Tor: Technology on Trial

Privacy in the Digital Age

Northeastern University School of Law
Legal Skills in Social Context
Social Justice Program
In conjunction with: Tor Project, Inc.

Law Office 11
Spring 2015

Lucia Curiel
Josh Demers
Kevin Fields
Jacob C. Miller
William J. Rainsford
Molly Shea
Matthew Schwartz
Tiffany Tsang
Jamie Upham
Lee VanderLinden
Morgan A. Wilson
Jacob B. Wolk
Esther Zolotova
Eduardo Gonzalez, Lawyering Fellow
Thomas Duquette, Lawyering Fellow
Mason Hortz, Advising Attorney
Alfreda Russell, Research Librarian
Brittney Strojny, Legal Librarian Intern
Susan Maze-Rothstein, Faculty Supervisor

ACKNOWLEDGMENTS

We would like to thank the following people for their invaluable assistance and support in completing this project.

Eduardo Gonzalez
Thomas Duquette
Susan Maze-Rothstein
Mason Kortz
Sarah Cortes
Andrew Lewman
Andrea Matwyshyn
Alfreda Russell
Brittney Strojny
Jootaek Lee
Frank Speiser

We would not have been able to complete this project without your input and appreciate the help.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Tor gives its users a means of protecting their privacy online. Current estimates indicate that there are approximately 2.5 million users of Tor around the world. Due to the evolving nature of laws regarding online activity, in some ways Tor is in legal limbo regarding the issues its users could face. This manual aims to discuss the legal implications of using online anonymity tools, such as the Tor Browser. In the process, it examines the current legal framework, different ways online privacy is threatened, and strategies to protect online-privacy tools from legal attacks. As the clients for this project include representatives from Tor Project, Inc. and the American Civil Liberties Union, this manual reflects the interrelationship between privacy, online anonymity, and the law.

Section 1 discusses under what major federal laws the government assumes its surveillance authority. It primarily focuses on the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA). The section lays out each statute's primary organizing principles, define what information each individual act protects, and the legal procedures the government must follow to acquire protected information. It considers the implications each act may have on Tor users. It closes with a constitutional analysis of some specific provisions.

Section 2 examines whether Tor falls under the scope of the ECPA or the Communications Assistance for Law Enforcement Act (CALEA). This issue is important to Tor because if found to be subject to the ECPA or CALEA, it could be obligated to disclose user information to law enforcement. Currently, Tor must be considered an Internet service provider (ISP) or communication service provider (CSP) to fall under the ECPA and CALEA requirements respectively. This is unlikely. However, the government could expand the ECPA

and CALEA definitions to include more than traditional CSPs and ISPs, and could even reach Tor.

Section 3 discusses the legality of using Mutual Legal Assistance Treaties (MLATs) to de-anonymize Tor users. MLATs are agreements between nations to coordinate judicial assistance in criminal matters. These treaties are the legal framework through which a nation may request evidentiary support in ongoing international criminal investigations and prosecutions. As such, MLATs provide the legal basis for the formulation and operation of Joint Investigation Teams. Joint Investigation Teams are comprised of international law enforcement agencies working together across jurisdictional lines to execute MLAT evidentiary requests. Procedural empowerments embedded in MLATs, together with the broad range of discretionary power given to joint investigation teams, permits the erosion of civil liberties in the interest of intra- and extra-territorial surveillance. Within this framework, MLATs can be used to legally de-anonymize Tor users.

Section 4 explores the third party doctrine and whether or not Tor could be considered a third party. The third party doctrine holds that people who voluntarily give information to third parties, such as banks, phone companies, Internet service providers (ISP), and email servers, have no *reasonable expectation of privacy*. This lack of privacy then allows the U.S. government to obtain information from the third parties without a judicial search warrant. The section consists of a general discussion of the third party doctrine and how it developed into what it is today, followed by an overview of the arguments and rationales of whether Tor could be subject to the third party doctrine. Most likely, Tor cannot be considered a third party for the purposes of the third party doctrine because users only disclose a limited amount of information to Tor by design, and because the users have a reasonable expectation of privacy in the information they

provide. Even if Tor was construed as a third party, there is proposed legislation that would effectively invalidate the doctrine.

Section 5 examines in further detail whether Tor falls under the scope of the CALEA. The CALEA was enacted in 1994 in response to the difficulty faced by law enforcement agencies in conducting electronic surveillance of communications using evolving digital technologies. This evolution undermined the traditional methods of lawful interception. The CALEA was adopted to clarify the duties of telecommunications carriers in aiding law enforcement in the interception of communications. The scope of the CALEA is constantly in flux because it expands as new telecommunications technology emerges. In managing its scope, three competing interests are at play: (1) the FBI is concerned with ensuring law enforcement's ability to surveil and intercept communications expeditiously; (2) the telecommunications industry has a strong interest in keeping compliance costs low and preserving its ability to innovate; and (3) privacy advocates are concerned with the level of government access and intrusion into private communications. While the CALEA does not currently apply to Tor, past applications indicate that the CALEA could be expanded to apply to Tor in the future.

Section 6 analyzes whether academic researchers at the University of Colorado violated the federal Wiretap Act by participating in the Tor network and capturing Tor user data. By examining the type of data governed by the Act and the Act's enumerated exemptions, the section concludes that the Colorado researchers did not violate the Wiretap Act. However, less scrupulous researchers or other researchers acquiring different types of Tor user data may fall within the Act's reach. Additionally, this section considers whether the Colorado researchers violated federal protocols for research on human subjects.

Section 7 explores the legality of operating a Tor relay as an individual and as an academic institution conducting research over the Tor network. Again there are an estimated 2.5 million users of Tor, with only a small fraction using it for illegal or illegitimate purposes. The harm created by those who utilize Tor for illegal purposes causes many relay operators to worry about prosecution, and ultimately to decide to no longer run relays. Overall, this section argues that running a Tor relay is legal. In deciding whether to run a relay, an academic institution must weigh the low risk of legal prosecution against the benefit of the research obtained by running a relay.

Section 8 discusses the constitutionality of anti-harassment laws like the updated Violence Against Women Act (VAWA). Since VAWA's enactment in 1994, online harassment and cyberstalking has become increasingly prevalent and difficult to combat. When viewed as part of the escalating cycle of violence that occurs in abusive relationships, online harassment and stalking can be a clear indication of an abusive relationship that could turn physically violent. Congress updated VAWA to include language that specifically criminalizes cyberstalking. This revision raises concerns among free speech advocates who feel that the language is overly broad. Section 8 explores recent federal cases that examine the constitutionality of cyberstalking laws like the one in VAWA, and argues that they are constitutional. The section further discusses how the language of the laws could be improved to ease the concerns of free speech advocates while also protecting victims of online abuse.

Section 9 discusses how to handle misused technology that also provides important societal benefits. Despite the misuse of Tor by some of its users, this section argues that Tor should not be banned. Certain technologies provide such significant social benefit that it would be a mistake to ban them. The existence of Tor is not the problem. The types of abuses that occur

on the Tor network existed prior to Tor's creation. The government has made it their policy to promote the Internet. The section argues that the anonymity that Tor provides enables a freer form of speech when using the Internet and furthers the government's goals. Instead of banning Tor, Congress should adopt different regulations that deter people from misusing Tor. Lastly, the section describes the *PinkMeth* lawsuit, and how Tor can defend itself against similar lawsuits.

Section 10 first discusses the development of online harassment as a legal concept and as a target for state legislative action. The section compares state laws that specifically address online harassment and those that do not. Second, the section examines the possibility of the use of Tor as a basis for creating enhanced penalties for users undergoing criminal prosecution. The section draws an analogy between enhanced penalties for crimes committed anonymously and enhanced penalties for crimes committed anonymously while using Tor. The likelihood of current legislation creating enhanced penalties is slim. However, future legislation may create enhanced penalties in sentencing for Tor use.

Finally, Section 11 discusses various issues raised by the recent Backpage lawsuits. It describes the arguments Backpage used to defend itself and argues that Tor could use similar arguments in a potential lawsuit by claiming immunity under the Communications Decency Act. Additionally, Tor could argue it is protected under the First Amendment because of its lack of scienter. The section then argues that shutting down technologies like Backpage or Tor will not have a meaningful effect on reducing criminal activity.

Section 1

A Review of Surveillance Law

Question Presented: Under what laws can the U.S. government conduct surveillance of U.S. citizens and non-U.S. citizens, both in U.S. territory and abroad? Are these laws constitutional?

INTRODUCTION

In the summer of 2013, Edward Snowden used Tor to anonymously disclose documents that revealed secret government surveillance programs to the public.[1] The leaks fed public awareness about the breadth of government surveillance and ignited debates on the proper limitations of government privacy intrusions.[2] This section will discuss which laws allow the government to conduct surveillance, including the following:

- The Electronic Communications Privacy Act (ECPA), enacted in 1986, includes the Wiretap Act, the Pen Register Act, and the Stored Communications Act[3]
- The Foreign Intelligence Surveillance Act (FISA), passed in 1978 and amended in 2008[4]
- The Communications Assistance for Law Enforcement Act (CALEA), passed in 1994[5]
- Mutual Legal Assistance Treaties (MLATs)[6]
- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, hereinafter referred to as "the Patriot Act"), passed in 2001[7]

This section examines the current statutory scheme, and also covers proposed legislation. It also discusses some surveillance programs that have come to light. It examines some challenges to the constitutionality of specific provisions of the ECPA and the FISA. In this and

[1] Klint Finley, *Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA,* WIRED MAGAZINE (April 14, 2014, 6:30 AM), http://www.wired.com/2014/04/tails.
[2] Matt Sledge, *The Snowden Effect: 8 Things That Happened Only Because Of The NSA Leaks*, HUFFINGTON POST (June 5, 2014, 7:31 AM), http://www.huffingtonpost.com/2014/06/05/edward-snowden-nsa-effect_n_5447431.html.
[3] 18 U.S.C. §§ 2510 - 2522, 2701–2712, 3121-3127 (2013).
[4] 50 U.S.C. ch. 36 § 1801 *et seq.* (2010).
[5] 47 U.S.C. §§1001-1010 (2014).
[6] U.S. CONST. art. VI, cl. 2.
[7] 115 Stat. 272 (2001).

later sections, this manual positions Tor in the debate as a privacy-protecting tool, keeping in mind legal measures that may undermine its effectiveness.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 1986

The following section begins by discussing the ECPA's primary organizing principles and identifying who is subject to its protections, and who is not. It then addresses the three individual acts that comprise the ECPA: the Wiretap Act, the Pen Register Act, and the Stored Communications Act. The Wiretap Act governs the contents of communications in transit, the Stored Communications Act governs stored communications, and the Pen Register Act governs the use of pen register and trap and trace devices. It defines what information each individual act protects, the legal procedures that the government must follow to acquire information that is otherwise protected, and reviews the implications each act may have on Tor users. It then introduces proposed legislation. This section closes with a constitutional analysis of specific provisions of the Stored Communications Act because it has been the most debated and questioned.

The ECPA Framework

Congress enacted the ECPA in 1986, at a time when the Internet was relatively inaccessible and technology was much less sophisticated.[8] The ECPA amended the original Wiretap Act, and implemented the Stored Communications Act (SCA) and the Pen Register Act (PRA). As previously stated, the Wiretap Act governs the contents of communications in transit, the Stored Communications Act governs stored communications, and the Pen Register Act governs the use of pen register and trap and trace devices. As a whole, the ECPA outlines

[8] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

procedures for conducting government surveillance of individuals within the United States. In 2001, the Patriot Act made significant amendments to key provisions of the ECPA.

The ECPA is structured around two primary categorical distinctions: (1) between communications in transit and stored communications, and (2) between content and non-content information.[9] In defining communications "in transit," the court has held that interception of communications must occur at the time of transmission.[10] The category of communications in transit includes interception of transient "packets" that are part of the transmission process itself.[11] Thus, intercepted transient packets will not be considered "stored information."[12] In the ECPA, information in transit is primarily subject to the Wiretap Act, while information in storage is subject to the Stored Communications Act. The distinction between communications in transit and stored communications accounts for different legal protections.

The content/non-content differentiation is arguably more complex and uncertain. Content is defined as "information concerning the substance, purport, or meaning of that

[9] 18 U.S.C. §§ 2510 - 2522, 2701–2712, 3121-3127 (2013).
[10] United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003).
[11] United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005).
[12] "The Internet is a packet-based network. An individual transmission is broken into chunks called packets. Each packet is sent separately from the sender to the recipient, often over totally different routes depending on network traffic at any given millisecond. The packets travel across a number of public networks that are often controlled by parties unrelated to the sender, the recipient, or their respective Internet Service Providers (ISPs). Once packets arrive at their destination, they are reassembled by the recipient. Internet communication through packets is made possible using a set of protocols called Transmission Control Protocol/Internet Protocol. Each computer on the Internet has an Internet Protocol (IP) address - four numbers from 0 to 255 with periods between them. Although most users are more familiar with domain names (e.g., georgetown.edu) than IP addresses, computers actually translate domain names into IP addresses (using a system called the Domain Name System (DNS)) before communicating over the Internet. Once a computer has done this, when a message is sent from one computer to another, the sending computer uses TCP/IP to break each message into packets, and puts a "packet header" at the beginning of the content portion (called the "payload") of each packet. This header indicates, among other things, the source IP address, the destination IP address, a packet number (for help during reassembly) and what kind of message is being sent (e-mail, Web browsing, instant message, etc.). As each packet moves from computer to computer along its route, computers at each location (called routers) read the packet headers to determine where to send the packet next. At the destination computer, TCP/IP is used again to remove the packet headers and reassemble the packet." Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1330 (2004).

communication."[13] Some information, like the body of an email, clearly falls into the category of "content." Similarly, data such as the timestamps of communications is widely accepted as non-content information.[14] Other sources of data, like the names of email attachments, are not so easily categorized.[15] The statutory language does not draw a definite line, nor has case law.[16] The line is even less definite when one considers the information that an accumulation of non-content data can reveal. Enough non-content data about an anonymous individual can reveal patterns, or "fingerprints" that can help to identify a person.[17] Another term for this phenomenon is the mosaic theory of surveillance.[18]

Who does the ECPA protect?

The protections of the ECPA extend to all information within the United States, regardless of an individual's citizenship status.[19] It is unclear, however, to what extent the ECPA applies to information abroad, if at all. It has been held that the ECPA does not protect foreign interception of communications abroad, even if that information was at one point routed through

[13] 18 U.S.C. § 2510(8) (2013).
[14] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1331(2004).
[15] *Id.*
[16] *Id.*
[17] Mike Masnick, *Anyone Brushing Off NSA Surveillance Because It's 'Just Metadata' Doesn't Know What Metadata Is,* TECHDIRT (July 18, 2013, 11:24 AM) https://www.techdirt.com/articles/20130708/01453123733/anyone-brushing-off-nsa-surveillance-because-its-just-metadata-doesnt-know-what-metadata-is.shtml.
[18] Orin Kerr, *Two district courts adopt the mosaic theory of the Fourth Amendment*, WASHINGTON POST (December 18, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/18/two-district-courts-adopt-the-mosaic-theory-of-the-fourth-amendment/.
[19] Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726 (9th Cir. 2011). (Suzlon Energy Ltd. demanded that Microsoft Corp. produce documents from the email account of Rajagopalan Sridhar, an Indian citizen imprisoned abroad. Sridhar's emails were stored on US servers. Court held that Sridhar was entitled to the protection the ECPA).

the US.[20] Current litigation is underway to decide if the ECPA applies to information that is stored abroad that is owned by US companies.[21]

The Wiretap Act

Congress originally enacted the Wiretap Act[22] in 1968 and included provisions that outlined protections for radio and wire communications.[23] The ECPA amended the Wiretap Act to extend protections to electronic communications.[24] As a whole, it prohibits intentional interception, use, or disclosure of the contents of communications that are "in transit," unless law enforcement has been granted a warrant or a statutory exception applies.[25] There are several exemptions, some of which will be explored in Section 6.

An application for a warrant can be filed if interception may provide or has provided evidence of any of the crimes listed in 18 USC § 2516, which includes anything from bribery at sports games to drug-related offenses.[26] The application must be fairly specific. It must include, among other things, the identity of the target (if known), the reasons for the warrant, a description of the kind of communication that is to be compelled, and a timeframe for interception.[27]

---

[20] "Because the alleged interceptions and disclosures occurred in [China] the ECPA does not apply to them, even if the communications, prior to their interception and disclosure, traveled electronically through a network located in the United States." Zheng v. Yahoo! Inc., No. C-08-1068 MMC, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009).
[21] Brief for Anthony J. Colangelo as Amici Curiae Supporting Appellant, Microsoft Corp. v. United States, No. 14-2985, Document 81 (2nd Cir filed Dec. 15, 2014), *available at* https://www.eff.org/files/2014/12/15/colangelo_microsoft_ireland_second_circuit_amicus_brief.pdf.
[22] Also known as Omnibus Crime Control and Safe Streets Act of 1968.
[23] Samantha L. Martin, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 450 (2006).
[24] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1561 (2004).
[25] 18 U.S.C. § 2511(1) (2008).
[26] 18 U.S.C. § 2516 (2012).
[27] *Id.*

A judge can grant a warrant upon a showing of probable cause that (1) the target is committing, has committed, or is about to commit the enumerated crime; (2) that interception will provide the particular communications sought; (3) the targeted facilities are commonly used by the alleged offender or are being used in connection with the offense; and (4) normal investigative procedures have been tried and have failed.[28] A judge can only issue a warrant for a target in the judge's district.[29] Notice is provided to the targets after the expiration of the order, although significant delays are possible.[30] If information has been surreptitiously intercepted without a warrant, the information may be suppressed in any judicial or administrative proceeding.[31] Overall, it is unlikely that law enforcement would be able to wiretap Tor users under the ECPA. It would be very difficult to establish the high degree of precision required for a wiretap warrant since the location of users is hidden. However, a proposed amendment to rule 41(b) of the Federal Rules of Criminal Procedure could make it much more likely for Tor users to be targeted under the Wiretap Act.

Proposed Amendments to Rule 41

The Federal Rules of Criminal Procedure describe procedural rules used in criminal trials. The rules control many aspects of criminal trials and investigations, such as when grand juries can be summoned.[32] The Rules are written by non-legislators, though Congress has the power to reject proposed rules or amendments. In the amendment process, there is also a time for public comment.

---

[28] The proposed change to rule 41 does not seek to change this requirement. Reena Raggi, *Report of the Advisory Committee on Criminal Rules*, JUD. CONF. U.S. at 325 (2014), http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf page 325.
[29] FED. R. CRIM. P.41(b)(6)(A).
[30] 18 U.S.C. § 2518(8)(d) (1998).
[31] 18 U.S.C. § 2518(10)(a)(1) (1998).
[32] FED. R. CRIM. P. 6.

Rule 41(b) controls the jurisdictional scope of a warrant. The Rule in its current form prevents a judge from issuing a warrant unless the target is known to be located within their district.[33] The proposal would add a provision to the procedure for warrants to the existing 41(b)(6):

> 41(b)(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[34]

The proposal also includes changes to Rule 41(f)(1)(C) to allow for only reasonable efforts to provide notice.[35] The current rule states:

> The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

The authors of the proposal list the use of proxy servers and anonymizing software as reasons for the changes. They argue that the condition of knowing the specific location of a computer to be searched should be relaxed in response to changing technology.[36] If accepted by all relevant committees and the Supreme Court, the change will be effective on December 1, 2016.[37]

The change would make it easier to use Network Investigative Techniques (NITs), a surveillance method that involves the remote access of a computer to install malicious software,

---

[33] Reena Raggi, *Report of the Advisory Committee on Criminal Rules*, JUD. CONF. U.S. (2014). http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.
[34] *Id*. at 338.
[35] *Id*. at 327.
[36] *Id*. at 325.
[37] Reena Raggi, *Report of the Advisory Committee on Criminal Rules*, JUD. CONF. U.S. (2014). http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.

because the LEO would not have to specify a location in applying to use a NIT.[38] By not having to specify a location, the LEO does not have to take steps to specifically identify the target in its investigative measures. When applying for a warrant for a NIT, the LEO could more easily apply for more expansive malware. Malware, a type of software, can be used for many purposes, like capturing keystrokes or turning on a webcam.[39] NITs could have a disproportionate effect on Tor users since Tor would likely fall under the proposed changes to 41(b)(6)(A): "when information is concealed through technological means."[40] Specifically, so-called "watering hole attacks" can be used to surveil many users of Tor. This describes a process wherein a LEO places a malware program on any website, especially those accessed through Tor hidden services. When an individual accesses that website, the malware software is downloaded on their device.[41]

Operation Torpedo is a mass data collection program that utilized a NIT.[42] The FBI developed a NIT to track IP addresses that visited a certain website. However, NIT malware can be used as a "driftnet instead of a fishing line," meaning it does not necessitate a targeted attack.[43] The NIT in Operation Torpedo was developed in a child pornography case, but the American Civil Liberties Union (ACLU) argues that they could be a step toward broader use.[44]

---

[38] Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY (September 16, 2014, 9:10 AM), http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance.
[39] Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired, (Aug. 8, 2014), http://www.wired.com/2014/08/operation_torpedo/.
[40] Reena Raggi, *Report of the Advisory Committee on Criminal Rules*, JUD. CONF. U.S. (2014). http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.
[41] Watering hole attacks work by placing a link or attachment connected to a specific website. When an individual accesses that website, the malware software is downloaded on their device. That software can act as a keystroke capture, or another method of information gathering that the LEO can use.
[42] Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired, Aug. 8, 2014, http://www.wired.com/2014/08/operation_torpedo/.
[43] *Id.*
[44] *Id.*

The application for the warrant for Operation Torpedo described Tor in detail.[45] The application also detailed the combined use of administrative subpoenas and MLATs in the investigation.[46] The explicit use of malware has resulted in dozens of arrests and months of data gathering.[47] For the implementation of Operation Torpedo, the LEO needed to include a section in the application that connected Aaron McGrath to "Bulletin Board A."[48] This section specified the ties from an individual to the targeted website. The LEO applied for the warrant in Nebraska because of this connection. Had the rule change already been implemented, the LEO in Operation Torpedo would not have needed to go to a Nebraska judge to obtain a warrant for a NIT; the LEO might not have needed to specify the location of Aaron McGrath at all. The rule change would grant a LEO more flexibility in such a section in their application for a warrant, making the application process easier. It would allow a LEO to apply for a NIT warrant even when the location of the targets is unknown or outside of the judge's jurisdiction.

In the public comments on the proposed amendment, the ACLU, Electronic Frontier Foundation (EFF), and other organizations submitted memoranda sharing their concerns surrounding the changes.[49] The ACLU expressed concerns with the FBI's use of malware. They maintain that the expanded authority to use remote access searches would give the FBI too much

[45] Application for a Search Warrant, In the Matter of the Search of Computers that Accessed the Website "Bulletin Board A," Doc. 8:13-cr-00108-JFB-TDT, Doc. 123-1 p.10 *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1261620/torpedo-affidavit.pdf.
[46] *Id.*
[47] Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired, Aug. 8, 2014, http://www.wired.com/2014/08/operation_torpedo/.
[48] Application for a Search Warrant, In the Matter of the Search of Computers that Accessed the Website "Bulletin Board A," Doc. 8:13-cr-00108-JFB-TDT, Doc. 123-1 p.24 *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1261620/torpedo-affidavit.pdf.
[49] Public Hearing on Proposed Amendments to the Federal Rules of Criminal Procedure, JUD. CONF. ADVISORY COMM. ON CRIM. RULES (2014), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2014-11-Criminal-Public-Hearing-Testimony.pdf.

power to access individuals' data and is a dangerous proposition that can erode Internet privacy.[50] The constitutionality of the proposed change is already in question. The ACLU argues:

> What looks like a procedural change actually creates a new substantive power: to use zero-day exploits, malware, spyware, and other software packages to circumvent privacy-protective proxy services, including at least one, Tor, which was created by the US government, and continues to receive US government funding.[51]

The ACLU insists that any change should be pursued legislatively, rather than through procedural rule revisions. The revision process is controlled by the judicial branch, whereas statutory changes are made by the legislature.[52] The ACLU also identifies a potential unreasonable search issue concerning the lack of required particularity and constitutional concerns with the relaxed notice requirement.

