_law- enforcement-free-speech-technology (discussing various criminal uses of Tor); Ryan Naraine, *Hacker Builds Tracking System to Nab Tor Pedophiles*, ZDNet (Mar. 6, 2007), http://www.zdnet.com/ blog/security/hacker-builds-tracking-system-to-nab-tor-pedophiles/114 (discussing a hacker working to track pedophiles on Tor).

[24] 18 U.S.C. § 2252.

[25] 18 U.S.C. § 2252(a)(2).

[26] 513 U.S. 64 (1994).

[27] *Commonwealth v. Eggers*, 13-F-00389 Boone County (Last hearing, April 26, 2013).

Tor and The Digital Millennium Copyright Act

In response to the copyright issues that arose as a result of the emerging popularity of file-sharing on the Internet, Congress enacted the Digital Millennium Copyright Act (DMCA) in 1998.[28] In drafting the DMCA, Congress acknowledged the unique relationship that an Internet service provider (ISP) has with both its customers and the copyright owners whose property may be transmitted through the ISP's systems and networks.[29] Accordingly, the DMCA differentiates between "direct infringement" and "secondary liability."[30] Direct infringement is assessed against those principally involved in the copyright infringing activity, while secondary liability attaches to "passive, automatic acts engaged in through a technological process initiated by another."[31] In creating this dichotomy, Congress intended to encourage cooperation between those attempting to enforce their copyrights and those in the position to "prevent ongoing infringement."[32]

Despite Congress's best intentions and the broad scope of the DMCA, time and advances in technology have revealed flaws in the statute that make it difficult to apply to anonymizers like the Tor network. In *RIAA v. Verizon*, the Second Circuit noted that the legislative history of the DMCA indicates that Congress never contemplated that Internet users would be able to "directly exchange files containing copyrighted works."[33] Consequently, the DMCA does not seem to attach liability when users directly interact with one another and the ISP is passive and merely provides access to the networks over which it has little or no control.[34]

But peer-to-peer sharing is not the only trigger for DMCA coverage. Use of the Tor network to conceal copyright infringement has not yet been litigated, so it is not clear whether a node operator could face liability under the act.

Theories of Liability Under the DMCA

Because Tor can be used to facilitate the transfer of copyrighted files without detection, the applicable doctrine is secondary copyright infringement. DMCA secondary infringement generally rests on three theories of liability: contributory, vicarious, and inducement. Contributory liability requires that a software developer "knowingly" and "materially" provide assistance to a direct infringer.[35] Vicarious liability requires a developer to have a "financial interest" in the infringement and have "the right and ability to supervise the infringing activity.[36] Inducement theory stems from the Supreme Court's decision in *Metro-Goldwyn-Mayer Studios*,

[28] Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.).

[29] H.R. Rep. No. 105-551(I), at 11 (1998).

[30] *Id.*

[31] *Id.*

[32] Katherine Raynolds, *One Verizon, Two Verizon, Three Verizon, More? A Comment: RIAA v. Verizon and How the DMCA Subpoena Power Became Powerless*, 23 Cardozo Arts & Ent L.J. 343, 349 (2005).

[33] *Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1238 (D.C. Cir. 2003).

[34] *See, e.g., Verizon*, 351 F.3d 1229 (holding that the DMCA only permits the issuance of subpoenas when an ISP engages in hosting copyright infringing materials on its servers, and not when the ISP is "acting as a conduit for P2P file-sharing") (emphasis added).

[35] See, e.g., Sony, 464 U.S. at 487 (citing Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

[36] See, e.g., Napster, 239 F.3d at 1022 (9th Cir. 2001) (citing Gershwin Publ'g Corp., 443 F.2d at 1162).

Inc. v. Grokster, Ltd.[37] There the Court held that software developers could be liable for secondary infringement if they "induced" the use of their software to commit copyright infringement.[38]

There is one important exception to secondary copyright liability. In *Sony Corporation v. Universal City Studios,*[39] the Court held that contributory liability for copyright infringement does not apply to the makers of a device if the device has "substantial non-infringing use."[40] While the Tor network clearly has non-copyright-infringing uses, through its protections of free speech and privacy, it is not clear that a court would see it as a "device" and allow it to be excepted from liability.

The most viable theory to apply DMCA liability to Tor node operators is likely the theory of contributory infringement, as neither vicarious liability nor inducement theory is likely to attach liability to a Tor operator. But even if this theory is successfully applied, Tor network operators may escape liability under the safe harbor provisions set out in 17 U.S.C. §512(a).

An ISP can be held vicariously liable for copyright infringing activity by one of its customers if the ISP: (1) possesses the right and ability to supervise the infringing conduct and (2) has an obvious and direct financial interest in the exploitation of the copyrighted materials. This theory is ill-suited for the Tor network because it would require showing that the node operator had an "obvious and direct financial interest in the exploitation of copyrighted materials." Tor operators gain no financial benefit from their actions. If anything, they incur costs in the form of reduced bandwidth and computer processing resources.

Inducement is also ill suited as a theory of liability because it would require a showing that the Tor operator intended to induce infringement by communicating messages "designed to stimulate others to commit violations."[41] This theory has not been heavily tested, but seems unlikely to succeed because Tor operators typically hold themselves out as providing a privacy and civil liberties tool, and generally discourage illegal file sharing over the network.

Contributory Infringement Theory Applied to the Tor Network

The most relevant theory of liability for Tor operators under the DMCA is that of contributory infringement. The file-sharing service Napster was famously enjoined under this theory of liability, and though the Tor network operates in a fundamentally different way than Napster, some of the characteristics of the networks are similar.[42] Operators of Tor nodes claim protection from liability, asserting that they simply move traffic from one point to another at the behest of others and as such they qualify for the safe harbor outlined in 17 U.S.C. § 512(a).

[37] 545 U.S. 913 (2005).

[38] Grokster, 545 U.S. at 936-38.

[39] 464 U.S. 417 (1984).

[40] *Sony*, 464 U.S. at 442.

[41] *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936-37 (2005).

[42] *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

To prevail under inducement theory, a plaintiff would need to prove that the Tor operator: (1) had knowledge of infringement and (2) materially contributed to it.[43] In the Tor context, the first element of contributory infringement – knowledge of infringement – may be established if the node operator received notice of alleged infringement (either from the operator's ISP or in the form of a complaint from the copyright holder). When an ISP receives a complaint from a copyright holder alleging infringement by one of the ISP's customers, the ISP may forward the notice to the alleged infringer as part of a statutorily prescribed process commonly known as "notice and takedown." Tor exit node operators are particularly likely to receive §512(c) notices, because theirs are the only IP addresses that a destination will ever see.

Plaintiffs could potentially establish the second element of contributory infringement, material contribution to the infringement, by arguing that Tor helps individuals access and disseminate the copyright-violating material. By anonymizing the direct infringer's Internet activity, the Tor operator arguably eliminates a fear of detection that may otherwise discourage such activity.

Tor Networks are Likely Entitled to Safe Harbor under the DMCA

Tor operators may be entitled to statutory safe harbor under DMCA §512(a) as conduits for transitory network communications. Section 512(a) limits monetary liability for digital network communication service providers that merely act as conduits for information.[44] "Service provider" is a term of art, defined within the statute to be "an entity offering the transmission, routing, or providing of connections of digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[45] Tor falls neatly into this exception because Tor does not modify the information routed on its network, but rather it merely relays traffic.

Tor likely meets the five requirements set out in the statute, and would thus be eligible for DMCA safe harbor protection. First, under §512(a)(1), the transmission must be "initiated by or at the direction of a person other than the service provider."[46] This is true of Tor operators in that they merely relay Internet traffic initiated by a Tor user.

Second, under §512(a)(2), "the transmission, routing, provision of connections, or storage" must be "carried out through an automated technical process without selections of the material by the service provider."[47] That is precisely what Tor software does: it automatically selects a random circuit of Tor operators through which it routes the Tor user's activity. Operators do not select the routed material – the software does it for them. The fact that exit node operators have the ability to set an exit policy (meaning that they can block their node from delivering requests to certain sites) might disqualify Tor operators from the conduit safe harbor under §512(a)(2). But an exit policy will affect all possible users of that port, which indicates that the level of control is not sufficiently precise to constitute a "selection" of material for §512(a)(2) purposes.

[43] *See Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971) (defining a contributory infringer as "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another").

[44] 17 U.S.C. § 512(a) (2006).

[45] 17 U.S.C. § 512(k)(1)(A).

[46] 17 U.S.C. § 512(a)(1).

[47] 17 U.S.C. § 512(a)(2).

The third safe harbor requirement is that service providers "not select the recipients of material except as an automatic response to the request of another person."[48] This is true as to the ultimate recipient of material transmitted through the Tor network because the destination is predetermined by the Tor user who initiated the request, and is not affected by the node operators.