Pen Register Act

The Pen Register Act (PRA) governs the real time interception of non-content information acquired through the use of pen register and trap and trace devices.[53] The first iteration of the PRA defined a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed."[54] The PRA defined a trap and trace device as "a device which captures the incoming electronic or other impulses which identify the originating number."[55] Essentially, LEOs used pen registers to collect outgoing phone numbers

---

[50] Public Hearing on Proposed Amendments to the Federal Rules of Criminal Procedure, JUD. CONF. ADVISORY COMM. ON CRIM. RULES (2014), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2014-11-Criminal-Public-Hearing-Testimony.pdf.
[51] *Id.* at 16.
[52] One reason the ACLU would prefer the change to go through the legislature is that it is structurally more responsive. The legislative process is commonly referred to a majoritarian, or representative process, whereas the judicial branch is more isolated. UNITED STATES HOUSE OF REPRESENTATIVES, *Branches of Government*, http://www.house.gov/content/learn/branches_of_government/. (last visited Mar. 8, 2015).
[53] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1322, 1327 (2004).
[54] 18 U.S.C. § 2510 (2002).
[55] *Id.*

placed from a specific telephone line, while they used trap and trace devices to capture the incoming calls on a specific telephone line.[56] The Patriot Act amended the PRA to extend their use to the Internet context, which will be discussed below.[57] A court must authorize the installation of such devices; however, court approval is more symbolic than substantive.[58] If a government attorney certifies that the "information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation," the statute mandates that a court authorize it.[59] Unlike content obtained through the Wiretap Act, information acquired through unauthorized pen registers is not protected by the exclusionary rule,[60] nor is there a requirement that the target of a pen register be notified.[61]

The relaxed standards are largely a reflection of Supreme Court jurisprudence. In *Smith v. Maryland,* the Court held that there is no constitutionally recognized privacy interest for the telephone numbers intercepted by pen register or trap and trace devices.[62] The ruling held that only the content of a conversation should receive full constitutional protection under the Fourth Amendment right to privacy.[63] Since pen registers do not intercept conversations, they do not pose as much of a threat to this right.[64] Underlying this understanding is the "third party doctrine" which will be explained further in Section 4.

---

[56] 18 U.S.C. § 2510 (2002).
[57] 50 U.S.C . § 1861 (2014).
[58] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1348 (2004).
[59] 18 USC § 3123(a)(1) (2001).
[60] The exclusionary rule allows the defense counsel to move the court to suppress evidence that has be illegally obtained.
[61] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1329 (2004).
[62] *Id.*
[63] *Id.*
[64] *Id.*

Section 216 of the Patriot Act amended the Pen Register Act.[65] Most importantly, it redefined both devices. Now a pen register is defined as

> A device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication[66]

while a trap and trace device is defined as

> A device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.[67]

The amendments essentially extended *Smith* by analogy to Internet pen registers. The amendments did not consider the important technical differences between telephone signaling and Internet transmission.[68] The Supreme Court, however, has never actually ruled on whether pen register use on the Internet is constitutional. The Patriot Act also authorized nationwide pen register orders and mandated reports on the use of government-installed pen registers.[69]

Exactly what a pen register order can obtain is unclear. The statute does not explain how to distinguish between content and routing information.[70] Different categories of information are not clearly delineated as content or routing, with little definitive direction from the judicial

---

[65] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1327, 1331(2004).
[66] 18 U.S.C. § 3127(3) (2001).
[67] 18 U.S.C. § 3127(4) (2001).
[68] "*Smith* relied on the fact that telephone users disclosed discrete signaling information to third parties, and this information could be easily intercepted using technology that would not also reveal the content of conversations...On the Internet, there is no longer such a clear line to draw. Users disclose both content and routing information, in exactly the same technical manner, to an enormous number of third parties. The exact same computers read both content and routing information, which are frequently intermingled within packets." Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1327, 1335 (2004).
[69] *Id.*
[70] *Id.* at 1337.

branch and limited insight on government policies and practices.[71] The government considers the "To" and "From" email fields to be routing and the "Subject" fields of an email to be content.[72] The incoming and outgoing Internet Protocol (IP) addresses by the subject Internet account are also considered routing.[73] In addition, the courts have ruled that search terms in a URL classify as content under the Wiretap Act.[74] However, there is still uncertainty about how other information, like names of email attachments, may be legally classified.[75] There are additional problems associated with developing technology that can reliably collect only non-content information. That leaves the public to defer to the government's good faith.[76]

In general, the government will usually request pen register information from an Internet service provider (ISP).[77] In cases where that may fail, it can look to the FBI's DCS1000 system.[78] DCS1000 is,

> a software package running on a computer that is placed directly on an Internet line at an ISP's office. It sorts through all packets on this line (including many belonging to non-targets using the same ISP line) and saves only packets that meet its filtering criteria, which should be set to match the court order authorizing surveillance.[79]

The case of "hacktivist" Jeremy Hammond illustrates how using Tor without appropriate overall security precautions can make some individuals vulnerable to surveillance in limited

---

[71] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1327, 1337(2004).
[72] *Id.*
[73] Deborah F. Buckman, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. FED. 2D 537 (2006).
[74] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1327, 1330 (2004). (citing *In re* Pharmatrakir. 2003).
[75] *Id.*
[76] *Id.*
[77] *Id.* at 1333.
[78] Previously known as the Carnivore system.
[79] Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1327, 1334 (2004). (citing *In re* Pharmatrakir. 2003).

circumstances.[80] Hammond's leaking of other personal information made him vulnerable to an intersection attack, using Tor timing correlation and Tor traffic correlation. In Hammond's case, the FBI worked closely with an informant, the well-known Sabu, who was in contact with Hammond. They parsed through all the communications between Hammond's online alias and the informant, Sabu, to identify Hammond as a suspect.

At the time of identification, the LEO did not know his name; they only knew the usernames he used online and the home address where his communications were originating. At that point, the FBI stationed themselves outside of his home to monitor the WiFi network. They discovered the Media Access Control (MAC) addresses of each device connected to the network.[81] Most of the time, there was only one device on the network: an Apple computer. The informant learned that Hammond had an Apple computer. The FBI then installed a pen register device to see what IP addresses the Apple computer was visiting. They discovered it was connecting to IP addresses known to be websites accessed through Tor.[82] They compared the times the Apple computer accessed Tor with the times Hammond left the building to officially identify him by name.[83] The government charged him with one count of violating the Computer Fraud and Abuse Act.[84] The court sentenced him to ten years in prison. The Hammond case illustrates that LEOs can use pen registers to deduce when a computer is accessing Tor. In

---

[80] *The Other Bradley Manning: Jeremy Hammond Faces Life Term for WikiLeaks and Hacked Stratfor Emails,* DEMOCRACY NOW! (December 27, 2012). http://www.democracynow.org/2012/12/27/the_other_bradley_manning_jeremy_hammond. (Computer hacker Jeremy Hammond, an alleged member of the group "Anonymous" was charged with hacking into the computers of the private intelligence firm Stratfor and turning over some five million emails to the whistleblowing website WikiLeaks)

[81] MAC addresses refer to the unique identifier attached to a device on a network. Interview with Frank Speiser, President, SocialFlow, Inc. (Feb. 2, 2015).

[82] Nate Anderson, *Stakeout: how the FBI tracked and busted a Chicago Anon,* ARS TECNICA (Mar 6, 2012, 10:30 PM). http://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/2.

[83] This kind of vulnerability is called an intersection attack, using timing correlation and traffic correlation.

[84] *Jeremy Hammond Sentenced to 10 Years in Prison for Cyber-Activism,* DEMOCRACY NOW! (November 15, 2013), http://www.democracynow.org/blog/2013/11/15/jeremy_hammond_sentenced_to_10_years_in.

limited circumstances, where no other users are accessing Tor, that very access can be an identifying act. It should serve to caution users that Tor does not provide complete anonymity.

Stored Communications Act

The SCA formally prohibits unauthorized access to an individual's stored information, including opened emails.[85] The SCA applies to information that is "stored," which is written to juxtapose information that is "in transit" and governed by the Wiretap Act.[86] This distinction is under debate, and might be modified in proposed legislation, discussed below.[87] In situations where the Wiretap Act and the Stored Communications Act might intersect, the courts have held that only one of the acts should apply.[88] The government cannot authorize surveillance under both, or a combination of the two.[89]

Acquiring Non-content under the SCA

The SCA authorizes various legal mechanisms that have less stringent requirements than warrants, such as administrative subpoenas and d orders (authorized under section 2703(d) of the statute).[90] The lesser requirements also depend on the difference between the content and non-content framework that underlies all of the ECPA. Under the SCA, authorized agencies can access two kinds of non-content information: customer records and transactional records.[91] To obtain customer records, LEOs use administrative subpoenas. To obtain transactional records, LEOs must use a d order.

---

[85] 18 U.S.C. § 2703(a) (2009).
[86] 18 U.S.C. § 2511 (2009). S*ee also* 18 U.S.C. § 2703 (2009).
[87] Electronic Communications Privacy Act Amendments Act of 2013, S.607, 113th Cong. (2013).
[88] United States v. Herring, 993 F.2d 784, 788 n. 4 (11th Cir.1993).
[89] Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 450 (C.D. Cal. 2007).
[90] 18 U.S.C. § 2701 (2014).
[91] Dozens upon dozens of agencies, such as the FDA, are authorized by federal statute to use administrative subpoenas. *Report to Congress on the Use of Administrative Subpoena Authorities of Executive Branch Agencies and Entities,* U.S. DEPARTMENT OF JUSTICE, http://www.justice.gov/archive/olp/rpt_to_congress.pdf.

Administrative Subpoenas

Administrative subpoena authority describes the power of authorized agencies to order a recipient to produce documents or testimony to the agency.[92] Administrative subpoenas are self-issued without judicial oversight when information sought is "relevant" to an ongoing investigation, which is a low standard in comparison to other surveillance methods. The courts can get involved if the recipient of an administrative subpoena requests judicial review to modify or quash the subpoena, or if an administrative agency initiates judicial enforcement.[93] Historically, courts have granted broad deference to agencies.[94] The government maintains that federal governmental entities would be unable to properly fulfill their duties and responsibilities without administrative subpoena power.[95]

The SCA authorizes the use of an administrative subpoena in the Internet context to compel a provider to produce customer records[96] and to obtain the contents of a stored communication, if it has been opened for at least 180 days.[97] Only those agencies granted prior statutory authority can issue administrative subpoenas. An agent can serve an administrative subpoena on an ISP and compel it to hand over all the records associated with an individual IP address, including a name, address, records of session times and durations, temporarily assigned network address, and means and source of payment.[98] The court can grant an agency the authority to delay notice to the individual who is the subject of a subpoena.[99] Administrative

[92] Definition from U.S.DOJ Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities. *Id*. at 6.
[93] *Id*. at 7.
[94] Definition from U.S.DOJ Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities. *Id*. at 8-9.
[95] *Id*. at 6.
[96] U.S.C. § 2703(c)(2)(F) (2009).
[97] U.S.C. § 2703(b)(1)(B) (2009).
[98] U.S.C. § 2703(c)(2) (2009).
[99] 2703(B)(1)(b)(ii), as demonstrated in United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).

subpoena use is estimated to be very extensive.[100] Some civil liberties advocates have begun to question their constitutionality.[101]

Administrative subpoenas in the foreign intelligence context are called "National Security Letters" (NSL). They can be, and usually are, served with a "gag order" prohibiting the recipient of the NSL from disclosing that the FBI sought information from them.[102]

D orders

The remainder of non-content information is acquired with a d order. D orders derive their name from their statutory authority, Section 2703(d). D orders are commonly used to obtain "transactional" information, which includes the websites a person has visited and the email addresses of people with whom the individual has corresponded.[103] Transactional information can also include:

> 1. records of user activity for any connections made to or from the Account, including date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
> 2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
> 3. correspondence and notes of records related to the account(s).[104]

In the application for a d order, the LEO can request delayed notice. If granted, the target of the d order will only become aware of its existence after the fact, if at all.

The ACLU challenged the application of a d order obtained against Twitter users who were affiliated with WikiLeaks.[105] The order asked for IP information, which would disclose the

---

[100] David Kravets, *We Don't Need No Stinking Warrant: The Disturbing Unchecked Rise of the Administrative Subponea,* WIRED (AUGUST 28, 2012, 6:00 AM), http://www.wired.com/2012/08/administrative-subpoenas/.
[101] Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED, (Aug. 8, 2014), http://www.wired.com/2014/08/operation_torpedo/.
[102] 18 U.S.C. § 2709 (c) (2014).
[103] The U.S. Internet Service Provider Association, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, U.S. Berkeley Technology Law Journal, 18 BERKELEY TECH. L.J. 945, 950-51. (2003).
[104] *In re* § 2703(d), 787 F. Supp. 2d 430, 435 (E.D. Va. 2011).

approximate physical locations of the individual's device, as well as identities of people with whom the Twitter users were communicating via private message.[106] The magistrate judge denied motions submitted by the ACLU to vacate the order on Twitter and to unseal the government's application for the order.[107] The d order withstood the challenge that the scope of the order was overly broad, as well as the claim that the information sought was private. As evidenced by this case, d orders are allowed to be far reaching, with more deference to the LEO's investigation. The U.S. government can conduct surveillance under the SCA in a way that can gather a great deal of information without the individual's ability to assert their right to privacy.

Proposed Legislation

As the SCA currently reads, if one keeps an unopened email more than 180 days, it is considered abandoned. LEOs only need a subpoena to access the content of abandoned emails.[108] If the email has been stored for less than 180 days, a LEO must obtain a probable cause warrant.[109] Different types of information, like timestamps and addresses, can be accessed under different authorities.

However, there is a bill in Congress now that would eliminate the 180-day distinction: the Electronic Communications Privacy Act Amendments Act of 2013. The proposed legislation would also prohibit service providers (third parties) from voluntarily releasing information to the government. It also proposes that the government be required to serve warrants on the individual,

---

[105] *In re* Application for a D Order, ACLU OF VIRGINIA, (last accessed March 8, 2015) https://acluva.org/7364/in-re-%C2%A72703d-orders/.
[106] *In re* § 2703(d), 787 F. Supp. 2d 430, 435 (E.D. Va. 2011).
[107] *In re* Application for a D Order, ACLU OF VIRGINIA, (last accessed March 8, 2015) https://acluva.org/7364/in-re-%C2%A72703d-orders/.
[108] 18 U.S.C. §2703(b)(1)(B)(i)(2014). Subject to United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
[109] 18 U.S.C. §2703 (a)(2014).

in addition to the ISP. If the ISP wants to communicate with the subscriber about the warrant, it must inform the LEO first. Still, a LEO could then request a delay of notification. This would amend Section 2705 as it currently exists. The S.B. 607 has been read and referred to the Committee on the Judiciary.[110]

Constitutionality of the SCA

The ECPA in its entirety has not and likely would not be facially challenged. The Wiretap Act is constitutional. It issues warrants under a standard of probable cause, as required by the Fourth Amendment.[111] Other provisions, however, merit more scrutiny. In particular, at least one federal court has held that 2703(b) of the SCA, which authorizes the acquisition of stored communications without a warrant, is unconstitutional.[112] Section 2703(b) of the SCA authorizing the use of administrative subpoena to obtain customer records and the ability to delay notice about the use of a surveillance mechanism are questioned, but unlikely to be invalidated. Section 2703(d) authorizing the use of d orders for transactional records is currently being reviewed.

Stored Contents without a Warrant

In *United States v. Warshak*, the Sixth Circuit ruled that the Fourth Amendment to the federal Constitution prevents law enforcement from obtaining stored email communications without a warrant based on a showing of probable cause. Accordingly, the court held that the provision of the SCA, 18 U.S.C. §§2701 et seq., a part of the ECPA, that permits warrantless

[110] There are sister bills in the house: Lofgren - Poe - DelBene, Online Communications and Geolocation Protection Act, H.R. 983.
[111] U.S. CONST. amend. IV: "[N]o Warrants shall issue, but upon probable cause."
[112] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

government access to certain stored emails after 180 days, is unconstitutional.[113] However, the judge allowed the evidence that was collected without a warrant in this specific case to be admissible "because the agents relied in good faith on provisions of the Stored Communications Act."[114] They further ruled that the SCA at large was not "conspicuously unconstitutional."[115] Going forward, LEOs cannot obtain email content without warrants in that jurisdiction because they would no longer be able to claim a good faith reliance.

Customer Records with an Administrative Subpoena

In 2012 *Wired* magazine argued that the use of administrative subpoenas had grown out of control in that they were issued too easily and too frequently.[116] The report relied primarily on anecdotal evidence. The actual use of administrative subpoenas cannot be corroborated because governmental agencies are not required to report how often they issue them.[117] However, some service providers have shared how many they have received,

> AT&T, the nation's second-largest mobile carrier, replied to a congressional inquiry in May that it had received 63,100 subpoenas for customer information in 2007. That more than doubled to 131,400 last year [2011]... By contrast, AT&T reported 36,900 court orders for subscriber data in 2007. That number grew to 49,700 court orders last year, a growth rate that's anemic compared to the doubling of subpoenas in the same period.[118]

If *Wired's* assertions are true, it is possible, though unlikely, to convince the court that the practice of over-issuing administrative subpoenas violates the Fourth Amendment right to

[113] United States v. Warshak, 631 F.3d 266, 290 (6th Cir. 2010).
[114] *Id.* at 274.
[115] *Id.* at 289.
[116] David Kravets, *We Don't Need No Stinking Warrant: The Disturbing Unchecked Rise of the Administrative Subponea,* WIRED (AUGUST 28, 2012, 6:00 AM), http://www.wired.com/2012/08/administrative-subpoenas/.
[117] *Id.*
[118] *Id.*

privacy. Court precedent leaves little room to argue that administrative subpoenas are unconstitutional because of broad deference previously granted to agencies.[119]

Courts have held that in contrast to warrants, subpoenas are "far less intrusive" and thus do not require a probable cause standard.[120] Courts have also explained that probable cause is not required because recipients can go to court to have them quashed.[121] Arguably, the reasoning does not properly consider that recipients of administrative subpoenas are generally third parties that are not directly implicated in investigations and thus not sufficiently motivated to challenge an administrative subpoena.[122] Nevertheless, courts have held that administrative subpoenas are only subject to a standard of "reasonableness" to comply with the Fourth Amendment.[123] Historically, when recipients have challenged administrative subpoenas, courts have been very deferential to agencies.[124]

Administrative subpoenas can be challenged at two points. A recipient, such as an Internet service provider, can request judicial review before they comply. Alternatively, the subject of an administrative subpoena, such as an individual or a corporation, can argue that the use of the administrative subpoena violated their constitutional right to privacy under the Fourth Amendment. To succeed in the latter constitutional challenge, a target would have to convince the court that they have a reasonable expectation of privacy in regards to their records. To demonstrate a reasonable expectation of privacy, a target must meet a two-pronged test: they must have a subjective expectation of privacy and that expectation must be objectively

---

[119] *Report to Congress on the Use of Administrative Subpoena Authorities of Exectuive Branch Agencies and Entities,* U.S. DEPARTMENT OF JUSTICE, 8-9, http://www.justice.gov/archive/olp/rpt_to_congress.pdf.
[120] United States v. Vilar, 2007 WL 1075041 (U.S. District Court for the Southern District of New York 2007).
[121] United States v. Bailey, 228 F.3d 341 (U.S. Court of Appeals for the 4th Circuit 2000).
[122] Susan Brennar, *Administrative Subpoenas and the 4th Amendment*, CYB3RCRIM3 (May 21, 2010, 10:22 AM), http://cyb3rcrim3.blogspot.com/2010/05/administrative-subpoenas-and-4th.html.
[123] *Report to Congress on the Use of Administrative Subpoena Authorities of Exectuive Branch Agencies and Entities,* U.S. DEPARTMENT OF JUSTICE, 8, http://www.justice.gov/archive/olp/rpt_to_congress.pdf.
[124] *Report to Congress on the Use of Administrative Subpoena Authorities of Exectuive Branch Agencies and Entities,* U.S. DEPARTMENT OF JUSTICE, 8-9, http://www.justice.gov/archive/olp/rpt_to_congress.pdf.

reasonable.[125]

Arguably, the public has come to assume that customer records are protected, and that agencies cannot routinely acquire that information with ease. Indeed, ISP actions in some way confirm this understanding. Google has stated "[ECPA] has failed to keep pace with how people use the Internet today. That's why we've been working with many advocacy groups, companies and others, through the Digital Due Process Coalition, to seek updates to this important law so it guarantees the level of privacy that you should reasonably expect when using our services."[126] Google and other ISPs been known to sometimes challenge orders they receive from agencies in order to protect customers' privacy and their own brand reputation.[127]

Courts, however, generally disagree. To convince the court that people have a reasonable expectation of privacy in regards to their records would require that the court overturn significant precedent. As noted in *Bynum*, "every federal court to address this issue has held that subscriber information provided to an Internet provider is not protected by the Fourth Amendment."[128] There is little indication that courts would accept this argument now. However, slowly, courts have been recognizing that the Internet is bringing about substantial changes that may require re-evaluation of existing practices.[129] It is possible that in the future, as life becomes increasingly

---

[125] Smith v. Maryland, 442 U.S. 735 (1979).

[126] *Google Transparency Report,* GOOGLE (last accessed March 7, 2015), https://www.google.com/transparencyreport/userdatarequests/legalprocess/#does_a_law_enforcement.

[127] "We review each request we receive before responding to make sure it satisfies applicable legal requirements and Google's policies. In certain cases we'll push back regardless of whether the user decides to challenge it legally." *Google Transparency Report,* GOOGLE (last accessed March 7, 2015), https://www.google.com/transparencyreport/userdatarequests/legalprocess/#does_a_law_enforcement.

[128] United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (quoting United States v. Perrine, 518 F.3d 1196 (U.S. Court of Appeals for the 10th Circuit 2008)).

[129] "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v Jones, 132 S.Ct. 945 (2012) (J. Sotomayor, concurring). "Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place… By obtaining access to someone's email, government agents gain the ability to peer deeply into [one's] activities." (United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010). Orin Kerr, *Two district courts adopt the mosaic theory of the Fourth Amendment*,

intertwined with the Internet and individuals leave more and more footprints online, courts may reconsider the privacy interest in online customer records.[130]

National Security Letters, a type of administrative subpoena, have been successfully challenged, specifically as to their use of gag orders.[131] The U.S. District Court of California declared the use of gag orders accompanying National Security Letters unconstitutional. It held that the prohibition of disclosure posed an impermissibly overbroad limitation on the First Amendment.[132] The government appealed and the trial is still underway.[133] While a complete prohibition on disclosure has, at least tentatively, been held as unconstitutional, the delay of notice has been upheld.

Delayed Notice

Delayed notice can give rise to a constitutional due process concern. Due process is protected under the Fourteenth amendment.[134] Privacy advocates argue that delayed notice allows the government to broadly collect information without oversight.[135] In *Warshak*, per the government's instructions, the ISP began archiving Warshak's emails without providing him notice.[136] He did not receive notice of the subpoena or of the order until a year later, after the

---

WASHINGTON POST (December 18, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/18/two-district-courts-adopt-the-mosaic-theory-of-the-fourth-amendment/.

[130] Two district courts have used the previously-discussed mosaic theory of surveillance in determining that the types of information that are collected for a long time can violate the Fourth Amendment. Orin Kerr, *Two district courts adopt the mosaic theory of the Fourth Amendment*, WASHINGTON POST (December 18, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/18/two-district-courts-adopt-the-mosaic-theory-of-the-fourth-amendment/.

[131] *In re* National Security Letters, Order Granting Motion to Set Aside NSL Letter. No. C 11-02173 SI.

[132] *In re* National Security Letters, Order Granting Motion to Set Aside NSL Letter. No. C 11-02173 SI.

[133] *National Security Letters are Unconstitutional,* Federal Judge Rules. ELECTRONIC FRONTIER FOUNDATION. Mar. 15, 2013. https://www.eff.org/press/releases/national-security-letters-are-unconstitutional-federal-judge-rules.

[134] U.S. Const. amend. XIV, § 1, cl. 4.

[135] *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, (last accessed on March 5, 2015) https://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa.

[136] United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).

contents of 27,000 emails were revealed.[137] LEOs defend their ability to delay notice because it prevents the subject from altering or ceasing their communications.[138] The DOJ also identifies delayed notice as a tool that "gives law enforcement time to identify the criminal's associates, eliminate immediate threats to our communities, and coordinate the arrests of multiple individuals without tipping them off beforehand."[139]

In 1979, the Supreme Court upheld the constitutionality of delaying notice of a warrant:[140]

> The Supreme Court has held the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant. The Supreme Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." In fact, the Court stated that an argument to the contrary was "frivolous."[141]

The House's proposed legislation would maintain the phenomenon of delayed notice, thereby continuing the practice of data collection without transparency.[142]

D orders

In *United States v. Davis*, a LEO used a d order to obtain Davis' location off of his cell phone signal.[143] The LEO used the information to place Davis at the scene of several crimes, for which he was convicted.[144] Davis appealed, arguing that the acquisition violated his Fourth

---

[137] United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).
[138] *Dispelling Some of the Major Myths about the USA PATRIOT Act,* US DEPT. OF JUSTICE (last accessed March 5, 2015) http://www.justice.gov/archive/ll/subs/u_myths.htm.
[139] *Id.*
[140] Dalia v. United States, 441 U.S. 238 (1979).
[141] *Dispelling Some of the Major Myths about the USA PATRIOT Act,* US DEPT. OF JUSTICE (last accessed March 5, 2015) http://www.justice.gov/archive/ll/subs/u_myths.htm.
[142] "In general.--A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity." H.R.283, 114th Cong. (2015) Electronic Communications Privacy Act Amendments Act of 2015.
[143] United States v. Davis, 754 F.3d 1205 (11th Cir. 2014).
[144] *Id.*

Amendment right to privacy.[145] Initially, the court sided with Davis. Since then, however, the court vacated the ruling and the case will be reheard *en banc*.[146]

FOREIGN INTELLIGENCE SURVEILLANCE ACT, 1978

The section that follows outlines the main purpose of the Foreign Intelligence Surveillance Act. It reviews procedures for conducting surveillance. Different procedures and protections exist depending on the intended target for surveillance and their suspected location. Next, the section discusses the most significant amendments made to the FISA via the Patriot Act and the FISA Amendments Act of 2008. Subsequently, it explores FISA-approved surveillance programs that have been leaked. The section closes with a discussion of the constitutionality of certain provisions of the FISA.

Overview of the FISA

The FISA, first authorized in 1978 and amended in 2008, details how and against whom the government can conduct electronic surveillance for the purpose of foreign intelligence.[147] It created special courts called Foreign Intelligence Surveillance Courts (FISCs) that operate under great secrecy to review applications for surveillance.[148] Applications can be submitted to surveil U.S. persons or non-U.S. persons, in the U.S. and internationally. U.S. persons are defined as citizens or permanent residents of the United States.[149] Different procedures are proscribed depending on who is targeted and their suspected location.

[145] United States v. Davis, 754 F.3d 1205 (11th Cir. 2014).
[146] United States v. Davis, 573 Fed. Appx. 925 (11th Cir. 2014).
[147] 50 U.S.C. ch. 36 § 1801 *et seq.* (2010).
[148] 50 U.S.C. §1803(a).
[149] 50 U.S.C. §1801(i).

Section 1804: Non-U.S. Persons

When targeting a non-U.S. person under Section 1804, a federal officer, after obtaining the Attorney General's approval, must submit an application to the FISC.[150] The federal officer must certify that a significant purpose of the surveillance is to obtain foreign intelligence.[151] Foreign intelligence information is defined broadly to include information concerning foreign affairs and national defense.[152] Prior to the Patriot Act, officers had to certify that foreign intelligence gathering constituted the primary purpose of the surveillance.[153]

In addition, the application must include, among other things: (1) the identity of the target; (2) the information relied on by the government to demonstrate that the target is a "foreign power" or an "agent of a foreign power;" (3) evidence that the place where the surveillance will occur is being used, or is about to be used, by the foreign power or its agent; (4) the type of surveillance to be used; and (5) a proposed plan to minimize the chance of targeting a U.S. person.[154] The presiding judge will then approve the application if there is probable cause to believe that the target is a foreign power or agent of a foreign power and the targeted facilities are being used or about to be used by a foreign power or agent of foreign power.[155] This is contrasted with the Wiretap Act warrants, where the judge must find probable cause to believe that the target has committed, is committing, or will commit a crime.[156] Significantly, non-U.S. persons do not need to be engaged in criminal activity for FISA surveillance.[157]

---

[150] 50 U.S.C. § 1804(a).
[151] 50 U.S.C. § 1804(6)(B).
[152] 50 U.S.C. § 1804(e).
[153] Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications,* 52 DUKE L.J. 179, 195 (2002).
[154] 50 U.S.C. § 1804(a)(2010).
[155] 50 U.S.C. § 1805(2)(A)(2010).
[156] 18 U.S.C. § 2516 (2012).
[157] *Why the FISA Amendments Act Is Unconstitutional*, ACLU (Feb. 5, 2008), https://www.aclu.org/national-security/why-fisa-amendments-act-unconstitutional.

Section 1881a: Non-U.S. Persons Outside the United States

Section 1881a of the FISA is intended for use in surveilling non-U.S. persons outside of the U.S.[158] Under this section, LEOs cannot intentionally target an individual if they are located within the U.S., or even believed to be located in the U.S. This section also prohibits intentionally targeting a U.S. person. The LEO does have added discretion in a post-Patriot Act surveillance environment, but the citizenship and location of the individual is quite relevant for FISA-authorized surveillance. The amendment of this section is also known by its legislative name: Section 702. The EFF writes that the NSA uses Section 702 to "sweep up" U.S. persons' communications, even though the original statute ostensibly targets non-U.S. persons.[159]

Section 1881c: U.S. Persons outside the United States

Section 1881c is used to acquire information about U.S. persons outside of the U.S.[160] To obtain FISA authority to be able to surveil U.S. persons abroad, LEOs need to follow a procedural standard comparable to the probable cause standard of obtaining a warrant in the U.S.;[161] however, certain "emergency" acquisition is allowed in situations that the Attorney General authorizes. In situations where the location is uncertain, the law "requires uncertainty to be resolved in favor of the government," instead of favoring individuals' privacy rights.[162]

[158] 50 U.S.C. § 1881a(a) (2014).
[159] Nadia Kayyali, *The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why*, ELECTRONIC FRONTIER FOUNDATION (March 5, 2015), https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why.
[160] 50 U.S.C. § 1881c (2014).
[161] 50 U.S.C. § 1881c (a)(2) (2014).
[162] *Why the FISA Amendments Act Is Unconstitutional*, ACLU (Feb. 5, 2008), https://www.aclu.org/national-security/why-fisa-amendments-act-unconstitutional.

Patriot Act Amendments

Like the ECPA, the FISA was significantly modified by the Patriot Act. Under Section 215 of the Patriot Act, the FISA now permits the FBI to compel production of "tangible things," including books, records, papers, and documents from businesses.[163] An order to compel can be authorized to obtain information relevant to an ongoing investigation if the information does not concern a U.S. person or if it is used to protect against terrorism.[164] Recipients are prohibited from disclosing that they received an order from the FBI.[165] The government obtained millions of Verizon customer phone records this way.[166] The EFF has sued the Department of Justice over a lack of disclosure on the use of Section 215.[167] The EFF questions the legality of this so-called "sensitive collection program" and alleges that it targets a large number of Americans.[168]

The Patriot Act Amendments also permit evidence to be used in criminal trials that the government discovered "incidentally" during the course of FISA surveillance.[169] There is concern that this allows the government to circumvent the protections of the Wiretap Act, particularly following the change from a "primary purpose" requirement to a "significant purpose."[170] Essentially, it is possible for evidence to be uncovered under the authorization of the FISA that would not have been authorized under the more stringent requirements of the Wiretap Act. In addition, Section 206 of the Patriot Act amended the FISA to permit multipoint, or

---

[163] 50 U.S.C. §1861(b)(1)(B) (2010).
[164] 50 U.S.C. §1861.
[165] 50 U.S.C. §1861(d).
[166] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[167] *Section 215 of the USA PATRIOT Act,* ELECTRONIC FRONTIER FOUNDATION (last accessed March 3, 2015), https://www.eff.org/foia/section-215-usa-patriot-act.
[168] *Id.*
[169] Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications,* 52 DUKE L.J. 179, 195 (2002).
[170] *Id*.

"roving" wiretaps.[171] Roving wiretaps permit the interception of a target's communications without specifying the particular device to be surveilled. Rather than following the device, the wiretap follows the target.[172]

The FISA Amendments Act

The most significant change to the FISA is section 702. It permits "mass acquisition" orders to surveil individuals abroad.[173] The Act does not require that the government demonstrate that targets are foreign agents.[174] In fact, it does not require the government to identify targets at all.[175] Additionally, the government is not required to specify the facilities to be monitored.[176] The Act only requires that the government adopt minimization procedures.[177] The government can order a provider to immediately "provide the Government with all the information, facilities, and assistance necessary to accomplish the acquisition."[178] The FISC court does not supervise the implementation of the surveillance once authorized.[179] Section 702 authorizes National Security Agency (NSA) programs like PRISM, which will be introduced below.[180]

---

[171] Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications,* 52 DUKE L.J. 179, 197 (2002).
[172] Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications,* 52 DUKE L.J. 179, 197 (2002) (citing United States v. Hermanek, 289 F.3d 1076, 1087 (9th Cir. 2002)).
[173]*Why the FISA Amendments Act is Unconstitutional*, ACLU, 1 (last accessed March 3, 2015), https://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf.
[174] *Why the FISA Amendments Act is Unconstitutional*, ACLU, 1 (last accessed March 3, 2015), https://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf.
[175] *Id.*
[176] *Id.*
[177] *Id*. at 2.
[178] 50 U.S.C. § 1881a(h)(1)(A) (2015).
[179] *Why the FISA Amendments Act is Unconstitutional*, ACLU, 2 (last accessed March 3, 2015), https://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf.
[180]*Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs*, BRENNAN CENTER FOR JUSTICE, 2 (last accessed March 3, 2015), https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf.

FISA in Action

In its practical application, the use of surveillance under the FISA has made a significant difference in the U.S. government's scope of surveillance. Of the 33,949 FISA applications that were reviewed from 1979-2012, only 11 were rejected.[181] A recently declassified FISC opinion revealed that the companies that received FISA requests for phone metadata have not challenged the orders, either. [182] If the electronic service provider refuses to comply, the Attorney General is authorized to file a petition for an order to compel, which might explain the high compliance.[183]

The Snowden leaks have cast light on what FISA-approved surveillance may look like. PRISM and XKeyscore in particular illustrate that the NSA, under the authority of the FISA, is likely conducting extensive and systematic surveillance. PRISM is an NSA program that collects stored Internet communications.[184] Using PRISM, the NSA purportedly receives the information directly from ISP servers based on court-approved search terms.[185] It is still unclear how exactly the information is collected. Journalists speculate that the NSA has some kind of "backdoor access" to ISP servers.[186] The communications collected include email, video and voice chat, videos, photos, and social networking details.[187] NSA intelligence analysts can subsequently search PRISM data using terms to identify targets that the analysts suspect, with at least 51

[181] *Foreign Intelligence Surveillance Act Court Orders 1979-2014,* EPIC (last visited Feb. 20, 2015),https://epic.org/privacy/wiretap/stats/fisa_stats.html.
[182] *FISA court: Phone tapping doesn't violate Constitution*, THE GUARDIAN, (September 18, 2013, 8:15AM), http://america.aljazeera.com/articles/2013/9/18/fisa-judge-no companyeverchallengedorderstoturnoverphonerecords.html.
[183] 50 U.S.C. § 1881c (2014).
[184] Barton Gellman *et al.*, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASHINGTON POST (Oct. 13, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.
[185] *Id*.
[186] *Id.*
[187] *Id.*

percent certainty, are not U.S. persons.[188] In the process, information regarding U.S. persons is incidentally intercepted and collected.[189]

PRISM data makes up one part of the NSA database. XKeyscore allows the NSA to sift through accumulated information. Accordingly to leaked information, it is a sophisticated system that allows analysts to search through the NSA's expansive database to locate specific information.[190] With a simple form to justify the search, analysts can find emails, IP addresses that have visited a particular website, and Facebook chats.[191] The database is huge. An NSA report from 2007 indicated that 1-2 billion records were added per day.[192] This repository of data is vast and the NSA continuously collects more. Thus, the data can only be stored for short periods of time.[193] Content remains in the XKeyscore system for three to five days, while metadata is stored for 30 days.[194] To deal with this, the NSA has created a tiered system, in which analysts can flag certain material and move it into other databases, where it can be stored for longer periods of time. According to Snowden, analysts are periodically reviewed. However, the "reviews" are often suggestions from superiors on how to legitimize the searches.[195] Journalists have only confirmed that the NSA intends to further develop these programs. It is unknown if the government is actually capable of successfully implementing technologically sophisticated programs such as PRISM and XKeyscore. Nevertheless, the programs warrant public vigilance. Tor user data in particular may be targeted for surveillance because Tor is international in nature.

---

[188] Barton Gellman *et al.*, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASHINGTON POST (Oct. 13, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.
[189] *Id.*
[190] Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'* THE GUARDIAN (July 31, 2013, 08:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'* THE GUARDIAN (July 31, 2013, 08:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Constitutionality of FISA

The ACLU filed a lawsuit challenging the 2008 amendments on the day they were enacted.[196] They argued that it is unconstitutional under the First Amendment, the Fourth Amendment, under Article III, and under the principle of the separation of powers.[197] The ACLU argues that the FISA Amendment Act is unconstitutional because it permits broad surveillance.[198] They argue that FISA authorizes information collection without specifying "facilities, places, premises, or property to be monitored" without limitations.[199] They argue the law violates the First Amendment because it burdens expressive activity and authorizes the interception of protected communications without meaningful judicial oversight.[200] Because the law would require the FISC to rule on questions not arising from cases or controversies, the law would violate Article III.[201] They also argue that the ability of the government to surveil after the FISC finds them illegal violates the principle of separation of powers.[202]

Allowing dragnet surveillance puts more surveillance information in the hands of the government, which is contrary to the ideal of protecting privacy.[203] Even though FISA is intended for foreign communications, the ACLU argues that the government is only restricted at time of acquisition. If a U.S. person's data is intercepted in error, uncertainty is resolved in favor of the government.[204]

---

[196] Complaint generally, Amnesty Int'l v. McConnell, 646 F. Supp. 2d 633, (S.D.N.Y. 2009) No. 08 Civ. 6259. https://www.aclu.org/sites/default/files/pdfs/safefree/faa_complaint_20080710.pdf.
[197] *Id*. at 41.
[198] *Why the FISA Amendments Act is Unconstitutional,* ACLU, https://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf (last visited Feb. 20, 2015).
[199] Complaint at 41, Amnesty Int'l v. McConnell, 646 F. Supp. 2d 633, (S.D.N.Y. 2009) No. 08 Civ. 6259. https://www.aclu.org/sites/default/files/pdfs/safefree/faa_complaint_20080710.pdf.
[200] *Id.* at 42
[201] *Id.* at 42
[202] *Id*. at 42
[203] *Id.* at 42
[204] *Why the FISA Amendments Act is Unconstitutional,* ACLU, https://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf (last visited Feb. 20, 2015).

In a released FISC decision the court held that the mass order for production of call detail records is not in violation of the Fourth Amendment of the Constitution.[205] The court affirmed that *Smith* remains controlling. According to the court there is no expectation of privacy in call records, and by extension there is no constitutional protection.[206]

Electronic privacy experts like the EFF, Electronic Privacy Information Center, and the ACLU consider the lack of transparency of the FISC and the high rate of approval to constitute "warrantless surveillance."[207]

MUTUAL LEGAL ASSISTANCE TREATIES

Mutual Legal Assistance Treaties (MLATs) codify agreements between countries to share information for the purpose of law enforcement. Many foreign nations establish MLATs with other countries, which allow for the formation of cross-jurisdictional or international criminal investigations of a country's citizens who are located abroad. For example, the United States has many MLATs with Argentina. If the agreement authorizes it, the U.S. government could ask for the Argentine government's assistance in locating an American fugitive in Argentina. MLATs can be used to enable surveillance of foreign nationals in the U.S., as well as U.S. persons abroad. Because of the international nature of Tor, the use of MLATs is reasonably foreseeable when Tor users are under investigation. MLATs will be explored in more depth in Section 3.

---

[205] *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-158 (FISC) at 5, *retrieved at* http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf.
[206] *Id.*
[207] Mitra Ebadolahi, *Warrantless Wiretapping Under the FISA Amendments Act*, AMERICAN BAR ASSOCIATION HUMAN RIGHTS MAGAZINE, Vol. 39. (last viewed March 5, 2015), http://www.americanbar.org/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/warrantless_wiretapping_fisa.html.

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT, 1994

Congress enacted the CALEA in 1994 to facilitate coordination between telecommunications carriers and law enforcement. In the government surveillance context, the CALEA requires telecommunications carriers to have built-in surveillance capacity for LEO's use. The CALEA will be discussed further in Section 5, with specific applicability to Tor.

CONCLUSION

Overall, the government has a number of ways to conduct surveillance on U.S. and non-U.S. persons, domestically and internationally, each with varying levels of oversight, restrictions, and comprehensiveness. Under the ECPA, law enforcement can intercept communications in transmission as well as content stored for less than 180 days with a court issued, probable cause warrant. It can obtain customer records and "abandoned" stored content with a self-issued relevancy-based administrative subpoena. It can also obtain transactional data with a court-issued relevancy-based d order. Under the FISA, law enforcement has wider discretion to surveil communications related to foreign intelligence, especially if targets are believed to be foreign powers. The expansiveness of FISA-authorized surveillance is still in question. Using MLATs, the government can coordinate with foreign governments to conduct intra- and extra-territorial surveillance. The CALEA is the statute that broadly enables the government to conduct surveillance. While the federal government is taking steps to update laws like the ECPA, the current status of surveillance by the United States government is pervasive. The use of Tor may be a possibility to guard against some of these mechanisms.

Section 2

Tor under the ECPA and CALEA via CSPs and ISPs

Question Presented: Given the relevancy of CSPs and ISPs to the definitions of electronic communications service and telecommunications carrier of the ECPA and CALEA, respectively, does Tor fall under the ECPA and CALEA by way of CSP and ISP definitions?

BRIEF ANSWER

Tor does not fall under the Electronic Communications Privacy Act (ECPA) or the Communications Assistance for Law Enforcement Act (CALEA) by way of the CSP and ISP definitions because communications service provider, Internet service provider, and information service provider are categories not applicable to Tor. Tor does not possess the capability and infrastructure necessary to be classified as a CSP or ISP. Therefore, Tor cannot be subject to the ECPA or CALEA regulations and protections, unless the government expands the regulations to incorporate more than the terms electronic communications service, remote computing service, and telecommunications carrier.

INTRODUCTION

Congress enacted the Electronic Communications Privacy Act (ECPA) in 1986 as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to protect individual privacy in electronic communications.[208] The ECPA, however, permits limited government surveillance in accordance with uniform standards.[209] The ECPA contains three separate acts: the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act

[208] Dept. of Justice, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, https://it.ojp.gov/default.aspx?area=privacy&page=1284 (last visited Feb. 25, 2015).
[209] 18 U.S.C.A. § 2510 (West 2002).

(PRA). All three allow wire or electronic communications services to assist law enforcement in the course of lawful surveillance. Section 1 discusses the ECPA in depth.

Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994, which requires telecommunications carriers to comply with certain standards and allows law enforcement to readily conduct surveillance using the telecommunications carriers' facilities.[210] The CALEA only applies to telecommunications carriers as defined by the statute and interpreted by courts and the Federal Communications Commission (FCC). In 2005, the FCC expanded the interpretation of a telecommunications carrier to apply to broadband internet services and Voice over Internet Protocol (VoIP) services.[211] There have been no challenges since the D.C. Circuit Court upheld the expansion in 2006.[212] Section 5 discusses the CALEA in depth.

"CSP" is generally interpreted as an acronym for communications service provider, while "ISP" is generally interpreted as an acronym for either an Internet service provider or information service provider. The term communications service provider encompasses a large variety of technologies. Tor cannot be considered a communications service provider, and by extension cannot be considered a wire and communications service. Therefore, Tor cannot fall under the ECPA as it currently exists. Similarly, the term Internet service provider encompasses those providers who provide Internet telecommunications, specifically those who provide broadband and VoIP services for a fee. Tor cannot be considered an Internet service provider, and by extension cannot be considered a telecommunications carrier. Therefore, Tor cannot fall under the CALEA as it currently exists. Lastly, the term information service provider is exempt

[210] 47 U.S.C.A. § 1001 (West 1994).
[211] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004).
[212] American Council on Education v. F.C.C., 451 F.3d 226, 232 (D.C. Cir. 2006).

from the CALEA, so even if Tor were to be considered an information service provider, which it cannot, Tor would still be exempt from the CALEA.

This section analyzes the terms communications service provider, Internet service provider, and information service provider and whether their definitions apply to Tor, followed by an analysis of how these terms encompass those providers referenced in the ECPA and CALEA.

CSP - COMMUNICATIONS SERVICE PROVIDER[213]

When interpreting CSP as communications service provider, it refers to "an entity that provides for a fee to one or more unaffiliated entities, by radio, wire, cable, satellite, and/or

[213] Communications service provider is not the only technology-related "CSP" term. Content security policy and converged service provider are also commonly utilized, though they do not explicitly apply to the ECPA and CALEA.
Converged Service Provider: When CSP stands for "converged service provider," it is a communication or Internet service provider that provides various forms of communication via the same network. Many have flaunted 'convergence' as the future of the communications industry, where traditional service providers no longer provide just one service, but rather integrate multiple services through the same network. These 'bundles' are most commonly a combination of television, Internet, and telephone services that are provided at a specific location, such as in a home or office. These bundles route the services through the same infrastructure. An example of this would be a Comcast bundle of TV, Internet, and mobile services wired through the same network of cables. Since a converged service provider is either an Internet service provider or a communications service provider, and Tor is neither of those, Tor would not be classified as a converged service provider. Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).
Content Security Policy: If CSP stands for "content security policy," it refers to a website protocol that has a whitelist, or exception, for an approval screening mechanism for loading content by extensions. GOOGLE CHROME, https://developer.chrome.com/extensions/contentSecurityPolicy (last visited Feb. 28, 2015). This protocol is the coding that protects your web application against cross-site scripting hacks. This code allows the web browser to block data or pages coming from an unexpected location. Interview with Michael Pliskaner, Assistant Vice President of Internet Technology, Merrimack Valley Federal Credit Union (February 25, 2015). The server administrator sets rules built into the coding of websites prohibiting a user from certain websites or keywords that are blacklisted or warned against. GOOGLE CHROME, https://developer.chrome.com/extensions/contentSecurityPolicy (last visited Feb. 28, 2015). An example of this would be when a user is browsing The Home Depot website and clicks on a Husky drill advertisement. A browser with a content security policy will not let the link process if it is not truly coming from Husky's website, as the coding expected. A browser with no content security policy could allow a link that was "hacked" to send you to a dating website or the like. "These policies provide security over and above the host permissions your extension requests; they're an additional layer of protection, not a replacement." Google Chrome, https://developer.chrome.com/extensions/contentSecurityPolicy (last visited Feb. 28, 2015). While some might argue that Tor is a content security policy because the end node user can adjust their settings to deny which types of information requests pass through their IP address, the end node user and Tor do not maintain complete control over which websites are visited. As such, Tor does not control which links a user accesses and should not be considered a content security policy.

lightguide: two-way voice and/or data communications, paging service, and/or SS7 communications."[214] From a technological standpoint, communications service provider is defined as a "service provider offering telecommunication services or some combination of information and media services, content, entertainment and applications services over networks, leveraging the network infrastructure as a rich, functional platform."[215] A communications service provider includes telecommunications carriers, content and applications service providers (CASP), cable service providers, satellite broadcasting operators, and cloud communications service providers.[216] The communications service provider tends to own the wires, routers, and other communication equipment.[217] Examples of communications service providers include Comcast and Verizon. While Tor allows users to utilize services similar to those listed above, it does not own the wires, routers, and other communication equipment, does not charge a fee, and requires an Internet connection from another source. Therefore, interested parties should not regard Tor as a communications service provider.