The fourth statutory requirement deals with data storage, and prohibits safe harbor conduits from making copies of the material passed through the network. Tor operators likely meet this requirement as operators do not store the transmitted data – they merely hand it off from one node to another until reaching the exit node, which then passes the data to the user's destination. It is technically possible for an exit node operator to capture and store information at this final handoff, but doing so would require modifying the Tor software itself. While such modified software may not satisfy this safe harbor requirement, the modification itself means that it is no longer Tor, and accordingly does not affect Tor's ability to meet this statutory requirement.

The final requirement is the transmission of material "through the system or network without modification of its content," and again Tor seems to satisfy this prong, as operators do not inspect content in the Tor network. Node operators merely route the information along a randomly assigned circuit until it reaches an exit node that will deliver it to its final destination.

State "Super DMCA" Laws

Since 2001, the Motion Picture Association of America (MPAA) has been lobbying state governments to pass laws that would build upon the federal DMCA to close loopholes left by the DMCA and address advancements in technology. Critics have dubbed these laws "Super" Digital Millennium Copyright Act laws (SDMCA) because they functionally expand the rights of copyright holders under the DMCA. The SDMCA laws have only been passed in a few states, and appear to encroach into areas of federal jurisdiction, which could indicate that the laws are preempted.[49] Washington has not, at this time, adopted a SDMCA law.

Section 4-First Amendment Protections

The following section briefly answers the question, what is the extent of the First Amendment's protection of anonymous speech, specifically speech anonymized by the use of the Tor network or other similar anonymity networks. It begins by providing a brief overview of the central issue surrounding anonymous Internet speech, then outlines the Supreme Court's consistent protection of anonymous speech as well as the boundaries of the protections for such speech.

[48] 17 U.S.C. § 512(a)(3).

[49] Kevin McReynolds, *Sdmca Laws: Preemption and Constitutional Issues*, 12 UCLA Ent. L. Rev. 63, 92 (2004)

Extent of Protections for Anonymous Speech through the Tor Network under the First Amendment

The legality of the Tor network, and other similar anonymity networks, ultimately centers on whether or not there must *always* be a way to identify a speaker. Critics insist that the potential for abuse is simply too great to allow complete anonymity online, however, there is everything to suggest that the First Amendment would not allow a complete ban on Internet anonymizers, as this would be a severe restriction on speech. The mere potential for abuse does not place speakers who use anonymity networks outside First Amendment protections. Rather, anonymous Internet speech should be afforded the same protections as more traditional methods of speech, such as handbills, which have always been vigorously protected.

When using the Internet or social networks, users' identities are protected only by company policies and user agreements; there are few affirmative things users can do to ensure their identity or location will not be discovered, subpoenaed, or sold. By utilizing Tor, individuals are able to take control of their personal information and ensure they are absolutely untraceable. Meaning that there is no way to identify a speaker who speaks outside of the protections of the First Amendment, in order establish criminal or civil liability. Also meaning, that speech may be able to occur in environments where it otherwise would be suppressed.

Anonymity networks are the digital equivalent of anonymous handbills and should be afforded the same protections. Any potential for abuse should be irrelevant for the legality of the Tor network, or other similar anonymity networks; anonymous speech is simply too valuable. The ability to engage in anonymous speech, particularly political or religious speech, is vigorously protected by the First Amendment. Accordingly, a blanket limitation or prohibition on the use of First Amendment rights is unsound.[50]

The Supreme Court has consistently protected anonymous speech

Just as the First Amendment protects a right to speak, so also, it protects the right to be silent and refrain from speaking.[51] The right not to speak includes a right not to disclose one's identity when speaking. This right should extend to Internet speech, the same as any other written communication.

The First Amendment was drafted partially in response to the "obnoxious press licensing laws of England, which [were] enforced on the Colonies [due] in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government."[52] The First Amendment is a reflection of the value that the American Constitution places on the ability of "[p]ersecuted groups and sects from time to time throughout history [to be able to] criticize oppressive practices and laws anonymously or not at all."[53] In light of this value, the Supreme Court has consistently protected anonymous speech—

[50] *Jaynes v. Com.*, 276 Va. 443, 666 S.E.2d 303 (208), *cert denied*, 129 S. Ct. 1670, 173 L. Ed. 2d 1036 (2009).

[51] *See West Virginia State Board of Education v. Barnette*, 319 U.S. 624, 642 (1943) ("If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion or other matters of opinion or force citizens to confess by word or act their faith therein").