ISP

ISP is an acronym for "Internet service provider" or an "information service provider." Few legal definitions exist to clarify each term, given the relatively recent advances in technology. Below is a general overview of each term as defined in an Internet technology aspect, as well as whether or not Tor can be considered to apply to any of the specific terms.

[214] 47 C.F.R. § 4.3(b) (2012).
[215] GARTNER IT GLOSSARY, http://www.gartner.com/it-glossary/csp-communications-service-provider (last visited Jan. 27, 2015).
[216] GARTNER IT GLOSSARY, http://www.gartner.com/it-glossary/csp-communications-service-provider (last visited Jan. 27, 2015).
[217] Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).

Internet Service Provider

"Internet service provider" is legally defined as a "business or other organization that offers Internet access, typically for a fee."[218] From a technological standpoint, Internet service provider refers to a company for hire that provides Internet access to its customers.[219] This Internet access can be provided either through a direct connection or a modem.[220] Tor would likely be classified as an online service provider rather than an Internet service provider. Internet service providers differ from online service providers because they always provide the connection to the Internet as a whole, whereas online service providers generally only allow access to specific content.[221] Online service providers are providers who allow "access to exclusive content, databases, and online discussion forums that are not available outside the service."[222] Online services range from simple to complex; a basic online service may help subscribers utilize a search engine such as Google, whereas a complex online service might provide an online tax form. Tor, via the Tor Browser, can be considered an online service provider, since Tor allows its users to access exclusive content through its browser. However, Tor cannot be an Internet service provider, as no one pays for its services or downloads over the network.[223] Additionally, Tor functions as an application that is only accessible once an Internet connection is established via another entity's network.[224] Unlike Internet service providers, Tor is a decentralized network with a widespread network of nodes; as such, Tor cannot provide a list

[218] BLACK'S LAW DICTIONARY (10th ed. 2014).
[219] GARTNER IT GLOSSARY, http://www.gartner.com/it-glossary/isp-internet-service-provider/ (last visited Feb. 15, 2015).
[220] U.S. v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).
[221] GARTNER IT GLOSSARY, http://www.gartner.com/it-glossary/isp-internet-service-provider/ (last visited Feb. 15, 2015).
[222] TECHOPEDIA DICTIONARY, http://www.techopedia.com/definition/3248/online-service (last visited Feb. 15, 2015).
[223] GARTNER IT GLOSSARY, http://www.gartner.com/it-glossary/isp-internet-service-provider/ (last visited Feb. 15, 2015).
[224] Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).

of exactly who is utilizing their program.[225] This is relevant based on the CALEA requirements for Internet service providers and will be discussed below.

Information Service Provider

When interpreting ISP as "information service provider," it is a bit more difficult to explicitly define in technical terms. Legally, "information service" is defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications . . . but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service."[226] Therefore, an information service provider provides the capability to perform those actions. An information service provider is similar to an online merchant, which is discussed in more detail in the CALEA section below.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

As discussed in previous sections, the Electronic Communications Privacy Act includes the Pen Register Act, the Wiretap Act, and the Stored Communications Act. Congress expanded the Wiretap Act to include "electronic communications" in 1986.[227] It prohibits the "interception of wire, oral, or electronic communications while those communications are in transmission."[228] Congress intended for the inclusion of wireless communications such as cell phones with the Wiretap Act, because "all communications contain a metal wire, satellite, or fiber optic cable at

[225] Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).
[226] 47 U.S.C.A. § 153(24) (2010).
[227] Robert Roll, *United States v. Councilman: An Appropriate Expansion of Internet Privacy Rights?* 10 COMPUTER L. REV. & TECH. J. 207, 208 (2006).
[228] Samantha L. Martin, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 443 (2006).

some point between transmission and reception."[229] The Stored Communications Act prohibits the "unauthorized access of electronic communications that are in storage."[230] Both the Wiretap Act and the Stored Communications Act utilize the term "electronic communication service," which means "any service which provides to users thereof the ability to send or receive wire or electronic communications."[231] The statute defines "electronic communications" as,

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--
> **(A)** any wire or oral communication;
> **(B)** any communication made through a tone-only paging device;
> **(C)** any communication from a tracking device (as defined in section 3117 of this title); or
> **(D)** electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.[232]

Remote Computing Service

The Stored Communications Act also utilizes the term "remote computing service" (RCS) when regulating providers.[233] An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[234] An off-site computer provides an RCS when it stores or processes data for a customer, which the customer or other entity can retrieve at a later date.[235] Unless an entity who operates an online

---

[229] Nicholas Matlach, *Who Let the Katz Out? How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in Katz v. United States Will Fix It*, 18 COMMLAW CONSPECTUS 421, 444 (2010).
[230] Samantha L. Martin, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 443 (2006).
[231] 18 U.S.C.A. § 2510(15) (West 2002).
[232] 18 U.S.C.A. § 2510(12) (West 2002).
[233] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004).
[234] 18 U.S.C.A. § 2711(2) (West 2009).
[235] Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994). *See also* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564-65. *See also* Steve Jackson Games, Inc. v. United States Secret Service, 816 F.Supp. 432, 442-43 (W.D. Tex. 1993) *aff'd on other grounds*, 36 F.3d 457 (5th Cir. 1994).

service offers a storage and processing service through their website, they cannot be considered an RCS.[236] For example, "an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into an RCS."[237] Tor does not offer any information storage options to its users, so it cannot be considered an RCS under the ECPA as it currently stands.

The ECPA and CSP

As defined earlier, a communications service provider is an entity that provides radio, wire, cable, satellite, and fiber optic communications to non-affiliated entities.[238] Non-affiliated entities are those who do not have any particular relationship to the company. For instance, an employer that just provides internal communications services to its employees is not a communications service provider. Similarly, to be considered an electronic communications service, the entity must provide wire or electronic communications to the public.[239] Moreover, the definition of electronic communications service is encompassed in the definition of communications service provider. If an entity is considered an electronic communications provider, it must be a communications service provider. Since Tor is not a communications service provider due to a lack of the requisite infrastructure, Tor cannot be considered an electronic communications service, and would therefore not be subject to the ECPA provisions.

[236] H. Marshall Jarrett, Michael W. Bailie, Ed Hagen, and Nathan Judish, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section Criminal Division (July 2009) at 119, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf
[237] *Id. referencing In re* Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005).
[238] 47 C.F.R. § 4.3(b) (2012).
[239] Anderson Consulting LLP v. UOP, 991 F.Supp. 1041, 1042-43 (N.D. Ill. 1998).

The ECPA and ISP

United States v. Warshak established that Internet service providers fall under the ECPA protections; the government must get a warrant (or use a similar mechanism) to compel a commercial Internet service provider to turn over the content of its users' emails.[240] As the *Warshak* court defined commercial Internet service provider,

> If we accept that an email is analogous to a letter or a phone call . . . agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment . . . [and] the ISP is the functional equivalent of a post office or a telephone company . . . the police may not storm the post office and intercept a letter, . . . unless they get a warrant, that is.[241]

Since Tor does not fall under the scope of Internet service provider, it cannot be considered an electronic communication service and subject to the ECPA provisions by way of the classification of Internet service provider. An information service provider is similar to an online merchant, such as Amazon, which is not currently classified as an electronic communications service. Therefore, information service providers do not fall under the ECPA protections.

Additional Avenues under the ECPA

The courts have construed electronic communications service under the ECPA to apply to various other terms. For example, courts have held that providers of email services are electronic communications services.[242] Tor previously provided an email service called Tor Mail; however, on August 4, 2013, Tor officially shut down the email service and ceased to provide

[240] United States v. Warshak, 631 F.3d 266, 282-84 (6th Cir. 2010). There are more than ten opinions issued in the history of this case. This specific section applies to the most recent appellate court decision in 2010.
[241] United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).
[242] Cornerstone Consultants, Inc. v. Production Input Solutions, LLC., 789 F.Supp.2d 1029, 1052 (N.D. Iowa 2011). *See also* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

email services.[243] Therefore, Tor cannot be considered an electronic communications service because it does not provide an email service.

Again, courts have consistently held that providers of Internet access are electronic communications services.[244] The companies that do business or provide services online are not electronic communications services because an established Internet connection is required to use them.[245] While not directly on point, Tor and the Tor Browser are analogous to online merchants, such as Amazon and JetBlue, in that they provide a service to consumers which requires an Internet connection prior to being able to access its services. Neither Amazon, nor JetBlue, nor Tor provide the Internet connection. Therefore, under this Internet access theory of electronic communications service, Tor cannot be an electronic communications service.

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

The Communications Assistance for Law Enforcement Act is described in detail in Section 5. The CALEA requires "telecommunications carriers to ensure that their networks are technologically capable of being accessed by authorized law enforcement officials."[246] "Telecommunications carriers" are defined as the following:

> **(A)** a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and
> **(B)** includes--
>
> > **(i)** a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of this title); or
> > **(ii)** a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the

[243] Joe Mullin, *FBI is keeping a giant stash of e-mails from defunct Tor Mail service*, arstechnica, (Jan. 27, 2014), http://arstechnica.com/tech-policy/2014/01/fbi-is-keeping-a-giant-stash-of-e-mails-from-defunct-tor-mail-service.
[244] *In re* JetBlue Airways Corp. Privacy Litig., 379 F.Supp.2d 299, 309 (E.D.N.Y. 2005). *See also In re* DoubleClick Inc. Privacy Litigation, 154 F.Supp.2d 497, 508 (S.D.N.Y. 2001).
[245] *In re* JetBlue Airways Corp. Privacy Litig., 379 F.Supp.2d 299, 309 (E.D.N.Y. 2005). *See also* Steinback v. Village of Forest Park 2009 WL 2605283. *See also* Crowley v. CyberSource Corp., 166 F.Supp.2d 1263, 1270 (N.D. Cal. 2001). *See also* Anderson Consulting LLP v. UOP, 991 F.Supp. 1041, 1042-43 (N.D. Ill. 1998).
[246] Barbara J. Van Arsdale, Annotation, *Construction and Application of Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C.A. §§ 1001 to 1010*, 25, A.L.R. FED. 2D 323 (2008).

> Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter; but
>
> **(C)** does not include--
>
> **(i)** persons or entities insofar as they are engaged in providing information services; and
>
> **(ii)** any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General.[247]

The FCC has concluded that the CALEA creates three categorical distinctions between those providers who are subject to the CALEA and those who are exempt: (1) pure telecommunications providers, who are subject to the CALEA requirements; (2) information service providers, who are exempt from the CALEA requirements; and (3) hybrid providers that provide both information services and telecommunications services, who are also subject to the CALEA requirements.[248]

Previously, Internet service providers and information service providers were exempt from the definition of telecommunications carrier for purposes of the CALEA.[249] However, the current definition only exempts information service provider (see above, (C)(i)).[250] In 2006, Internet service providers were removed from the exemptions and added to the scope of the CALEA. This shift made "providers of broadband Internet access and voice over Internet protocol (VoIP) services" telecommunications carriers under the CALEA.[251] Wireline broadband

---

[247] 47 U.S.C.A. § 1001(8) (West 1994).

[248] Time Warner Telecom, Inc. v. F.C.C., 507 F.3d 205, 219 (3d Cir. 2007). *See also* In the Matter of Communications Assistance of Law Enforcement Act and Broadband Access and Services, 20 F.C.C.R. 14989, 14998-99 (2005).

[249] Jeffrey Yeates, *Calea and the Ripa: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB. L.J. SCI. & TECH. 125, 139 (2001).

[250] "Federal Communications Commission (FCC) reasonably ruled that providers of broadband Internet access were regulable as "telecommunications carriers" under Communications Assistance for Law Enforcement Act (CALEA), thus broadband providers had to ensure that law-enforcement officers were able to intercept communications transmitted over providers' networks; although FCC interpreted phrase "information service" differently, for purpose of exclusion, than it had under the Telecom Act, CALEA and Telecom Act served significantly different purposes, among other things." American Council on Education v. F.C.C., 451 F.3d 226 (D.C. Cir. 2006).

[251] American Council on Education v. F.C.C., 451 F.3d 226, 227 (D.C. Cir. 2006).

Internet service, which is a hybrid of information service and Internet service, need to be compliant with the CALEA though, as "Congress did not intend that the terms 'telecommunications carrier' and 'information service' be mutually exclusive for purposes of identifying the entities that are subject to the statute's provisions."[252] Therefore, Internet service providers are subject to the CALEA regulations. However, information service providers are not subject to the CALEA regulations.[253] Communications service provider falls under the definition of telecommunications carrier because they provide the same services. Telecommunications carriers are subject to the CALEA; therefore, communications service providers are as well. While CSPs and ISPs are covered under the CALEA, Tor is an application or protocol rather than a CSP or ISP. Therefore, Tor is not subject to the requirements of the CALEA under any of the CSP or ISP terms as listed.

CONCLUSION

Tor is not likely to be considered a communications service provider, Internet service provider, or information service provider. Tor is the equivalent of a protocol or an application.[254] Tor is decentralized, does not own the Internet network, and does not have the infrastructure to determine who is sending or receiving information.[255] The ECPA utilizes the terms "electronic communications service" and "remote communication service," and the CALEA utilizes the term "telecommunications carriers." Expansion of these statutes could lead to broader definitions of

[252] "Wireline broadband Internet access service combines computer processing, information provision, and data transport, enabling end users to run a variety of applications (e.g., e-mail, web pages, and newsgroups)." Given the similarity between how end users perceive the finished product (Internet access), whether provided by wireline or cable modem providers, the FCC concluded that its decision to classify wireline broadband Internet access service as an information service logically flowed from the Supreme Court's Brand X decision." Time Warner Telecom, Inc. v. F.C.C., 507 F.3d 205, 220 (3d Cir. 2007).
[253] 47 U.S.C.A. § 1001(8)(C)(i) (West 1994).
[254] Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).
[255] Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).

these terms.[256] The ECPA, for example, has expanded the definition of electronic communication to include "'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce,' with certain exceptions."[257] Finally, if Tor were to be classified as a CSP or ISP, Tor could be subject to both the protections and requirements of the ECPA or CALEA. However, Tor does not currently fall under any of the CSP or ISP definitions, and as such would not be subject to the ECPA or CALEA regulations.[258]

[256] *In re* Pharmatrak, Inc., 329 F.3d 9, 18 (C.A.1 (Mass.),2003).
[257] *Id.*
[258] The FCC ruled in a 3-2 partisan vote in February 2015 to classify Internet service providers as a telecommunications service, rather than an information service under Title II of the Communications Act. Many have focused on the ability to access all Internet content equally, but there is the potential that Internet service providers could be more tightly regulated in the future. While it is likely that there will be challenges to this ruling and it may not stand, this provides an excellent example of the potential change to service providers under statutes, such as those discussed in this section. Michael Miller, *The FCC on Net Neutrality: Be Careful What You Wish For*, PCMag, (Feb. 27, 2015), http://forwardthinking.pcmag.com/none/332400-the-fcc-on-net-neutrality-be-careful-what-you-wish-for. For more information on the recent FCC ruling, *see e.g.*, Rebecca Ruiz and Steve Lohr, *F.C.C. Approves Net NeutralityRules, Classifiying Broadband Internet Service as a Utility*, NYTimes, (Feb. 26, 2015), http://www.nytimes.com/2015/02/27/technology/net-neutrality-fcc-vote-internet-utility.html?ref=topics&_r=0.

Section 3

Mutual Legal Assistance Treaties and Joint Investigation Teams

Question Presented: Is it legal to use a Mutual Legal Assistance Treaty (hereinafter "MLAT") and a Joint Investigation Team (hereinafter "JIT") to de-anonymize Tor users?

BRIEF ANSWER

In on-going criminal investigations or prosecutions it is legal to use MLATs and JITs to de-anonymize a Tor user from whom evidence is requested, or who is the subject of the investigation itself. Doing so however, erodes civil liberties that are guaranteed under Fourth Amendment.[259] To understand the effect of these erosions on Tor users, the section will focus on the implications of MLATs and JITs in context of privacy and surveillance.

Part I defines mutual legal assistance treaties and how they function. From there it discusses specific provisions within MLAT agreements that allow for identification of persons connected to criminal investigations. Part II lays out how JITs are structured, how they operate, and the use of JITs to elude formal legal channels in obtaining evidence. In addition, Part II applies MLATs and JITs to Tor users. Part III is an analysis of the constitutionality of MLATs and JITs within Fourth Amendment jurisprudence, and describes the implications for Tor users. Finally, Part IV is a discussion of the U.S. government's increased focus on Internet Service Provider (ISP)-related MLAT requests, and what that means for MLATs as identification tools going forward.

[259] IV of the Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* search and seizures, shall not be violated, and no Warrants shall issue, but upon Amendment probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*." (emphasis added) U.S. CONST. amend. IV.

INTRODUCTION

MLATs are treaties between two or more countries that facilitate the transfer of evidence in international criminal investigations and prosecutions, using legal mechanisms such as subpoenas and warrants.[260] As such, they are the framework through which governments may circumvent Fourth Amendment protections. This is best illustrated in the use of JITs to execute MLAT evidentiary requests. JITs are teams of law enforcement agencies (LEAs) working within the structural confines of a MLAT request to collect evidence. The synergic structure of JITs permit the creation of information sharing arrangements between international governments and intelligence agencies.[261] Each nation in a JIT may work together to sidestep heightened levels of proof required to collect evidence. For example, otherwise innocuous information can be shared among JIT members, who collaborate to reveal a broader picture of a person and their life allowing de-anonymization.[262] These formalized legal frameworks may therefore allow governments to surveil networks across the globe to the detriment of Tor and its users. In doing so, the privacy of relay operators, domestic violence survivors, victims of fraud, political dissidents, and whistleblowers may be compromised for the sake of criminal investigations.[263]

---

[260] T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, FED. JUDICIAL CTR., 2 (2014), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf.

[261] Article 13, §1(b) states, "A joint investigation team may, in particular, be set up where: *a number of Member States are conducting investigations* into criminal offences in which the circumstances of the case necessitate coordinated, concerted action in the Member States involved." (emphasis added) *Convention on Mutual Assistance on Criminal Matters between the Member States of the European Union* art. 13, May 29, 2000, C.E.T.S. No. 3 [hereinafter EU MLAC], *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/243321/7054.pdf.

[262] For example, JIT members watching Tor traffic pass through relays in different countries could plausibly de-anonymize a Tor user by piecing together disparate information and viewing it as a whole.

[263] *See generally* TOR PROJECT, https://www.torproject.org/about/torusers.html.en. (last visited Mar. 8, 2015).

PART I

Mutual Legal Assistance Treaties

MLATs are treaty-based, transnational requests for assistance in obtaining foreign evidence in criminal investigations and proceedings.[264] They are negotiated within the Executive Branch[265] by the Department of Justice (DOJ) in conjunction with the Department of State.[266] MLATs are officially utilized in ongoing criminal investigations.[267] MLATs may be (1) bilateral, as between two countries, (2) multilateral, as between three or more countries, or (3) hybrids.[268] Because MLATs are negotiated separately[269] each treaty is specific to the named parties, the type of legal assistance available, and the jurisdictional scope.[270] Limiting MLATs to the named parties confines use of these treaties to government entities,[271] thereby making them unavailable

---

[264] T. Markus Funk, Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges, Fed. Judicial Ctr., 2 (2014), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf.

[265] The Constitution gives the Executive Branch the right to negotiate foreign treaties. Article II, § 2 of the Constitution states, "[The President] shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur…" U.S. CONST. art. II, § 2, cl. 2. Additionally, Article VI, cl. 2 states, "This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and *all Treaties made, or which shall be made,* under the Authority of the United States, shall be the supreme Law of the Land, and the Judges in every State shall be bound thereby, and any Thing in the Constitution or Laws of any State to the Contrary notwithstanding." (emphasis added) U.S. CONT. art. VI, cl. 2.

[266] Funk, *supra* note 264, at 6.

[267] Law Enforcement Agencies are capable of manipulating rules to theoretically "inconceivable" ends. For example, shortly after Hoover's death, the FBI was found guilty of keeping "ongoing" investigations open for 46 years.

[268] For example, the U.S.-E.U. MLAT applies to the relationship of each European Union member state with the addition of the U.S., thereby making the treaty a hybrid of the bilateral and multilateral structures. The International Chamber of Commerce [ICC] Commission on the Digital Economy, *Using Mutual Legal Assistance Treaties (MLATs) to Improve Cross-Border Lawful Intercept Procedures*, 3, Document No. 373/512 (Sept. 12. 2012) *available at* http://www.iccindiaonline.org/policy-statement/3.pdf.

[269] The United States Attorney's Criminal Resource manual states, "[MLATs] are negotiated separately, each one differs from the next. Experience with one should not be considered universally applicable." United States Attorney's Manual (USAM), Title 9 Criminal Resource Manual, *Treaty Requests*, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm (last visited Mar. 4, 2015).

[270] Jurisdictional scope defines what type of criminal activity, which territories, and which judicial proceedings are recognized under the treaty. Access, *Mutual Legal Assistance Treaties FAQ*, https://mlat.info/faq (last visited Feb. 27. 2015).

[271] In fact, most treaties have specific provisions limiting their use. Article 1, §3 of the U.S.-China treaty states, "This Agreement is intended solely for mutual legal assistance between the Parties. The provisions of this Agreement *shall not give rise to a right on the part of any private person* to obtain, suppress, or exclude any evidence, or to impede the execution of a request." (emphasis added) Treaty on Mutual Legal Assistance in Criminal

for use in civil litigation by criminal defendants, specifically, or by private citizens, generally.[272] This inaccessibility confounds traditional notions of due process[273], and creates unequal bargaining power and informational asymmetry in criminal litigation.[274]

MLATs include procedural empowerments available exclusively to law enforcement officials and prosecutors in criminal matters; and are executed pursuant to the laws of the requested state[275] and the terms of the agreement.[276] Ultimately, these treaties are the legal vehicle through which other technological or legal mechanisms may be used to collect evidence or de-anonymize a Tor user.

How To: Executing an MLAT Request

To execute an MLAT request, an agency in each country, referred to in the text of the treaty as the "Central Authority," is designated to handle incoming and outgoing evidentiary and investigatory requests.[277] In the United States, the Central Authority is the DOJ Criminal

---

Matters, U.S.-China, art. 1, June 19, 2000, T.I.A.S No.13102 [hereinafter U.S.-China MLAT], *available at* http://www.state.gov/documents/organization/126977.pdf. *See also* U.S-Japan MLAT Article 1, §5 at 2; U.S.-Russia MLAT Article 1, §4 at 2.

[272] Funk, *supra* note 264, at 2.

[273] The Fifth Amendment Due Process Clause states in relevant part, "...nor shall [any person] be deprived of life, liberty, or property, without due process of law…" U.S. Const. amend. V. Similarly, the Fourteenth Amendment Due Process Clause states, "...nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny any person within its jurisdiction the equal protection of the laws." U.S. CONST. amend. XIV, § 1. The restriction on MLATs to exclusive use by the government raises due process issues and begs the question of what constitutes due process under the law.

[274] T. Markus Funk notes, "Defense counsel and civil litigants must rely on letters rogatory to gather evidence located abroad." Funk, *supra* note 264, at 3.

[275] The "Requested State" is the state receiving a MLAT request for assistance. The "Requesting State" is the state sending the MLAT request.

[276] "Requests made under a MLAT are executed pursuant to the terms of the treaty and United States domestic law, specifically Title 28 U.S.C. §1782 and Title 18 U.S.C. §3512." Comm. on Crime Prevention and Criminal Justice, *Requesting mutual legal assistance in criminal matters from G8 countries: A step-by-step guide*, Apr. 11-15, 2011, E/CN.15/2011/CRP.6, at 56 (Apr. 12, 2011), http://www.coe.int/T/dghl/standardsetting/pc-oc/PCOC_documents/8_MLA%20step-by-step_CN152011_CRP.6_eV1182196.pdf.

[277] For example, in the U.S.-China MLAT Article 2, §1 states, "Each party shall designate a Central Authority to make and receive requests pursuant to this Agreement". U.S.-China MLAT *supra* note 271, art. 2, §1.

Division's Office of International Affairs (DOJ CRM/OIA).[278] Upon receipt of a MLAT request for assistance, a DOJ CRM/OIA attorney will review the request and either approve or deny it. The MLAT sets forth any limitations on assistance that would allow a Central Authority to deny a request.[279] Approved requests are typically sent to the US Attorney's Office[280], where the evidence or witness is located[281], to be filed with the appropriate federal district court judge.[282] The judge, as necessary to execute the request, may issue warrants or subpoenas to aid in the collection of evidence.[283] Once obtained, evidence is transmitted to the requesting foreign Central Authority, as outlined in the MLAT, who will use the information for investigation and/or prosecution.[284] Although MLATs are silent as to whether or not all legally obtained evidence is made available to the requesting foreign Central Authority, most treaties do allow the

[278]Bruce Swartz, Dep. Assistant Att'y General, Dept. of Justice, Statement before the Committee on Foreign Relations United States Senate concerning the Mutual Legal Assistance Treaty with Bermuda (June 7, 2011), at 2, http://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/06/07/11//06-07-11-crm-swartz-testimony-re-the-mutual-legal-assistance-treaty-with-bermuda.pdf.

[279] Because MLATs are country specific, the terms on which a Central Authority may deny a request for assistance varies by country. However, there are consistent themes running throughout most MLATs on which a request may be denied. Those are: requests that would not constitute an offense in the country receiving the MLAT request, political or military offenses, or if the country receiving the request believes that the requesting country will use the information to prosecute a person on the basis of race, religion, nationality, or political opinions. To be clear, the Central Authority *may* deny the request on these grounds, but it is not required to. The discretion, therefore, to deny or approve MLAT requests falls within the purview of the Central Authority. See Article 3, §1-3 of the U.S.-China MLAT; Article 3 of the U.S.-Japan MLAT. Article 6 of the U.S.-Fr. MLAT lists only two reasons for denial of assistance. As such, the U.S.-Fr. MLAT arguably makes it more difficult to deny a request for assistance.

[280] The United States Attorney's Offices (USAOs) are the DOJ branches within each state. Contingent upon the number of federal districts, some states have more than one USAO.

[281] Comm. on Crime Prevention and Criminal Justice, *supra* note 276, at 56.

[282] Funk, *supra* note 264, at 9.

[283] The Foreign Evidence Efficiency Act of 2009, codified in 18 U.S.C. §3512, states in relevant part: **(1) In general.**--Upon application, duly authorized by an appropriate official of the Department of Justice, of an attorney for the Government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses, including proceedings regarding forfeiture, sentencing, and restitution.
(2) Scope of orders.--Any order issued by a Federal judge pursuant to paragraph (1) may include the issuance of--
(A) a search warrant, as provided under Rule 41 of the Federal Rules of Criminal Procedure;
(B) a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703 of this title;
(C) an order for a pen register or trap and trace device as provided under section 3123 of this title; or
(D) an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both. 18 U.S.C.A. § 3512 (West 2009).

[284] Comm. on Crime Prevention and Criminal Justice, *supra* note 276, at 56.

requested state to postpone execution or "make execution subject to conditions determined necessary" when "execution of a request would interfere with an ongoing criminal investigation" in the requested state.[285]

MLATs: Identification and Anonymity

This section will look at four bilateral MLATs currently in force between the United States and: (1) China, (2) Japan, (3) Russia, and (4) France.[286] Contained in all but one of the aforementioned MLATs are provisions for the location and identification of persons. These provisions are broad in scope. They do not delineate the type or amount of information necessary to determine whether or not identification is appropriate within the parameters of the request. Moreover, confidentiality provisions within the treaties stymie Fourth Amendment privacy challenges. Determining what information a requesting party provided in the request, if possible, would be a herculean task.

The Irony of Competing Interests: Identification of Persons and Confidentiality

Each MLAT defines the type of assistance a nation may request in international criminal investigations and prosecutions. For example, Article 1 of the U.S.-China MLAT states, "Assistance shall include: locating or identifying persons."[287] Similarly, the U.S.-Japan treaty states, "The assistance shall include the following: locating or identifying person, items, or places."[288] Additionally, Article 2 the U.S.-Russia MLAT provides, "Legal assistance under this

[285] U.S.-China MLAT *supra* note 271, art. 6 §4, at 6.
[286] Of the four MLATs chosen, all but China are listed on Tor's website in the top-10 countries of estimated number of directly-connecting users. The mean daily users by percentage are: Japan at 2.32%; Russia at 6.76%; and France at 6.31%. TOR PROJECT, *Tor Metrics: Top-10 Countries by directly connecting users*, https://metrics.torproject.org/userstats-relay-table.html (last visited Feb. 27, 2015).
[287] U.S.-China MLAT *supra* note 271, art. 1, at 2.
[288] Treaty on Mutual Legal Assistance, U.S.-Japan, art. 1, Aug. 5, 2003, T.I.A.S No.06-721.3 [hereinafter U.S.-Japan MLAT], *available at* http://www.state.gov/documents/organization/191629.pdf.

Treaty shall include: locating and identifying persons and items."[289] The plain language of the U.S.-France treaty, however, is silent on the explicit use of the treaty for identification purposes. Article 4 of the U.S.-France treaty may be read as allowing identification of persons. It states,

> Requests for assistance shall be in writing and shall include the following information: (d) *insofar as possible*, the identity and nationality of the person who is the subject of the investigation or proceeding; (e) *insofar as possible*, the identity, nationality, and address or location of any person to be served or from whom assistance is sought.[290]

It is conceivable, under this provision, that a party would identify a person to comply with a request. Furthermore, the treaty as a whole contains no overt pronouncement that a request will be denied if a person presumably connected to the criminal investigation is unknown at the time of the request. Article 11 of the U.S.-Japan Treaty,[291] Article 13 of the U.S.-China treaty,[292] and Article 14 of the U.S.-Russia treaty[293] contain analogous language to the U.S.-France treaty. These provisions may be read as circumventing the Fourth Amendment search and seizure protections which calls for "particularly describing the place to be searched, and the persons or things to be seized."[294] Unfortunately, confidentiality provisions[295] in MLATs make it challenging to know if the information presented in the request would withstand a Fourth Amendment challenge. For Tor users specifically, identification provisions allow privacy intrusions by the government under the auspices of evidence collection in an on-going criminal

---

[289] Treaty on Mutual Legal Assistance, U.S.-Russia, art. 2, June 17, 1999, T.I.A.S No.13046 [hereinafter U.S.-Russia MLAT], *available at http://www.state.gov/documents/organization/123676.pdf.*

[290] Treaty on Mutual Legal Assistance, U.S.-Fr., art. 4, Dec. 10, 1998), T.I.A.S No.13010 [hereinafter U.S.-Fr. MLAT], *available at* http://www.state.gov/documents/organization/121413.pdf. (emphasis added).

[291] Article 11 states, "The Requested Party shall make it *best efforts* to locate or identify persons, items, or places". U.S.-Japan MLAT *supra* note 288, art. 11, at 9. (emphasis added).

[292] Article 13 Location of Identification of Persons or Items, states in relevant part, "The Requested Party shall, in accordance with the request, endeavor to find out the location of identity of the person or item referred to in the request". U.S.-China MLAT *supra* note 271, art 13, at 12.

[293] Article 14 Location of Identification of Persons and Items, states, "If the Requesting Party seeks the location or identity of persons or information about items in the Requested Party, the Requested Party shall use its best efforts to execute the request". U.S.-Russia MLAT *supra* note 289, art. 14 at 8.

[294] U.S. CONST. amend. IV.

[295] Article 7 of the U.S.-China treaty allows the parties to "keep confidential a request and its contents, including any supporting documents, and any action taken pursuant to the request." U.S.-China MLAT *supra* note 271, art. 7, at 7.

investigation. Ultimately, Tor users have little expectation of privacy in the execution of an MLAT request.

PART II

Joint Investigation Teams

Joint Investigation Teams (JITs) are coordinated investigative efforts among law enforcement agencies in criminal matters[296] that allow "two or more countries to form a team to conduct a single criminal investigation".[297] They are set up on the basis of a written agreement[298] for the express purpose of judicial cooperation, expediency, and efficiency in transnational criminal investigations.[299] JITs may be comprised of international law enforcement agencies, administrative personnel, judges, and lawyers who work together to execute MLAT evidentiary requests.[300] Similar to MLATs, JITs are limited in duration and tailored to specific investigations.[301]

Structure and Operation

The 2000 European Union Convention on Mutual Legal Assistance in Criminal Matters (EU MLAC) formalized the use of JITs for cross-border criminal investigations in the EU.[302] Article 13 of the EU MLAC states that a JIT will operate in the territory where the investigation is expected to be carried out, and the team will "carry out its operations in accordance with the

[296] Organisation for Economic Co-operation and Development [OECD], *Typology on Mutual Legal Assistance in Foreign Bribery Cases* 51 (2012). http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf [hereinafter OECD].
[297] *Id.*
[298] Council of the European Union, Council Resolution of 26 February 2010 on a Model Agreement for setting up a Joint Investigation Team (JIT), 2010 0.J. (C 70) 1, 2 [hereinafter Council Resolution]
[299] OECD, *supra* note 296, at 2.
[300] OECD, *supra* note 296, at 51.
[301] Europol, *Joint Investigation Teams (JITs)* (Nov. 4, 2011), https://www.europol.europa.eu/content/page/joint-investigation-teams-989 (last visited Feb. 27. 2015) [hereinafter Europol JIT Manual].
[302] Europol, *Historical Background* (last visited Mar. 5, 2015), https://www.europol.europa.eu/content/page/JITs-history.

law of the Member State in which it operates."[303] The territory where the investigation will take place is determined by the location of evidence. It may span multiple countries and jurisdictions, thus "a number of people [may temporarily work] outside of their own Member States."[304]

JITs may also be created in countries outside of the EU[305] provided that a legal basis for the creation of the JIT exists.[306] A bilateral or multilateral MLAT can serve as that legal basis.[307] This is best illustrated in the U.S.-EU MLAT that entered into force in 2010. Article 5 of the treaty, which provides for the authorization and formation of JITs between each EU Member State and the U.S., states in relevant part: "Contracting Parties shall…take such measures as may be necessary to enable joint investigative teams to be established and operated in the respective territories of the United States of America and each Member State for the purpose of facilitating criminal investigations or prosecutions."[308] Because the U.S.-EU treaty is multilateral, certain enumerated provisions (like Article 5) listed therein are applied to pre-existing bilateral treaties between the U.S. and a specific EU Member State.[309] Consequently, incorporation gives the U.S. authority to formulate and operate JITs with EU Member states where a bilateral treaty does not explicitly grant such a right.

Once it is determined that a JIT is necessary for the successful execution of a MLAT request, a JIT Agreement is created to establish team members, duration, purpose, and

---

[303] EU MLAC, *supra* note 261, art. 13 at 11-13.
[304] Europol JIT Manual, *supra* note 301, at 8.
[305] There are currently 28 Member States in the European Union.
[306] Europol JIT Manual, *supra* note 301, at 5.
[307] Europol JIT Manual, *supra* note 301, at 5.
[308] Treaty on Mutual Legal Assistance, U.S.-E.U., art. 5, June 25, 2003, T.I.A.S No.10-201.1 [hereinafter U.S.-E.U. MLAT], *available at* http://www.state.gov/documents/organization/180815.pdf.
[309] Article 3, §1, paragraph (b) states, "that the provisions of this Agreement are applied in relation to bilateral mutual legal assistance treaties between Members States and the United States of America, in force at the time of entry into force of this Agreement under the following terms: Article 5 shall be applied to authorize the formation and activities of joint investigative teams in addition to any authority already provided under bilateral treaty provisions . . . " U.S.-E.U. MLAT *supra* note 308, at 5-6.

approach.[310] JITs follow a hierarchical structure such that "[t]he leader of the JIT team is a member of the law enforcement authorities in the Member State in which the team operates. If the JIT operates in multiple Member States, leadership of the JIT will change depending on where the investigation is being conducted at a given time."[311] This allows for a broad range of investigative power and information sharing whereby JITs become domestic and international surveillance mechanisms. Team members may "make direct requests of one another for use of investigative methods, without the need for further formal [Mutual Legal Assistance]."[312] They may also share information available in their home state relevant to the investigation provided that their national law permits this exchange.[313] The Joint Investigation Teams Manual[314] states that a team member may provide information such as "subscriber details, car registrations, and criminal records" to another team member without channeling the information through their respective Central Authorities.[315]

Cross-jurisdictional information sharing by international law enforcement agencies (LEAs) is firmly grounded in the mosaic theory of intelligence gathering.[316] Mosaic theory holds that,

> Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts.[317]

---

[310] Europol JIT Manual, *supra* note 301, at 23-24.
[311] OECD, *supra* note 296, at 52.
[312] OECD, *supra* note 296, at 52.
[313] OECD, *supra* note 296, at 52.
[314] The JIT Manual supplements the "existing Eurojust/Europol document ―Guide to EU Member States' legislation on Joint Investigation Teams". Europol JIT Manual, *supra* note 301, at 1.
[315] Europol JIT Manual, *supra* note 301, at 12.
[316] *See generally* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 Yale L.J. 628 (2005), *available at* http://www.yalelawjournal.org/note/the-mosaic-theory-national-security-and-the-freedom-of-information-act.
[317] *Id.* at 630.

Conceivably, evidence collected by JIT members could be pieced together such that the information creates a composite revealing the identity of a Tor user.[318] By legally obtaining disparate pieces of information with lower judicial procedural standards to be used together with information collected in the same manner by other JIT members, governments may gain access to information otherwise unavailable to them. Aggregating information in this manner raises privacy concerns as to what constitutes a search within the meaning of the Fourth Amendment.[319]

Anonymity within the Context of JITs

JITs have broad discretionary power in executing MLAT requests, particularly with regard to anonymous operations. That anonymity is foundational to the successful operation of law enforcement agencies highlights its' importance in the everyday fabric of our society. Just as law enforcement officers rely on operational anonymity for their safety, private citizens rely on anonymity tools like Tor for protection from violent abusers, identity thieves, and government intrusions. Somewhat ironically, the anonymity that frustrates law enforcement officers during the course of investigation is the same anonymity that law enforcement officers justify in their use of JITs.

JITs: the Irony of using Anonymity

In addition to establishing the creation of JITs for use in international criminal investigations, the EU MLAC also established parameters for the use of covert investigations by

[318] Cross-jurisdictional law enforcement agency collaboration may move towards de-anonymization, although de-anonymization would still be very difficult.
[319] *See supra* note 180.

these teams.[320] Within the context of JITs, anonymity functions on multiple frequencies. For example, the Council of the European Union determined that "cases of terrorism that require maximum security" are "good grounds for the protecting the identity of one or more members of the JIT."[321] Law enforcement agencies argue that team members need to operate "under covert of false identity"[322] for their protection (and presumably that of their families), and "to avoid disclosing details about other possible suspects still subject to other investigations."[323] Because covert operations offset law enforcement concerns about retaliation, cold trails, and suspects in the wind, anonymity becomes a safeguard to ensure the integrity of an investigation.

The Council of the European Union further determined that operational plans and organizational information in JIT Agreements are also deserving of anonymity. In drafting a JIT Agreement, consideration is given to the content listed therein as it "may be subject to disclosure proceedings."[324] Thus, in an effort to "reduce...the level of detail of the underlying JIT Agreement" the Council created an Operational Action Plan, "which is a separate document from the JIT Agreement, whose purpose is laying down *actual* operational details, strategy and planning."[325] Presumably, the Operational Action Plan is not subject to disclosure proceedings, although the Council is silent as to how the law treats this document. Ultimately, these safeguards pose a significant hardship on private citizens. Tor users who wish to challenge de-anonymization by a JIT are forced to confront the uncomfortable reality that any evidence collected by the JIT may be couched in double anonymity: the JIT may operate covertly and the

[320] EU MLAC, *supra* note 261, art. 14, at 12.
[321] Council Resolution, *supra* note 298, at 4.
[322] Article 14 Covert Investigations states,. "The requesting and the requested Member State may agree to assist one another in the conduct of investigations into crime by officers acting under covert or false identity (covert investigations)." EU MLAC, *supra* note 261, art. 14 §1, at 12.
[323] Europol JIT Manual, *supra* note 301, at 16.
[324] Europol JIT Manual, *supra* note 301, at 16.
[325] Europol JIT Manual, *supra* note 301, at 16. (emphasis added)

MLAT parties may stipulate to confidentiality. The intentional and malicious use of anonymity in this regard raises Sixth Amendment due process concerns. [326]

APPLICATION SECTION

A hypothetical case to show how MLATs and JITs work together

A law enforcement officer in France is investigating a case of identity theft and has evidence that the perpetrator is using Tor to anonymize his or her location and identity. To continue the investigation, the officer, using the existing U.S.-France mutual legal assistance treaty, petitions their Central Authority to request assistance from the Department of Justice Office of International Affairs in obtaining online records. Once received, the DOJ assesses compliance with U.S. domestic law and the Constitution, before accepting or denying the request. If accepted, the OIA hands the request to the appropriate U.S. Attorney's office, which works through the federal district court to obtain the ECPA warrants.[327] The FBI would serve the warrants on Tor and the ISP. Since Tor does not own or run the Tor network (it is run by volunteers), it has no information to provide the U.S. government, the U.S. Attorney's office, or to the officer in the France. Instead, any available information pertaining to the investigation would be filtered through the ISP to the FBI.

If the investigation so required, law enforcement agencies in France and the U.S would agree to set up a joint investigation team to help facilitate the collection of evidence. To do so, JIT members watch traffic going through the Tor relay in their respective jurisdictions. As evidence is compiled, the JIT members work together in an effort to de-anonymize a Tor user by

[326] The Sixth Amendment states in relevant part, "In all criminal prosecutions, the accused shall enjoy the right...to be informed of the nature and cause of the accusation; [and] to be confronted with the witnesses against him…" U.S. CONST. amend. VI.
[327] For more information on EPCA, see Section 1.

matching information collected from the relay and timing correlation attacks.[328] Once evidence collection is complete, the FBI would notify the district court and the U.S. Attorney's office. The district court and the U.S. Attorney's office would confirm the information collected complies with domestic law and the MLAT request. Once approved, the evidence is sent to OIA, who transmits it to the requesting foreign Central Authority.[329]

PART III

Legality of MLATs and JITs to de-anonymize Tor users

As noted above, the Constitution gives the Executive Branch the authority to negotiate foreign treaties.[330] Mutual legal assistance treaties, and presumably by extension joint investigation teams, have been ruled constitutional within the context of Fourth Amendment search and seizure protections. As such, it is legal to use MLATs and JITs in criminal investigations to de-anonymize a Tor user.[331] In *United States v. Verdugo-Urquidez*, the Supreme Court held that the Fourth Amendment has no extraterritorial application to searches of aliens[332] conducted outside of the United States.[333] The international nature of Tor's relay network lends itself toward the use of MLATs and JITs to de-anonymize users connected to on-going criminal investigations. U.S. persons using the Tor network are especially vulnerable to erosions of their

---

[328] *Supra* note 79.
[329] *See generally* STANFORD, *MLAT Flow Chart*, (2014), http://cyberlaw.stanford.edu/files/blogs/MLAT%20flowchart%20-%2012.19.14.pdf.
[330] *See supra* note 266.
[331] Although not a MLAT case, *United States v. Morrow* involved a conspiracy for the distribution of stolen and counterfeited securities across state and national lines. The court held,
Normal lines of communication between the law enforcement agencies of different countries are beneficial without question and are to be encouraged. Criminal conspiracies, as this case amply demonstrates, are sometimes international in scope, and the routine transmittal of the name and telephone number of a possibly valuable informant across national borders clearly is permissible under the fourth amendment.
United States v. Morrow, 537 F.2d 120, 140 (5th Cir. 1976).
[332] The *Verdugo-Urquidez* Court expanded on who constitute "people" within the meaning of the Fourth Amendment. The court suggested that "'the people' protected by the Fourth Amendment...refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).
[333] *Id.* at 275

Fourth Amendment protections. Because a Tor user and their location are anonymous, the government does not know that the MLAT request may lead to a Tor user in the United States. An argument could be made that MLATs and JITs (to the extent that they are used to execute the request) circumvent the particularity requirement of the Fourth Amendment in that the treaties don't require specificity.[334]

In *U.S. v. Getto*, the court convicted Getto, an American citizen, of conspiracy to commit mail and wire fraud against U.S. citizens. Getto was involved in a lottery telemarketing scheme based in Israel that targeted U.S. citizens.[335] Operating undercover, Federal Bureau Investigation agents traced telephone numbers and bank account information of the suspected conspirators to Israel.[336] Pursuant to the U.S.-Israel mutual legal assistance treaty, the FBI filed a request with the Israeli National Police (INP) to investigate.[337] The FBI agents shared the results of their preliminary investigation with the INP for use in the Israeli investigation.[338] Getto moved to suppress the evidence gathered by the INP. He argued that the FBI agents controlled the INP investigation to such an extent that it rendered the INP 'virtual agents' of the U.S. government.[339] In addition, Getto alleged that the INP conducted warrantless searches and surveillance abroad in violation of the Fourth Amendment.[340] The appellate court affirmed the district court's ruling that there was no violation of Getto's Fourth Amendment rights.[341] In the instant case, use of the preexisting U.S.-Israel MLAT to request evidentiary assistance was legal. Just as the FBI traced

---

[334] *See supra* note 259.
[335] United States v. Getto, 729 F.3d 221 (2d Cir. 2013).
[336] *Id.* at 227.
[337] *Id.* at 226.
[338] *Id.* at 231.
[339] United States v. Getto, 729 F.3d 221, 226 (2d Cir. 2013).
[340] *Id*.
[341] The holding states, "that the information in the record--the MLAT request, the information-sharing between American law enforcement and the INP, and American receipt of the fruits of the INP's investigation in Israel--reveals no cooperation 'designed to evade constitutional requirements.' but only successful coordinated law enforcement activity". *Id.* at 233.

bank account record and telephone information to suspected conspirators, so too could a law enforcement officer employ a similar strategy to de-anonymize a Tor user pursuant to an MLAT request. Arguably, U.S. persons using Tor should have a diminished expectation of Fourth Amendment privacy protections because online anonymity prevents the law enforcement officer from ascertaining whether or not the user is an U.S. citizen.[342]

De-anonymization of a Tor user is also legal where MLAT evidentiary requests are executed under the Wiretap Act.[343] In *U.S. v. Juan Vincent Gomez Castrillon*, defendants were charged with importing cocaine to the United States.[344] The U.S. obtained recorded telephone conversations from the Colombian government pursuant to a request made under the U.S.-Colombia MLAT.[345] Upon receipt of the request, law enforcement officials in Colombia "investigated the telephone numbers listed in the MLAT requests and identified additional telephone numbers believed to be of interest to the investigation, which numbers were then intercepted."[346] The defendants argued that court should suppress the evidence pursuant to the Fourth and Fifth Amendments.[347] The court held that "responding to an MLAT by conducting an investigation in one's own country does not render foreign officials agents of the United States," and therefore no constitutional challenge applied.[348]

Conceivably, law enforcement officials could argue that where a Tor user is implicated in an investigation, de-anonymizing them is in the interest of the investigation. This makes Tor

---

[342] In *United States v. Liersch*, an unreported case involving money laundering, the court held, "the fact that the United States has entered into Mutual Legal Assistance Treaties with Switzerland and Austria suggests that Liersch had no reasonable expectation of privacy in his foreign bank records." United States v. Liersch, No. 04CR2521, 2006 WL 6469421, *15 (S.D. Cal. June 26, 2006).
[343] 18 U.S.C. §§ 2510-2520. In *United States v. Maturo*, the court held, "When conducted in this country, wiretaps by federal officials are largely governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, *see* 18 U.S.C. §§ 2510–2520, which does not apply outside the United States." United States v. Maturo, 982 F.2d 57, 60 (2d Cir. 1992).
[344] United States v. Juan Vincent Gomez Castrillon, 2007 WL 2398810, *1 (S.D.N.Y. Aug. 15, 2007).
[345] *Id.* at 1.
[346] United States v. Juan Vincent Gomez Castrillon, 2007 WL 2398810, *2 (S.D.N.Y. Aug. 15, 2007).
[347] *Id.*
[348] *Id*. at 4.

users vulnerable to privacy infringements within the context MLATs and JITs. Fourth Amendment privacy protections of U.S. persons may be curtailed when evidence is collected pursuant to the terms of an MLAT agreement because users lack control over where the network bounces their signal and the government is unable to ascertain the location of the user, their citizenship or status.