[52] *Talley v. California*, 362 U.S. 60, 63 (1960).

[53] *Id*. at 64.

declaring unconstitutional: a ban on anonymous handbills[54], a law prohibiting the distribution of anonymous campaign literature[55], and a law regulating the gathering of signatures on petitions for ballot initiatives, which, among other things, specifically required petition circulators to be registered voters and wear a badge bearing their names,.[56]

The underlying issue faced by the Supreme Court in each of its cases addressing the right to anonymous speech is the question of how to balance the benefits of secrecy and disclosure.[57] While Tor can certainly be used abusively, its ability to promote otherwise suppressed speech is simply invaluable.

Scope of First Amendment protections of anonymous speech

While individuals have a First Amendment right to anonymous speech on the Internet, that right is subject to limitation.[58] There are two substantial limitations to the First Amendment's protections. First, the First Amendment only protects against invasive or coercive *governmental* activities. This means that if service providers voluntarily relinquish information concerning a users' identity, there are few protections outside of remedies provided in contract law for breach of service agreements.

Second, the simple fact that speech may be made anonymously does not grant greater speech rights than non-anonymous speech; accordingly, anonymous speech remains subject to certain limitations—fighting words, incitement, defamation, and obscene speech are all unprotected categories of speech. Furthermore, not all speech equally implicates First Amendment protections. For instance, when Internet users share files, the First Amendment interest implicated is minimal, since file-sharers' ultimate aim is not to communicate a thought or convey an idea, but rather to obtain copyrighted music or movies for without cost. Even if expression is an ancillary aim, if the method of speech is illegal the First Amendment rights are exceedingly small.[59]

However, even where a private party seeks to obtain the names of Internet users, courts may require a specific showing by the plaintiff to demonstrate that the First Amendment concerns are outweighed by the pending legal matter. Some court have required plaintiffs to establish a prima facie case before releasing of anonymous activity, others have established a several step procedure to prevent needless disclosures and to give the poster advance notice of the disclosure.[60] This is consistent with courts' continual emphasis that an author's decision to

[54] *Talley*, 632 U.S. at 64

[55] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995)

[56] *Buckley v. American Constitutional Law Foundation*, 525 U.S. 182 (1999)

[57] *See Doe v. Reed*, 130 S. Ct. 2811 (2010) (finding that disclosing petitions for a ballot referendum does not inherently violate the First Amendment, though the Court left open the possibility of challenge if it could be demonstrated that disclosure would lead to chilling, threats, intimidation, or reprisals)

[58] In re Does 1-10, 242 S.W.3d 805 (Tex. App. Texarkana 2007) (holding the trial court abused its discretion by issuing an order compelling an ISP to disclose the identity of a blogger who allegedly posted defamatory comments on an internet site apart from the applicable rules of procedures).

[59] *Call of the Wild Movie, LLC v. Does 1-1, 062*, 700 F.Supp.2d 332 (D.D.C. 2011) (holding the First Amendment right to anonymity when file-sharing on the internet is exceedingly small).

[60] *See Dendrite Intern., Inc. v. Doe No. 3*, 342 N.J. Super. 134, 775 A.2d 756, 17 I.E.R. Cas. (2001) (In order to obtain identity of anonymous poster on Internet, party must make a showing that he plaintiff suffered harm as a result of the alleged defamatory postings); *Immunomedics, Inc. v. Doe*, 342 N.J. Super. 160, 75 A.2d 773 (2001)(

remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[61]

Conclusion

The extent of protections afforded to Internet speech anonymized through use of the Tor network, or other anonymity network, is uncertain. However, both the value of and protections for anonymous speech are well established. All methods of speech are subject to abuse, and the mere possibility that speakers may abuse a means of speech does not remove them from the scope of First Amendment protection. So long as speakers use the Tor network for expressive activity, its First Amendment protection will be ensured.

Applies a four-part test: 1. Make effort to notify the posters that they are subject to an application of disclosure; 2. Identify the statements made; 3. Must provide evidence to support prima facie the cause of action; and 4. Court must balance interest of the parties.); *La Societe Metro Cash & Carry France v. Time Warner Cable*, 36 Conn. L. Reptr. 170, 2003 WL 22962857 (Conn. Super. Ct. 2003) (subpoena of names of anonymous Web users given strict scrutiny but allowed)

[61] *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011) (*citing McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995)).