THE FUTURE OF MLATS: AN AGGRESSIVE RESPONSE TO GROWING ISP REQUESTS

Criminal Division Assistant Attorney General Leslie R. Caldwell, in her testimony before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism, said,

> All the while, technological advances, including advances designed to protect privacy, such as *anonymizing software and encryption*, are being used to frustrate criminal or civil investigations and, perversely, protect the wrongdoers. Our cyber crimefighters must be equipped with the tools and expertise to compete with and overcome our adversaries.[349]

Of the necessary tools, AAG Caldwell noted that MLAT reform is necessary to "reduce the amount of time to comply with legally sufficient requests to a matter of weeks, as well as to strengthen the Department's relationships with [their] foreign law enforcement partners, particularly in regard to cyber investigations."[350] Reduction in the turnaround time for MLAT requests will allow the United States Government to increase its international global surveillance

[349] Leslie R. Caldwell, Asst. Att'y Gen., *Testimony before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism*, DEP'T. OF JUSTICE (July 15, 2014), http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-testifies-senate-committee-judiciary (emphasis added). The irony of presenting anonymizing software in a categorically negative light belies the fact that the U.S. government and law enforcement agencies not only use, but also depend upon anonymity software and confidentiality in the everyday operation of their jobs. According to the Tor website the software "...was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others." Tor, https://www.torproject.org/about/overview.html.en. MLATs also contain confidentiality provisions that allow the parties to keep confidential that a request for assistance has been made and the contents of that request. *See* U.S.-EU MLAT *supra* note 308, art. 10, at 19. Furthermore, the line of reasoning that suggests anonymizing software "protects the wrongdoers" does not recognize the range of other non-criminal uses anonymity software provides. For example domestic violence survivors rely on software like Tor to remain anonymous from their abusers.

[350] *Id.*

efforts through both the formation of JITs and presumably the enactment of new MLAT agreements. Nowhere is the push for reform more evident than the Justice Department's and the FBI's Fiscal Year 2015 (FY 2015) budgets as submitted to Congress.[351]

For FY 2015, the DOJ Criminal Division (DOJ/CRM) in conjunction with the FBI requested $24.1 million in program increases[352] for the implementation of a Mutual Legal Assistance Treaty Process Reform; the goal of which is to "prevent terrorism and promote the Nation's security consistent with the rule of law."[353] To achieve this goal, the proposed reform and increased funding will (1) permit the DOJ/CRM Office of International Affairs (OIA) "to itself execute foreign requests for assistance in criminal and counterterrorism cases, rather than having to rely upon local U.S. Attorney's Offices,"[354] (2) foster greater "reciprocal cooperation" in complying with MLAT requests from the USG, and (3) allow the DOJ and its divisions and agencies (OIA, CCIPS,[355] FBI) to create MLAT intake units,[356] with dedicated personnel. These

[351] The 2015 Fiscal Year spans October 1, 2014 through September 30, 2015. *See* U.S. Dep't of Justice (DOJ) *FY 2015 Budget Request for Mutual Legal Assistance Treaty Process Reform (Overview)* for more information on the DOJ and FBI budgets, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf. *See also* the *DOJ Criminal Division FY 2015 President's Budget and Performance Submission*, 18-27, http://www.justice.gov/sites/default/files/jmd/legacy/2013/11/14/crm-justification.pdf, and the *FBI FY 2015 Authorization and Budget Request to Congress,*78, section 5-4, http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/03/fbi-justification.pdf for information pertaining to specific budgets. For information on past DOJ budgets *see generally* http://www.justice.gov/about/budget-and-performance.

[352] These increases include: (1) $19.6 million for the Criminal Division Mutual Legal Assistance Reform; (2) $1.3 million for the United States Attorney's Offices in the District of Columbia and the Northern District of California to assign dedicated attorney's and support personnel to OIA's centralization project; and (3) $3.2 million for the FBI to establish a dedicated MLAT unit for intake, tracking, and management of all MLAT requests, as well as, training and ISP outreach. DOJ, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf (last visited Mar. 5. 2015).

[353] *FY 2015 President's Budget and Performance Submission*, DOJ Criminal Division 18 (2014), http://www.justice.gov/sites/default/files/jmd/legacy/2013/11/14/crm-justification.pdf [hereinafter DOJ FY 2015 Budget].

[354] *Id.*

[355] Computer Crimes and Intellectual Property Section.

[356] The proposed unit will centralize and standardize FBI responsibilities related to MLAT requests. *FY 2015 Authorization and Budget Request to Congress*, FBI 78 (Mar. 2014), http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/03/fbi-justification.pdf.

units will allow the DOJ to respond more efficiently to foreign assistance requests, specifically those involving Internet Service Provider (ISP) records.

The number of foreign MLAT requests for computer records has increased significantly since the 9/11 terrorist attacks, when they numbered under 200.[357] As of 2012, the Criminal Division's OIA received nearly 1000 MLAT requests for computer records,[358] evidencing a collective global trend in the prosecution of cyber crimes.[359] Google, for example, maintains that if an MLAT approved by DOJ CRM/OIA satisfies their policies, they will respond to it.[360] It is important to note that the legal instrument used to fulfill the MLAT request dictates what information an ISP is legally required to make available for criminal investigative purposes. This information may include: subscriber registration information (e.g., name, account creation information, associated email addresses, phone number), sign-in IP addresses and associated time stamps, non-content information (such as non-content email header information), and/or email content.[361]

Ultimately, the creation of parallel intake units within OIA and FBI, and an increased focus on counterterrorism measures, with specific emphasis on the use of MLATs for ISP records, is evidence of a trend toward heightened surveillance of private citizens. It also illustrates a desire to control how governments are requesting and accessing user data. As this trend progresses, Tor will continue to engage researchers to track how increased surveillance measures may create new attack vectors for the U.S. Government and other foreign governmental entities.

---

[357] DOJ FY 2015 Budget *supra* note 353, at 21.
[358] DOJ FY 2015 Budget *supra* note 353, at 21.
[359] While the number of MLATs, generally, has increased by 60% over the past decade, the growth of foreign requests for computer records has increased ten fold. In 2012, the Department received roughly 3000 MLAT requests, 1000 of which were for ISP records. DOJ FY 2015 Budget *supra* note 353, at 20-21.
[360] VERIZON, http://transparency.verizon.com/us-report (last visited Mar. 5. 2015).
[361] GOOGLE, http://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited Mar. 5 2015).

CONCLUSION

Heightened global surveillance, as exercised through MLATs and JITs, could mean less anonymity for Tor users from both U.S. and international governments. As these tools become more pervasive, it's important for private citizens and organizations like Tor to continue collaborating thereby forcing the government to recognize the beneficial uses of anonymity software. Without this collaboration, encroachments into the private lives of citizens will accelerate. This is best illustrated in the use of the Third Party Doctrine.

Section 4

The Third Party Doctrine

Question Presented: Since its inception, the third party doctrine has been applied to various entities that provide services. In 2012, however, Justice Sotomayor of the Supreme Court said, in a concurring opinion, that the third party doctrine is "ill suited to the digital age."[362] Given that Tor provides a service on the Internet with the Tor Browser, how does or may the third party doctrine apply to it?

BRIEF ANSWER

The third party doctrine has been crucial in the development of Fourth Amendment search and seizure procedures and mechanisms. The third party doctrine allows the government to obtain certain types of information on people from third parties, to whom the information is disclosed, without a search warrant. There is criticism of, as well as support for, the third party doctrine. However, there is indication that the third party doctrine could no longer be a vehicle for the government to use. Most likely, Tor cannot be considered a third party for the purposes of the third party doctrine because users only disclose a limited amount of information to Tor by design, and because the users have a reasonable expectation of privacy in the information they provide. Even if Tor was construed as a third party, there is proposed legislation that would effectively invalidate the doctrine.

INTRODUCTION

The third party doctrine is a legal doctrine upheld by the Supreme Court that states that people who voluntarily give certain types of information to third parties, such as banks, phone companies, Internet service providers (ISP), and email servers have no constitutionally protected

[362] United States v. Jones, 132 S. Ct. 945, 948 (2012) (J. Sotomayor, concurring).

right to privacy in that information.[363] When people convey the information to third parties, it is considered exposed to the public. The specific information then loses its Fourth Amendment protections against unreasonable search and seizure without probable cause, thus allowing the U.S. government to obtain the information from the third parties without a judicial search warrant.[364]

Tor has not yet received a request from the government to provide users' information, such as IP addresses, under the third party doctrine. However, the possibility exists that the government could ask Tor for user information for the purpose of identifying users pursuant to the third party doctrine.[365] The following is a general discussion of the third party doctrine and how it has developed into what it is today, followed by an overview of the arguments for whether Tor could be considered a third party, and thus subject to the third party doctrine.

DEVELOPMENT OF THE THIRD PARTY DOCTRINE

The Fourth Amendment states that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[366] The courts have construed a right to privacy from this Amendment. In the modern era, the courts and legislature have attempted to categorize exactly what is covered as private under the Fourth Amendment.

[363] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[364] Katz v. United States, 389 U.S. 347, 351 (1967).
[365] Interview with Andrew Lewman, Executive Director and Secretary and Treasurer of the Board, Tor Project, in Boston, MA (September 26, 2014).
[366] U.S. CONST. AMEND. IV.

Fourth Amendment in General - Pre-Katz era

The Articles of the Constitution and the Bill of Rights are devoted to the structure and procedure of the United States government.[367] The Fourth Amendment does not specifically mention any affirmative rights to privacy, but rather details a procedural standard to which government needs to adhere.[368] In 1886, the Supreme Court decided *Boyd v. United States*, where the court abandoned the traditional procedural view of the Fourth Amendment. Instead, the court construed an overarching individual right to privacy in private property that limited the government's ability to intervene in affairs surrounding property rights.[369] After *Boyd*, the Fourth Amendment was understood to protect property rights and protect against government trespass into private property.[370] Although argued under the theory of trespass against private property,[371] the court decided *Katz v. United States* on different grounds.[372]

Katz

Our current notion of an affirmative right to privacy in tangible and intangible things outside of private property was first discussed in the United States Supreme Court case *Katz v. United States*.[373] *Katz* dealt largely with intangible things, such as a conversation, and defined a

[367] JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 88-103 (1980), *reprinted in* FARBER, ESKRIDGE, FRICKEY, SCHACTER, CASES AND MATERIALS ON CONSTITUTIONAL LAW THEMES FOR THE CONSTITUTION'S THIRD CENTURY 161-67 (5th ed. 2014).
[368] *Id.* at 163.
[369] Boyd v. United States, 116 U.S. 616, 623 (1886). as explained in: Christian M. Halliburton, *How Privacy Killed Katz: A Tale of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm*, 42 AKRON L. REV. 803, 814-20, (2009).
[370] Christian M. Halliburton, *How Privacy Killed Katz: A Tale of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm*, 42 AKRON L. REV. 803, 814-20, (2009). *See e.g.*, Olmstead v. United States, 277 U.S. 438 (1928); *See also* Goldman v. United States, 316 U.S. 129 (1942).
[371] *Olmstead* and *Goldman* are just two of the numerous cases that reaffirmed the notion that the Fourth Amendment applied only when there was a physical trespass on private property. Where there was no physical intrusion or seizure of personal property, the Fourth Amendment did not apply.
[372] Katz v. United States, 389 U.S. 347 (1967).
[373] *Id.*

reasonable expectation of privacy in certain types of information.[374] Information voluntarily conveyed to a third party, for instance, is not protected from warrantless search and seizure under the Fourth Amendment. This is the foundational principle of the third party doctrine, which is largely a product of *Katz* and subsequent cases interpreting and expanding *Katz*.

In 1965, Katz was observed using three public telephone booths at roughly the same time, every day.[375] Federal Bureau of Investigation (FBI) agents subsequently attached microphones, connected to a wire recorder, to the outside of the booths, and only turned the recorders on when Katz approached the booths or occupied the booths.[376] Based on the information contained in the recordings of Katz's conversations, the FBI obtained a judicial search warrant to search Katz's apartment and collected more evidence that subsequently led to Katz's arrest and conviction under a California anti-betting statute.[377] The Ninth Circuit Court of Appeals affirmed the conviction.[378] This decision was based on the fact that the government did not physically intrude into the phone booths that Katz occupied.[379] Thus, given the precedent, there was no violation of Katz's Fourth Amendment rights.[380]

Upon Supreme Court review, the arguments revolved around whether a phone booth was a constitutionally protected area, and whether physical intrusion of a constitutionally protected area was necessary for Fourth Amendment protection.[381] The court declined to decide the case based upon these notions and instead stressed that the Fourth Amendment protects *people* and not places.[382] Furthermore, the court reinterpreted the precedent and stated that the Fourth

[374] Katz v. United States, 389 U.S. 347 (1967).
[375] Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966) *rev'd by* Katz v. United States, 389 U.S. 347 (1967).
[376] *Id.*
[377] Katz v. United States, 389 U.S. 347, 348 (1967).
[378] Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966).
[379] *Id.*
[380] *Id.*
[381] Katz v. United States, 389 U.S. 347, 349 (1967).
[382] *Id.*

Amendment does not translate into a general overarching right to privacy in everything.[383] The Fourth Amendment, however, does provide people with a right against certain kinds of governmental intrusions.[384]

The court overruled the traditional trespass doctrine and determined that the government, in listening to and recording Katz, violated the Fourth Amendment because their actions constituted a search and seizure.[385] They reasoned that although the Fourth Amendment does not provide an overarching right to privacy, what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[386] In this case, it did not matter that the government did not physically intrude on the booth because Katz had justifiably relied on the privacy of the booth.[387] In his concurrence, Justice Harlan explains the justifiable reliance on privacy as a reasonable expectation of privacy.[388] Justice Harlan further explained that for there to be a reasonable expectation of privacy: (1) a person has to have an actual (subjective) expectation of privacy; and (2) said expectation is one that society is prepared to recognize as reasonable.[389]

Reasonable Expectation of Privacy

While the majority opinion of *Katz* did not include Justice Harlan's standard for reasonable expectation of privacy, it would not be long before his iteration of the test became the standard for all Fourth Amendment cases and many state constitutional cases. Twelve years after *Katz*, Justice Blackmun incorporated Justice Harlan's two-pronged test for reasonable

[383] Katz v. United States, 389 U.S. 347, 350 (1967).
[384] *Id.*
[385] *Id.* at 353.
[386] *Id.* at 351.
[387] Katz v. United States, 389 U.S. 347, 351 (1967).
[388] *Id.* at 360.
[389] *Id.* at 361.

expectation of privacy into the majority opinion of *Smith v. Maryland*.[390] People continue to have a reasonable expectation of privacy in their private property, including their houses, papers, and effects.[391] They also have a reasonable expectation of privacy in public places that are designed to be private, such as public restrooms, tents and campsites, and phone booths.[392] However, the most important developments in constitutional privacy cases have surrounded papers, effects, and personal information that have been voluntarily conveyed to third parties.

Between Katz and Smith

After *Katz*, three Supreme Court decisions solidified the use of a reasonable expectation of privacy in determining third party cases. The first was *United States v. White*, which decided whether or not oral conversations made in person were protected by the Fourth Amendment. In *White*, information obtained by an informant wearing a wire during a conversation with White was held to be admissible as evidence and not a violation of White's Fourth Amendment rights.[393] The court reasoned that the informant was not an uninvited eavesdropper, unlike the FBI in *Katz*, but rather was a party to the conversation. As such, the informant was free to report what he had heard to the authorities, and therefore White had assumed the risk of this occurring and had no justifiable expectation of privacy.[394]

The second case was *Couch v. United States*, a case largely arguing against self-incrimination under the Fifth Amendment.[395] However, the Supreme Court provided valuable insights into Fourth Amendment jurisprudence. The defendant had argued, in small part, that she

---

[390] Smith v. Maryland, 442 U.S. 735, 740 (1979).
[391] U.S. CONST. amend. IV.
[392] *See e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967); *See also* Doyle Baker, *Search and Seizure: Reasonable Expectation of Privacy in Tents and Campsites*, 66 A.L.R.5TH 373 (1999); *See also* Michael R. Flaherty, *Search and Seizure: Reasonable Expectation of Privacy in Public Restroom*, 74 A.L.R.4TH 508 (1989).
[393] United States v. White, 401 U.S. 745, 753-54 (1971).
[394] *Id.* at 750-52.
[395] Couch v. United States, 409 U.S. 322 (1973).

had an expectation of privacy when she turned over business records to her accountant for tax return preparations.[396] The court held that "there can be little expectation of privacy where [tax] records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."[397] Couch therefore could not rely on a Fourth Amendment argument because she voluntarily provided her accountant with the records, while knowing that the information contained in the records would be disclosed to the government.[398]

The third case was *United States v. Miller*, which dealt with transactional records. Miller was under investigation for possible involvement in an illegal whiskey distillery business, and the government subpoenaed records from all of Miller's banks to gain evidence of potential involvement.[399] The banks complied without notifying Miller of the subpoenas, and because of the information contained in the records, Miller was convicted of various crimes pertaining to the operation of an unregistered whiskey distillery.[400] The question on appeal to the Supreme Court was whether a subpoena was sufficient to provide access to the records.[401] Miller argued that the bank kept copies of personal records that he gave to the bank for a limited purpose, and in which he retained a reasonable expectation of privacy under *Katz*.[402]

First, Miller had no legitimate expectation of privacy in the records due to the Bank Secrecy Act.[403] Next, pursuant to *Katz*, the court stated that "[w]hat a person knowingly exposes

[396] Couch v. United States, 409 U.S. 335 (1973).
[397] *Id.*
[398] *Id.* at 322.
[399] United States v. Miller, 425 U.S. 435, 437 (1976).
[400] *Id.* at 436.
[401] *Id.* at 437-39.
[402] *Id.* at 442.
[403] 12 U.S.C. § 1829b(a)(1) (2011). The Bank Secrecy Act states that Congress finds that adequate records maintained by banking institutions have a high degree of usefulness in criminal, tax, and regulatory investigations or proceedings. *Id.* The court in *Miller* thus concluded that since Congress explicitly stated that a use of these records

to the public . . . is not a subject of Fourth Amendment protection."[404] The court then used the approach outlined in *Couch* by looking at the nature of the documents. The bank records were not "confidential communications," but rather "negotiable instruments required to transact business."[405] Furthermore, all of the documents contained information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[406] The court then cited to *White* and stated that "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[407] The court concluded with a statement that would define the third party doctrine and promulgate its use,

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[408]

As a result, the information obtained was not subject to Fourth Amendment protections and the court upheld Miller's conviction.[409]

Smith

Three years after *Miller*, the Supreme Court decided *Smith v. Maryland*.[410] In *Smith*, a woman had been robbed and later received obscene phone calls from a man who identified himself as the robber.[411] The police identified Smith as a suspect as a result of the description

---

was inevitable in various government proceedings, a person could hold no expectation of privacy in those records. United States v. Miller, 425 U.S. 435, 442 (1976).

[404] United States v. Miller, 425 U.S. 435, 442 (1976) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[405] *Id.*

[406] *Id.*

[407] United States v. Miller, 425 U.S. 435, 443 (1976) (quoting United States v. White, 401 U.S. 745, 751-52 (1971)).

[408] *Id.*

[409] *Id.* at 437-39.

[410] Smith v. Maryland, 442 U.S. 735 (1979).

[411] *Id.* at 737.

provided by the victim.[412] However, to obtain more concrete evidence, the police requested that the telephone company install a pen register at its central office to record the numbers dialed from Smith's house.[413] The pen register revealed that Smith was in fact dialing the victim's telephone number, and he was subsequently arrested and indicted.[414] The issue decided by the Supreme Court was whether or not the use of pen registers was a violation of Smith's Fourth Amendment rights.[415] The court relied on the two-pronged test that Justice Harlan presented in *Katz*[416] to determine this issue.[417]

The court first determined that a person could have no actual expectation of privacy since dialing the telephone number required an operator to "switch"[418] to complete the calls. Additionally, telephone companies routinely use pen registers and similar devices for various business operations.[419] This assumes that one has knowledge of how telephone calling operates, and thus voluntarily conveys the information. Smith argued that he had an expectation of privacy since he was conducting the call from the privacy of his home.[420] The court rejected this argument, stating that even if a subjective expectation existed, the objective portion of the test was not satisfied.[421] The expectation of privacy was not one that society was prepared to

[412] Smith v. Maryland, 442 U.S. 735, 737 (1979).
[413] *Id.*
[414] *Id.*
[415] *Id.* at 738.
[416] Katz v. United States, 389 U.S. 347, 360 (1967). There exists a reasonable expectation of privacy when: (1) a person has to have an actual (subjective) expectation of privacy; and (2) said expectation is one that society is prepared to recognize as 'reasonable.' *Id.*
[417] Smith v. Maryland, 442 U.S. 735, 740 (1979).
[418] Switching via switchboards and physical human operators was the only way to complete calls before the digital age. So when a person picked up their phone, they were connected to an operator who would ask for the recipient's telephone number and manually connect the phone lines via the switchboard. J. B. Calvert, *Basic Telephone* http://mysite.du.edu/~jcalvert/tech/phones.htm (Mar. 8, 2015).
[419] Smith v. Maryland, 442 U.S. 735, 742 (1979).
[420] *Id.* at 743.
[421] *Id.* at 743.

recognize as reasonable, since a person has no legitimate expectation of privacy in information they voluntarily turn over to third parties, as outlined in the previous cases.[422]

Information that is Subject to the Third Party Doctrine

Since *Smith*, the courts have applied the third party doctrine to a wide variety of third parties.[423] However, not all of the information provided to a third party is subject to the doctrine. The distinction between content data and non-content data is one of the most notable distinctions between what has been considered private information and what has been considered subject to the third party doctrine. Content data is defined as "any information concerning the substance, purport, or meaning of that communication."[424] Everything else, including transactional information, is considered non-content data.

Historically, the 1877 case *Ex parte Jackson* outlined that the contents of a mailed letter were protected under the Fourth Amendment, while the address on the outside was not protected.[425] Similarly, in *Katz*, the contents of a conversation were protected, and the decision rested on the premise that the *content* of the phone call was expected to be private.[426] However, the phone number dialed to connect a telephone call was not protected.[427]

---

[422] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[423] The following types of information are some that have been held as not subject to Fourth Amendment protection and thus have been subject to the third party doctrine: *See e.g.*, United States v. Willis, 759 F.2d 1486, 1498 (1985) (motel registration records). *See also* United States v. Phibbs, 999 F.2d 1053, 1077-78 (1993) (credit card statements). *See also* Kyllo v. United States, 533 U.S. 27, 44-46 (2001) (utility bills); *See also* United States v. Hamilton, 434 F. Supp. 2d 974, 979 (2006) (employment and power records). *See also* United States v. Graham, 846 F. Supp. 2d 384, 403 (D. Mar. 2012) (historical cell-site locations). *See also* United States v. Stanley, 753 F.3d 114 (2014) (internet usage records). *See also* United States v. Hambrick, 225 F.3d 656 (2000) (IP address, subscriber name and contact information). *See also* United States v. Bynum, 604 F.3d 161 (2010) (IP address, email, phone number, and subscriber information). *See also In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d), 830 F. Supp. 2d 114 (D. Va. 2011) (subscriber information from social media).
[424] 18 U.S.C. § 2510(8) (2002).
[425] *Ex parte* Jacksons, 96 U.S. 727 (1877).
[426] Katz v. United States, 389 U.S. 347, 351 (1967).
[427] Smith v. Maryland, 442 U.S. 735 (1979).

While the Supreme Court has not specifically addressed the distinction, the appellate courts have drawn a distinction between content and non-content data. In *United States v. Warshak*, the Sixth Circuit held that the content of emails is subject to Fourth Amendment protections.[428] The Ninth Circuit in *United States v. Forrester* held that recipient addresses of emails, IP addresses of destination websites, and the aggregate data that a person transmits to/from a certain IP address are not protected under the Fourth Amendment.[429] Furthermore, when customers use a communications service provider (CSP) or ISP, they voluntarily relinquish their reasonable expectation of privacy. The subscribers rely on Internet technology to access the service, indicating an intention to relinquish control of whatever information would be necessary to complete their communication.[430] This distinction stems largely from the notion of what the third party needs to know to complete the communication, as compared to what is being communicated. More specifically, it is "the difference between the recipient of the information and companies that act merely as a conduit or intermediary between two people communicating with each other."[431]

Information transmitted to a third party for their own transactional records provides another distinction as to what is subject to the third party doctrine and what is not subject to the third party doctrine. Regarding historical cell site data, which is often data collected by a telecommunications service provider, several courts have recognized that although the data allowed the government to paint an intimate picture of the defendant's whereabouts over an

[428] United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).
[429] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).
[430] *In re* Application of the United States for an Order Pursuant to 18 U.S.C. 2703(d), 830 F.Supp.2d 114, 133 (E.D.Va. 2011).
[431] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.

extended period of time, the data was still subject to the third party doctrine.[432] The rationale was that the cell site records were business records and the provider was a party to the transaction, as the cell site data was transmitted only to them.[433] Much of the case law surrounding historical cell site data cites to *Jones* as the basis for their decision.[434]

Jones

In *United States v. Jones*, the court revisited the basic notions of expectations of privacy.[435] In 2004, law enforcement officers (LEOs) began investigating Jones for suspicion of drug trafficking.[436] To aid the investigation, the LEOs obtained a warrant to place a GPS tracker on Jones' wife's car, but due to a failure in following the limitations of the warrant,[437] the installation became warrantless.[438] The LEOs collected data for a period of 1 month, 24 hours per day.[439] The data then linked Jones to a large amount of money and drugs.[440] The government successfully convicted Jones of conspiracy to distribute and possess cocaine, but the Court of

---

[432] *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013). *See also In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 449-50 (S.D.N.Y. 2005). *See also* United States v. Graham, 846 F. Supp. 2d 384, 403 (D. Mar. 2012). *But see* Commonwealth v. Augustine, 4 N.E.3d. 846, 865 (Mass. 2014); State v. Earls, 70 A.3d 630, 643-44 (N.J. 2013). There have been several court decisions that have found a reasonable expectation of privacy when the historical cell site data is collected for a large enough period of time so as to enable law enforcement to piece together an intimate picture of the individual's daily life. Commonwealth v. Augustine, 4 N.E.3d. 846, 865 (Mass. 2014). There are two possible methods for law enforcement to obtain historical cell cite data: through the third party doctrine or with a warrant. The courts must establish if the amount of amount of time that law enforcement seeks to obtain is reasonable in order to determine which method is appropriate to authorize law enforcement access to the data. The temporal line that has been drawn, at least in Massachusetts, is between twenty nine hours and two weeks. Commonwealth v. Augustine, 4 N.E.3d. 846, 865 (Mass. 2014); Commonwealth v. Princiotta, No. 2009-0965, 2014 WL 5317765, at *2-4 (Mass. Sup. Oct. 9, 2014).

[433] *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013).

[434] *See e.g.* Commonwealth v. Augustine, 4 N.E.3d. 846, 865 (Mass. 2014); *See also* State v. Earls, 70 A.3d 630, 643-44 (N.J. 2013).

[435] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[436] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[437] The warrant specified that the GPS device could be installed within 10 days in the District of Columbia, however law enforcement installed the device on the 11th day while the car was parked in Maryland and not in the District of Columbia. United States v. Jones, 132 S. Ct. 945, 948 (2012).

[438] *Id.* at 946.

[439] United States v. Jones, 132 S. Ct. 945, 946 (2012).

[440] *Id.*

Appeals reversed the conviction on the grounds that the installation of the GPS device and the subsequent use of the data was a Fourth Amendment violation.[441] The Supreme Court granted certiorari.[442]

The Supreme Court agreed that installation of the GPS device and subsequent use of the data constituted a search within the scope of the Fourth Amendment.[443] However, the justices had varying opinions as to why it was a Fourth Amendment violation. Justice Scalia wrote the majority opinion and held that the installation and use of the GPS device was a search because the police officers invaded Jones' car when they installed the transmitter.[444] Therefore, under the traditional trespass doctrine of the Fourth Amendment, which was the standard prior to *Katz*, the judgment of the appellate court was affirmed.[445] While the majority relied on the trespass doctrine in making the decision, they noted that where no physical trespass occurs as with wireless surveillance, the *Katz* standard still applied.[446]

Justice Sotomayor, in her concurrence, noted several issues that the majority opinion failed to address.[447] First, Sotomayor noted that the real issue in *Jones* was whether police agencies can use the warrantless acquisition of GPS or other technological location data in an investigation.[448] She specifically addressed the issue that GPS monitoring can generate a precise and comprehensive record of a person's familial, political, professional, religious, and sexual

[441] United States v. Jones, 132 S. Ct. 945, 949 (2012).
[442] *Id.*
[443] *Id*. at 952-53.
[444] *Id.* at 952.
[445] *Id.* at 953. Five justices joined in the majority opinion, one of whom was Justice Sotomayor, who submitted a concurring opinion. The other four justices concurred in the judgment but criticized Justice Scalia's revitalization of the trespass doctrine, as it was clearly overruled in *Katz*. This decision, written by Justice Alito, arrived at the conclusion by applying the reasonable expectation of privacy test. United States v. Jones, 132 S. Ct. 945, 957-58 (2012) (Alito, J., concurring in judgment).
[446] United States v. Jones, 132 S. Ct. 945, 953 (2012).
[447] United States v. Jones, 132 S. Ct. 945, 954-58 (2012) (Sotomayor, J., concurring).
[448] *Id.* at 954.

associations.[449] She alludes to the idea that if people were aware of the extensive amount of information that could be gathered and used at a later date, they would complain and cite a reasonable expectation of privacy in their movements and associations.[450]

The second problem that Sotomayor pointed out was that this type of location monitoring was possible in the past without warrants, but required an immense amount of resources and manpower to achieve the same result as a low cost GPS device.[451] She noted that modern technology has allowed law enforcement officers to evade the ordinary checks, such as resource allocation and community hostility, that constrain abusive law enforcement practices.[452] The low cost GPS tracking could provide the government with a "quantum of intimate information" that could potentially lead to an alteration of "the relationship between citizen and government in a way that is inimical to democratic society."[453]

Lastly, Justice Sotomayor noted that the third party doctrine may need to be reviewed because of the assumption that people have no reasonable expectation of privacy in the information that they voluntarily disclose to third parties.[454] She heralds this approach as ill suited to the digital age since most people reveal a great deal of information to neutral third parties within the course of a day while going about mundane tasks.[455] The current state of the third party doctrine as applied in a technological aspect, is uncertain as more criticisms have arisen.

---

[449] United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring).
[450] *Id.* at 955-57.
[451] *Id.* at 955.
[452] *Id.* (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).
[453] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas–Perez, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring)).
[454] *Id.* at 957.
[455] *Id.* at 957-58.

SUPPORT FOR THE THIRD PARTY DOCTRINE

Since its inception, the third party doctrine has incurred both criticism and praise. Supporters of the third party doctrine suggest that it is necessary because: (1) it is consistent with the rest of the Fourth Amendment case law[456] and (2) it maintains the technological neutrality of the Fourth Amendment rules through the equilibrium-adjustment theory.[457] Tor is an example of a technological development that exemplifies this equilibrium-adjustment theory. If Tor is considered a third party, it could be required to provide information about its users and their activity.

The third party doctrine is consistent with Fourth Amendment case law

The first argument is that the third party doctrine is on point with current Fourth Amendment case law. While the Fourth Amendment offers protection against unreasonable searches and seizures in certain circumstances, many public acts are not protected under the Fourth Amendment.[458] Courts that have found that the government's actions violate the Fourth Amendment have also held that the defendants did not have a reasonable expectation of privacy. For example, in *California v. Greenwood*, the court held that when the defendant left plastic trash bags in front of his house to be collected, he no longer had a reasonable expectation of privacy in his trash because he had discarded it in an area where the public could access it.[459]

---

[456] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.
[457] Orin S. Kerr, *An equilibrium-adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476, 487-488 (2011). The theory is that when technology, in particular, is developed that limits law enforcement's capabilities to gather evidence in the same way as prior to the technology's development, the courts will adjust the equilibrium and construe the Fourth Amendment more loosely. This enables the government to recover for the loss of capabilities as a result of the technology. The same occurs when the opposite happens. If technology is developed that enhances law enforcement's capabilities, the courts will adjust the equilibrium and construe the Fourth Amendment more broadly to ensure that the technology is not abused by law enforcement.
[458] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.
[459] California v. Greenwood, 486 U.S. 35, 37 (1988).

Therefore, the police could search the trash bags for contraband or other evidence of criminal activity.[460] Without a reasonable expectation of privacy, Greenwood's trash could not be protected under the Fourth Amendment.[461] Similarly, individuals who voluntarily disclose their information to a third party no longer have a reasonable expectation of privacy in that information, and therefore are not protected by the Fourth Amendment. People rely on consistent standards, so it is beneficial for the court to continue their Fourth Amendment jurisprudence even under the guise of reasonable expectation of privacy.

The third party doctrine maintains technological neutrality through the equilibrium-adjustment theory

In the same vein, Orin S. Kerr, a professor of law at the George Washington University Law School, suggests that the third party doctrine helps maintain technological neutrality of Fourth Amendment rules.[462] Without the third party doctrine, criminals could hide their otherwise public transactions behind third party services due to developments in technology.[463] The third party doctrine counteracts anonymity by removing Fourth Amendment protections, thereby holding criminals accountable for their actions and maintaining technological neutrality.[464]

The conflict between protecting individuals' privacy rights and ensuring security through deterrent and retributive forces of criminal law has existed since the inception of the Fourth Amendment.[465] In *Lee v. Carlson*, the court held that the Fourth Amendment does not protect a prisoner's right to privacy during phone conversations because security and order need to be

[460] California v. Greenwood, 486 U.S. 35, 37 (1988).
[461] *Id.*
[462] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009),
[463] *Id.* at 564.
[464] *Id.* at 564.
[465] *Id.* at 564.

preserved in the institution and in the public arena.[466] Since then, the development of technology has caused the balance between privacy and security to shift.[467] The doctrine requires third parties to provide certain kinds of information about their users to the government without a probable cause warrant, thereby connecting individuals to their online crimes and stripping away their Fourth Amendment protections.[468] Without the third party doctrine, individuals could more easily avoid detection when conducting illegal activities online from the sanctuary of their own home. The doctrine acts as a check to prevent criminals from concealing their criminal activity behind third parties as a result of technological advances.[469] This restores the Fourth Amendment balance between privacy and security.[470]

Smith is an example of how the third party doctrine provided equilibrium-adjustment theory to maintain technological neutrality.[471] In this case, described above, police used a pen register to record the phone number that Smith was dialing. Smith dialed the victim's phone number on several occasions, which helped the police obtain a probable cause warrant to search his home. The government proved that the defendant was in fact the robber because of the phone calls he had placed to the victim's residence. He was subsequently arrested and convicted.[472]

Prior to the advent of telephone technology, Smith would have had to physically go to the victim's home to contact her. In that situation, the police would have had to physically follow him to connect him to the crime. Without the police's ability to install the pen register, the police would have no way to connect Smith with the crime he had committed. The third party doctrine gave the police the ability to record the phone numbers that Smith was dialing and allowed the

[466] Lee v. Carlson, 645 F. Supp. 1430, 1438 (S.D.N.Y. 1986) *aff'd*, 812 F.2d 712 (2d Cir. 1987) *abrogated on other grounds* McGann v. State of New York, 77 F.3d 672 (2d Cir. 1996).
[467] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009),
[468] *Id.* at 564.
[469] *Id.* at 564.
[470] *Id.* at 564.
[471] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[472] *Id.*

police to arrest him.[473] This could not have occurred without the third party doctrine because in order to obtain a warrant, the police would have had to observe Smith interacting with the victim, which was impossible. Furthermore, without the third party doctrine, Smith could have evaded arrest. Thus, the third party doctrine maintains technology neutrality.

CRITICISMS OF THE THIRD PARTY DOCTRINE

Despite the support for the third party doctrine, critics have identified three different propositions regarding the doctrine's application. First, "privacy is not an all-or-nothing proposition,"[474] in so far as when a person reveals their information to a third party, the person cannot lose *all* privacy protections associated with that information. Second, the third party doctrine may provide an avenue for the government to circumvent longstanding privacy protections that are afforded by the Fourth Amendment.[475] Lastly, the third party doctrine rests on the premise that information is provided voluntarily to third parties. However, this is not necessarily true, as one must absolutely relinquish personal information to third parties to be an active participant in modern society.[476]

Privacy is not be an all or nothing proposition

The first argument examines whether or not privacy is relinquished once the information is disclosed to another person, company, or revealed in a public space.[477] Justice Marshall, in his dissent in *Smith*, wrote that "privacy is not a discrete commodity, possessed absolutely or not at

[473] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[474] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.
[475] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009),
[476]Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.
[477] *Id.*

all."[478] This suggests that people who disclose information to third parties such as banks or phone companies, for limited business purposes, retain a privacy interest in the disclosed information. People should be able to disclose information to third parties without worrying about the information becoming public.

Furthermore, courts have differed in their rulings on what exactly satisfies the reasonable expectation of privacy standard. For example, the holdings in *Katz*[479] and *Smith*[480] illustrate the difference between information that is considered content data versus non-content data. *Katz* held that the content of a conversation is protected under the Fourth Amendment, while *Smith* held that the telephone numbers dialed are not protected. However, since the development of technology and the mosaic theory, courts have recognized the possibility of painting an intimate picture of someone's life when non-content data is gathered over a long period of time.[481] This demonstrates that information cannot be divided into two categories and similarly cannot be an all or nothing proposition.

The mosaic theory refers to a method of intelligence gathering that involves first collecting disparate types of information, then combining those different individual pieces of knowledge to illuminate new ideas through their relationships.[482] This results in a "mosaic of information [that] is worth more than the sum of its parts."[483] Courts have yet to consider whether the mosaic theory is applicable to electronic records, but the Supreme Court has suggested that the theory significantly affects personal privacy because computer compilations

---

[478] Smith v. Maryland, 442 U.S. 735, 749 (1979).
[479] Katz v. United States, 389 U.S. 347, 360 (1967).
[480] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[481] *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013); *In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 449-50 (S.D.N.Y. 2005); United States v. Graham, 846 F. Supp. 2d 384, 403 (D. Mar. 2012).
[482] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 YALE L.J. 628, 630 (2005).
[483] *Id.*

provide unique dangers.[484] In *Jones*, the court recognized the intimate nature of some non-content data and its effect on society.[485] There are different types or privacy that all require Fourth Amendment protections. These protections cannot be protected if privacy is an all or nothing proposition. In *Jones*, Justice Sotomayor's concurrence explains, "GPS monitoring . . . [allows the government to obtain] such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track [and] may alter the relationship between citizen and government in a way that is inimical to democratic society." [486] The mosaic theory suggests that even non-content could provide content-like information, demonstrating that there are different levels and types of privacy which all require protection under the Fourth Amendment. Therefore, the all or nothing proposition cannot comport with the Fourth Amendment.

The third party doctrine allows the government to circumvent longstanding privacy protections of the Fourth Amendment

Secondly, the third party doctrine allows the government to take more invasive measures that should be protected under the Fourth Amendment.[487] An example of one of these invasive measures can be found in *Gouled v. United States.*[488] The Court upheld a ruling that allowed a business acquaintance to pretend to socially visit a criminal suspect, but actually intended to search the suspect's office for evidence.[489] Another example is found in *Sorrells v. United States*, where an undercover prohibition agent posed as a tourist in order to access a suspect's home to

[484] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763-64(1989).
[485] United States v. Jones, 132 S. Ct. 945, 957 (2012).
[486] *Id.* at 957.
[487] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009),
[488] Gouled v. United States, 255 U.S. 298 (1921).
[489] *Id.*

search for alcohol.[490] While these cases were not decided in accordance with the third party doctrine, they show that the court has held that it is constitutional for the government to deceivingly invade an individual's privacy for a criminal investigation.

The third party doctrine provides another way for the government to take invasive measures. In *Kyllo*, the court examined levels of government intrusiveness. This case involved the government's use of sense-enhancing technology, thermal imaging, to gather information about activities inside a home.[491] Agents used thermal imaging devices, which allowed them to scan the home in order to determine the amount of heat emitted from objects inside the house.[492] Scans showed that the defendant's garage roof and side wall were hotter than the rest of his house and his surrounding neighbors' houses.[493] Furthermore, using information gathered by this technique allowed the government to determine that the amount of heat being emitted was consistent with the amount normally emitted by high-intensity lamps, concluding that marijuana was likely being grown and therefore proceeded to search the house.[494]

The district court found that the thermal imaging machine was non-intrusive because it did not emit beams, penetrate any walls or windows, provide any information about activity inside the house, or reveal any intimate conversations.[495] Furthermore, the appellate court on appeal affirmed the conviction because he had no reasonable expectation of privacy. The Supreme Court found that "intimate details of Kyllo's home" are normally protected under the Fourth Amendment.[496] While the government could not collect the thermal imaging information, the court ruled that the third party doctrine allowed the government to use utility bills instead as

[490] Sorrells v. United States, 287 U.S. 435 (1932).
[491] Kyllo v. United States, 533 U.S. 27, 27 (2001).
[492] *Id.* at 27.
[493] *Id.* at 27.
[494] *Id.* at 27.
[495] *Id.* at 37.
[496] Kyllo v. United States, 533 U.S. 27, 37 (2001).

a reason to search the home.[497] This intrusion allowed the government to make inferences about what the defendant was doing in the privacy of his home. The increased invasiveness that the third party doctrine allows gives the government a lot of power that they could abuse.

Providing information to necessary third party services is not voluntary

Finally, critics have argued that individuals require the services provided by third parties; therefore, releasing their private information to these third parties is not voluntary.[498] In *Jones*, Justice Sotomayor argued that the third party doctrine is ill suited for this day and age because people need to reveal a lot of information to third parties.[499] In *Miller*, a case that highlights Justice Sotomayor's concern, the court held that financial statements and deposit slips were voluntarily conveyed.[500] Since most people use banks to store their money, it has become a service that is required for a reasonable person living in society.[501] Therefore, providing information to the bank is no longer a voluntary action, but rather a required one.

Additionally in *Smith*, the court held that the defendant "voluntarily conveyed numerical information to the telephone company."[502] Cell phones have grown to become an essential part of an individual's life, and therefore are a necessity based on the practical norms of society.[503] As such, a defendant or person is forced to share information with their cell phone company. Even if a defendant did not want to reveal information to their phone company, the necessity of having a cell phone forces a defendant to share that information.[504] Moreover, since people need

[497] Kyllo v. United States, 533 U.S. 27, 44-46 (2001).
[498] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.
[499] United States v. Jones, 132 S. Ct. 945, 948 (2012) (J. Sotomayor, concurring).
[500] *Id.* at 47.
[501] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, CONGRESSIONAL RESEARCH SERVICE REPORT (June 5, 2014), http://www.fas.org/sgp/crs/misc/R43586.pdf.
[502] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[503] *Id.* at 744.
[504] *Id.* at 744.

telephone service, they may not be aware of the privacy concerns surrounding that service. Tor addresses these privacy concerns by providing a way for its users to use the Internet without revealing any information about their Internet activity to their Internet service providers.[505]

ARGUMENTS FOR WHETHER TOR IS A THIRD PARTY

Tor is not a third party because it is an instrument used to instruct the transfer of information and does not possess information about user activity

Tor is most likely not a third party because the Tor Browser is only a medium through which communication occurs. Unlike other third parties who are able to provide information to the government, such as banks who keep records of their customers' transactions, Tor is unable to provide information about a user's activity online because it uses an unpredictable algorithm that merely instructs the transfer of information.[506] Relay operators, who are volunteers rather than employees of Tor, make their personal servers available to Tor users. These servers owned and operated by independent Internet service providers, not the Tor Browser, are responsible for the actual transfer of information. Internet service providers transfer information between one another, and record information about those transfers. Specific Internet service providers, which provide service for relay operators, are considered third parties because (1) they provide the technology that allows for the transfer of information, and (2) they have the ability to provide information about which IP addresses are passing through their servers.

The roles of Tor and the relay operator's Internet service provider can be analogized to the roles of a cell phone and a wireless service provider, respectively. Like Internet service providers, the wireless service provider transfers calls by allowing the signal to bounce through cell towers that they own. Like Tor, a cell phone is used merely as an instrument that allows the

[505] Tor Project, https://www.torproject.org/index.html.en (last visited February 27, 2015).
[506] Interview with Andrew Lewman, Executive Director and Secretary and Treasurer of the Board, Tor Project, in Boston, MA (September 26, 2014)

wireless service provider to transfer the call. Tor is not a third party, but rather an instrument through which the relay operators' Internet service providers transfer information and they are unable to provide information about user activity. Sections 2 and 5 expand on whether Tor qualify as a service provider.

Tor is not considered a third party because they provide a reasonable expectation of privacy

Tor differs from other entities considered third parties under the doctrine because it is a technological medium in which people have a reasonable expectation of privacy. Unlike other entities that may be considered third parties, such as Internet service providers, Tor specifically states that it "defend[s] against traffic analysis, a form of network surveillance that threatens personal freedom and privacy."[507] As stated previously, in *Katz,* Harlan explained that for there to be a reasonable expectation of privacy: (1) a person has to have an actual (subjective) expectation of privacy; and (2) said expectation is one that society is prepared to recognize as reasonable.[508] Tor allows a person to have an actual expectation of privacy because Tor's technology makes it extremely difficult for anyone to trace a user's activity online.[509] Society should be prepared to recognize this expectation as reasonable because the Internet is becoming a more widely used piece of technology that people have come to rely on to transfer important information. When users use Tor, they have a reasonable expectation of privacy. As such, information transmitted via Tor should not be subject to the third party doctrine.

Additionally, Tor may be further distinguished from other service providers that may be considered third parties because an intercepted IP address using Tor cannot reasonably be traced

[507] Tor Project, https://www.torproject.org/index.html.en (last visited February 27, 2015).
[508] Katz v. United States, 389 U.S. 347, 361 (1967).
[509] Interview with Andrew Lewman, Executive Director and Secretary and Treasurer of the Board, Tor Project, in Boston, MA (September 26, 2014). Tor promotes itself as an anonymity tool on the Internet. While anonymity and privacy are not synonymous, the subjective expectation of privacy can be construed because people associate anonymity with privacy.

back to its originating location.[510] Tor allows an IP address to be bounced through two nodes before passing through an exit node.[511] Each node operator is able to figure out the IP address of both the node operator directly before and directly after their particular node, but not any other IP addresses.[512] This only lasts for ten minutes, making it extremely difficult for the government to trace the IP address of the original user's device.[513] Even if every relay operator installed technology to record every incoming IP address, it would be very challenging to establish a clear connection because the nodes are located in different countries, with different laws, and Tor's algorithm ensures a different path each time a user tries to access a website.[514] This provides a user with a level of anonymity on the Internet because their information cannot easily be traced back to the Tor user. However, anonymity is not synonymous with privacy. A person can remain anonymous even if a piece of private information is disclosed publicly. If the information does not contain any personally identifiable information, it cannot be traced back to the individual. At the same time, the information exists in the public sphere. Thus, in that sense, the information is no longer private. If Tor is not considered a third party, users have a reasonable expectation of privacy and can remain anonymous. Therefore, this encourages free speech. For example, activists using Tor do not need to worry about the repercussions of voicing their opinions. As stated above, the same anonymity that provides free speech benefits can be utilized by individuals for nefarious purposes.

[510] Interview with Andrew Lewman, Executive Director and Secretary and Treasurer of the Board, Tor Project, in Boston, MA (September 26, 2014).
[511] *Id.*
[512] *Id.*
[513] *Id.*
[514] *Id.*

PROPOSED LEGISLATION AND THE FUTURE OF THE THIRD PARTY DOCTRINE

There is proposed legislation to,

> permit the government to obtain, and a court to admit, information relating to an individual held by a third party in a system of records only if: (1) the individual whose name or identification information the government is using to access the information provides express and informed consent to the search; or (2) the government obtains a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.[515]

If passed, the third party doctrine will essentially be repealed. The Communication Assistance of Law Enforcement Act (CALEA) is an extension of the third party doctrine with a narrower scope, focusing only on telecommunications carriers.[516] Can Tor still be subject to the third party doctrine via the CALEA? The next section will address this issue.

[515] Fourth Amendment Preservation and Protection Act of 2013, S. 1037, 113th Cong. (2013) *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1037.
[516] 47 U.S.C.A. §1001-1010 (West 2014).

Section 5

The Communications Assistance for Law Enforcement Act

Question Presented: Does Tor fall within the scope of the CALEA?

BRIEF ANSWER

The Communications Assistance for Law Enforcement Act (CALEA) extends to entities that are classified as telecommunications carriers. This section posits that Tor cannot be classified as a telecommunications carrier. However, the scope of the CALEA is constantly in flux because it expands to cover new telecommunications technologies as they emerge, which leaves open the possibility that Tor may fall within its scope in the future. This section will first examine the history and intent of the CALEA. It will then explore the requirements of CALEA compliance and the type of information that can be accessed through the CALEA. Next, this section will analyze the CALEA's definition of telecommunications carrier and its possible application to Tor. Finally, it will discuss the direction of the CALEA's scope and offer suggestions for how the scope should be managed going forward.

INTRODUCTION

The CALEA is an extension of the third party doctrine. The third party doctrine, which is analyzed in Section 4, is based in common law,[517] whereas the CALEA is a codified version of the third party doctrine aimed at a very specific third party group: telecommunications carriers.[518] Individuals voluntarily release their information to third party telecommunications carriers, such as their cable company or Internet service provider (ISP).[519] With the proper legal

[517] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[518] 47 U.S.C.A. §1001-1010 (West 2014).
[519] Katz v. United States, 389 U.S. 347, 351 (1967).

authority, law enforcement agencies may intercept the information that subscribers voluntarily release to telecommunications carriers.[520] The CALEA requires that telecommunications carriers design their equipment with certain interception capabilities in order for law enforcement to more easily capture wire and electronic communications.[521]

Congress enacted the CALEA as a response to the surveillance issues faced by law enforcement as a result of technology's rapid evolution.[522] The CALEA intended to ensure the protection of privacy in communications while still enabling law enforcement to intercept communications pursuant to lawful authorization.[523] The Federal Communications Commission (FCC) has the authority to oversee the implementation of the CALEA and is charged with the responsibility of balancing the competing interests of three groups: privacy advocates, law enforcement agencies, and the telecommunications industry.[524] The FCC has tended to give preference to law enforcement interests over those of privacy advocates and the telecommunications industry.[525] The FCC's trend of favoring law enforcement interests could pose a problem for Tor and its users, as FCC has the authority to expand the CALEA through its regulatory process.[526] While it seems clear that Tor does not currently fall within the CALEA scope, the CALEA could be expanded in the future to encompass Tor and similar technologies.

WHAT IS THE CALEA?

Congress adopted the CALEA in 1994 as a response to changing telecommunications technology, and to clarify the duties of the telecommunications industry in aiding law

[520] Katz v. United States, 389 U.S. 347, 351 (1967).
[521] 47 U.S.C.A. §§ 1001-1010 (West 2014).
[522] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 4 (2007).
[523] H.R. Rep. No. 103-827, pt. 1 at 12 (1994), http://askcalea.fbi.gov/docs/hr103827.pdf.
[524] *Id.* at 14-15.
[525] Gene D. Park, *Internet Wiretaps: Applying the Communications Assistance for Law Enforcement Act to Broadband Services*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 599 (2006).
[526] 47 U.S.C.A. §§ 1001-1010 (West 2014).

enforcement with the lawful interception of communications.[527] Congress did not design the CALEA to expand the government's surveillance capabilities, but rather to preserve the government's ability to perform lawful interception of communications as technology advanced.[528] The CALEA originally targeted traditional telephone services but its scope encompassed all telecommunications services, such as those providing wireline, wireless, cable, satellite, and electric or other utilities.[529]

The CALEA expanded in 2005 to include Voice Internet Protocol (VoIP) and facilities-based broadband Internet access providers, which includes ISPs.[530] In 2004, the Federal Bureau of Investigation (FBI) and the United States Department of Justice (DOJ) jointly petitioned the FCC to expand the CALEA to include VoIP and Internet communications and to clarify the scope of the CALEA.[531] The FCC then issued its First Report and Order approving the expansion. The FCC reasoned that "covering all broadband Internet access service providers prevents migration of criminal activity onto less regulated platforms."[532] The Order also found that VoIP fell under the substantial replacement provision of the CALEA.[533] Privacy advocacy groups and members of the telecommunications industry were dissatisfied with this expansion and consequently filed a petition for a review of the First Report and Order in the United States

[527] 47 U.S.C. §§ 1001-1010 (West 2014).
[528] CENTER FOR DEMOCRACY AND TECHNOLOGY, *Insights - CALEA Background*, cdt.org, https://cdt.org/insight/calea-background/ (Sept. 28, 2010).
[529] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 4 (2007).
[530] Am. Council on Educ. v. F.C.C., 451 F.3d 226 (D.C. Cir. 2006).
[531] Joint Petition for Expedited Rulemaking, RM-10865 (filed Mar. 10, 2004) (DOJ Petition), *Comment Sought on Calea*, 19 F.C.C. RCD. 4691, 4691 (2004), http://askcalea.fbi.gov/pet/docs/20040310.calea.jper.pdf.
[532] FCC 99-229, Second Report and Order, CC Docket No. 97-213, released August 31, 1999.
[533] Joint Petition for Expedited Rulemaking, RM-10865 (filed Mar. 10, 2004) (DOJ Petition).

Court of Appeals for the District of Columbia Circuit.[534] The court ruled in favor of the FCC and upheld the expansion, finding the expansion to be a reasonable policy choice.[535]

WHAT DOES IT MEAN TO BE CALEA COMPLIANT?

To be CALEA compliant, a telecommunications carrier that provides a customer or subscriber with the ability to originate, terminate, or direct communications, must design or modify their facilities, equipment, or services so that they are capable of expeditiously tapping phone conversations and recording call-identifying information.[536] CALEA compliance requires that telecommunications carriers enable the government to access the information before, during, or immediately after the wire or electronic information is transmitted.[537] This means that the ability to intercept the communication must be available at any point during the transmission. The CALEA requires a "minimum of interference" with a subscriber's service, meaning that telecommunications carriers must be unobtrusive while intercepting the communication so that the subscriber is not aware of the interception.[538]

The CALEA states that the Attorney General shall coordinate with law enforcement agencies and consult with the appropriate organizations of the telecommunications industry to create standards for compliance.[539] The Attorney General is also authorized to pay telecommunications carriers for some costs associated with compliance.[540] The Attorney General delegated the compliance implementation authority to the FBI.[541] The FBI and the

[534] Am. Council on Educ. v. F.C.C., 451 F.3d 226 (D.C. Cir. 2006).
[535] *Id*.
[536] 47 U.S.C.A. § 1002 (West 2014).
[537] *Id.*
[538] *Id.*
[539] 47 U.S.C.A. § 1006 (West 2014).
[540] 47 U.S.C.A. § 1008 (West 2014).
[541] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 4 (2007).

telecommunications industry have clashed over compliance standards.[542] One of the first disagreements between the FBI and the telecommunications industry concerned how long it would take to achieve compliance.[543] The FBI believed that compliance could be reached in one year, while the industry argued for three years.[544] Without a uniform standard, compliance took longer than the FBI expected, prompting it to invoke its power to impose regulations that would enable government to recover compliance costs from non-compliant telecommunications carriers.[545] In 1997, The Telecommunications Industry Association (TIA)[546] adopted a technical standard for compliance, referred to as the J-Standard.[547]

The FBI wanted telecommunications carriers to have more interception capabilities than what the J-Standard provided, and in 1998 petitioned the FCC to require telecommunications carriers to incorporate the following list of capabilities into the standard:

1. Content of subject-initiated conference calls -- Capability would enable law enforcement to access the content of conference calls supported by the subject's service (including the call content of parties on hold).
2. Party hold, join, drop -- Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference call.
3. Subject-initiated dialing and signaling information -- Capability would provide a LEA access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features (such as the use of flash-hook and other feature keys).

---

[542] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 4 (2007).
[543] *Id.*
[544] *Id.*
[545] *Id.*
[546] "TIA is a national, full-service trade association of over 900 small and large companies that provide communications and information technology products, materials, systems, distribution services and professional services in the United States and around the world. TIA is accredited by the American National Standards Institute ("ANSI") to issue standards for the industry." Notice of Proposed Rulemaking, *In the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, FCC Docket No. 97-356 (released Oct. 10, 1997)("NPRM"), *See also* TIA, *Comments of the Telecommunications Industry Association*, FEDERAL COMMUNICATIONS COMMISSION, (May 8, 1998), http://www.tiaonline.org/sites/default/files/pages/Comments5898.pdf.
[547] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 4 (2007).

4. In-band and out-of-band signaling (notification message) -- A message would be sent to a LEA whenever a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy).
5. Timing information -- Information necessary to correlate call-identifying information with the call content of a communications interception would be sent to a LEA.
6. Surveillance status -- A message that would verify that an interception is still functioning on the appropriate subject would be sent to a LEA.
7. Continuity check tone (c-tone) -- An electronic signal would alert a LEA if the facility used for delivery of call content interception has failed or lost continuity.
8. Feature status -- A message would affirmatively notify a LEA of any changes in features to which a subject subscribes.
9. Dialed digit extraction -- Information sent to a LEA would include those digits dialed by a subject after the initial call setup is completed.[548]

Conversely, privacy rights advocates and TIA members argue that the original J-Standard provided law enforcement with more information than what the CALEA requires.[549] The inability of the telecommunications industry and the FBI to agree on compliance standards forced the FCC to get involved.[550] The FCC determined that of the nine capabilities that the FBI requested, the following six should have been incorporated into the J-Standard: (1) content of subject-initiated conference calls; (2) party hold, join, (3) drop on conference calls; (4) subject-initiated dialing and signaling information; (5) in-band and out-of-band signaling; (6) timing information; and dialed digit extraction.[551]

WHO MUST BE CALEA COMPLIANT?

The scope of the CALEA extends to any person or entity that is considered a telecommunications carrier.[552] The CALEA defines telecommunications carrier as "a person or

[548] Joint Petition for Expedited Rulemaking, RM-10865 (filed Mar. 10, 2004) (DOJ Petition).
[549] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 6 (2007).
[550] *Id.* at 7.
[551] FCC 99-230, Third Report and Order, CC Docket No. 97-213, released August 31, 1999.
[552] 47 U.S.C.A. § 1001 (West 2014).

entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[553] The definition includes,

> A person or entity engaged in providing commercial mobile services or a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter.[554]

The CALEA attempted to create a broad definition of telecommunications carrier in anticipation of the changes in the way people communicate. The CALEA aims to equip law enforcement with the capability of conducting authorized surveillance regardless of the telecommunications system being deployed.[555] It is meant to apply to any person or entity that acts as a telecommunications carrier. The application of the CALEA may change over time because the scope of the definition allows entities that are not currently considered telecommunications carriers may be considered telecommunications carriers in the future.

According to the FCC, the definition of "telecommunications carrier" includes such service providers as "local exchange carriers, interexchange carriers, competitive access providers, cellular carriers, providers of personal communications services, satellite-based service providers, cable operators, and electric and other utilities that provide telecommunications services for hire to the public, and any other wireline or wireless service for hire to the public."[556] Verizon, Sprint, T-Mobile, Comcast, and Vonage are examples of telecommunications carriers.

---

[553] 47 U.S.C.A. § 1001 (West 2014).
[554] *Id.*
[555] Patricia Moloney Figliola, *Digital Surveillance: Communications Assistance for Law Enforcement Act*, RL30677, at 3 (2007).
[556] FCC 99-11, Report and Order CC Docket No. 97-213, released March 15, 1999.

WHAT INFORMATION CAN BE ACCESSED THROUGH THE CALEA?

Telecommunications carriers must only release information to law enforcement in accordance with some lawful authorization such as a court order.[557] The telecommunications carrier must always have the ability to intercept the information. However, under the CALEA the subscriber's information may only be released to law enforcement pursuant to a warrant or other legal authority. The CALEA provides that telecommunications carriers are only permitted to deliver call-identifying information to law enforcement as opposed to content information.[558] The statute defines call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[559] The statute also states that, "such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[560] A 2000 court decision negated this portion of the CALEA.[561] The court denied petitions for review regarding antenna tower location information and packet-mode data, classifying them as required capabilities.[562] Both antenna tower location information and packet-mode data can potentially reveal information that law enforcement can use to trace the location of a subscriber's device, and potentially link it to the subscriber.[563]

[557] 47 U.S.C.A. § 1004 (West 2014).
[558] 47 U.S.C.A. § 1001(West 2014).
[559] *Id.*
[560] 47 U.S.C.A. § 1002 (West 2014).
[561] U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450 (D.C. Cir. 2000).
[562] *Id.*
[563] *Id.*

In 1994, when Congress enacted the CALEA the term "call-identifying information" referred to telephone numbers.[564] Advances in Internet technology have reshaped the understanding of the term. The technology used to transmit Internet signals, compared to traditional phone signals, makes it very difficult to distinguish signaling information from content, like the conversation between two parties conducted over a telephone line. Transmission over the Internet occurs via packets.[565] The packets are broken up and sent over multiple layers.[566] Whether a component is "signaling information" or "content" depends on which layer is being read.[567] Sometimes a packet must be analyzed in its entirety in order to determine if it contains signaling or content information. This poses a threat to privacy. If the government analyzes an entire packet, it may have access to content information that is beyond the scope of the CALEA. If subjected to the CALEA, Tor would not be able to distinguish between content and signaling information or know with certainty whose information it was providing to law enforcement and therefore could not reasonably comply with the CALEA.

IS TOR A TELECOMMUNICATIONS CARRIER?

Tor is a free software and open network.[568] The term telecommunications carrier specifically refers to persons or entities for hire.[569] Tor does not own any of the infrastructure that users access, such as the wires or cables used to provide the connection and cannot be sure whose information they would be providing to law enforcement. Therefore, Tor should fall outside the CALEA scope. Even if Tor were a person or entity for hire, it is not engaged in the

[564] 47 U.S.C.A. § 1001 (West 2014).
[565] Susan Landau, *Institute of Electric and Electronics Engineers Computer Society*, CALEA AND NETWORK SECURITY (2005), http://privacyink.org/pdf/SWatI.pdf.
[566] *Id.*
[567] *Id*.
[568] TOR PROJECT, https://www.torproject.org/ (last visited Feb 23, 2015).
[569] 47 U.S.C.A. § 1001 (West 2014).

transmission or switching of wire or electronic communications.[570] Tor is an application that sends a protocol over a private network.[571] Tor does not power the network over which communication is sent.[572] Internet service providers power the networks over which Tor users' send information.

The second part of the CALEA's telecommunications carrier definition allows the FCC to deem some commercial mobile service providers as telecommunications carriers if the FCC finds they are engaged in "providing wire or electronic communication switching or transmission service to the extent that the FCC finds is a replacement for a substantial portion of the local telephone exchange service."[573] As Tor is not engaged in providing wire or electronic communication switching or transmission services at all[574], the FCC could not reach Tor through this exception.

Tor does not fit into the current definition of telecommunications carrier and is therefore not required to be CALEA compliant. However, when technology has gotten ahead of government eavesdropping capabilities in the past, the FCC expanded the CALEA to cover the new technology. The scope of the CALEA seems to be constantly changing and a review of proposed changes is necessary to understand the direction that the FCC and the FBI will take concerning CALEA's scope.

WHERE IS THE CALEA SCOPE HEADED?

[570] Interview with Frank Speiser, President and Co-Founder, SocialFlow, Inc. (Feb. 2, 2015).
[571] *Id.*
[572] *Id.*
[573] 47 U.S.C.A. § 1001 (West 2014).
[574] Imagine a switch board operator connecting callers on a switchboard. Tor does not function as the switchboard operator, instead it functions as the instruction from the person making the call to the switchboard operator as to which wires should be connected to complete the communication.

In October 2014, FBI Director James Comey gave a speech discussing the technological challenges to lawful interception.[575] He stated that the law has not kept up with technology, which the FBI believes poses public safety problems.[576] In describing the public safety concerns, Comey stated,

> We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[577]

Comey compared the process of lawful interception before the advent of modern Internet communications with that of today.[578] Law enforcement would identify a target phone being used by an individual that had a single carrier, obtain a court order for a wiretap, and collect the call-identifying information.[579] Comey explained that today, criminals, like most of the public, use multiple devices on several networks and switch among various applications and law enforcement "may not have the capability to quickly switch lawful surveillance between devices, methods, and networks."[580] Comey also stated that the CALEA was adopted twenty years ago and does not cover new means of communication.[581] For these reasons, Comey believes that the CALEA needs to expand to require a wider array of communications services to have built-in interception capabilities or law enforcement will be left in the dark and have no method of lawfully intercepting communications.[582]

---

[575] James Comey, Director, FBI, Address at the Brookings Institute (Oct. 16, 2004), http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[576] *Id.*
[577] *Id.*
[578] *Id.*
[579] James Comey, Director, FBI, Address at the Brookings Institute (Oct. 16, 2004), http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[580] *Id.*
[581] *Id.*
[582] *Id.*

Comey referenced Apple and Google's plans to use default encryption settings for their smart phones, the iPhone and the Android.[583] With the default encryption settings, Apple and Google, which are telecommunications carriers, would not be capable of unlocking phones, thus restricting access to a subscriber's information stored within the phone, such as photos, emails, or other documents.[584] Comey believes that this type of encryption puts law enforcement at a dead end. He supports requiring telecommunications carriers with these settings to build capabilities that would allow law enforcement to access the information despite the encryption service into their service.[585] This would defeat the purpose of the service which is to provide privacy and security.

The Tor Browser poses similar challenges to law enforcement. Tor, like the telecommunications carriers that provide these default encryption services, offers a service that shields a user's information from interception by the third party over whose infrastructure their information is being sent. If the CALEA were extended to include this type of technology, it would be impossible to comply with the CALEA and still offer privacy and security to users. Ultimately, Comey is arguing that the need for law enforcement to access communications for the purpose of catching criminals and preventing terrorist attacks outweighs the rights of telecommunications carriers to offer certain types of privacy services and the rights of individuals to protect their privacy. The future of the CALEA scope rests on the ability of the FCC, and ultimately the courts, to recognize that the rapid and expansive transformation in communication calls for a different approach to lawful interception and privacy protection.

---

[583] James Comey, Director, FBI, Address at the Brookings Institute (Oct. 16, 2004), http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[584] *Id.*
[585] *Id.*

CONCLUSION

Tor is beyond the scope of the current understanding of the CALEA because the CALEA specifically applies to telecommunications carriers and Tor is not a telecommunications carrier. Unless the definition of telecommunications carrier is drastically expanded or Tor begins to offer new telecommunications-like services, it is unlikely that Tor will be considered a telecommunications carrier. However, given that the FCC has historically deferred to law enforcement, the scope of the CALEA may be drastically expanded in the future.

The scope of the CALEA is purposefully broad in order to allow it to expand and apply to new and different telecommunications services as they develop. However, the expansions have largely been directed at the range of telecommunications services that the CALEA covers. The CALEA's provisions that protect a subscriber's information should be expanded to reflect the changes in the telecommunications industry. The services we use to communicate today are vastly different than they were in 1994 when Congress enacted the CALEA. Current methods of communication not only make traditional surveillance methods more difficult, but they also make the isolation of information that law enforcement can legally access a challenge. This poses a threat to privacy. New methods and forms of communication technology require new forms of protection. Tor is a method of privacy protection. Some methods of privacy protection clash with the government's ability to conduct surveillance. Expanding the CALEA's scope to cover these methods of protection should be done with caution so as to ensure that privacy rights are not sacrificed as law enforcement attempts to keep up with technology.

Section 6

Academic Research Under the Wiretap Act

Question Presented: Academic researchers at the University of Colorado recently recorded network communications traffic exiting from a Tor relay they were operating. Is it a violation of the Wiretap Act? Is it a violation of the researchers' contract to abide by the protocols regarding ethics of using human subjects in research?

BRIEF ANSWER

The Colorado researchers did not violate the Wiretap Act. The Wiretap Act only governs the interception of content data and the researchers recorded non-content data from the Tor relay they were operating. However, other researchers may not take the same precautions and thus may fall within the Act's reach. Researchers will probably not be able to invoke any of the Wiretap Act's enumerated exemptions in order to record Tor user data as Tor use does not imply consent to have their data recorded. Additionally, Tor node operators are not parties to a Tor user's communication and Tor is likely not a provider under the Act. Furthermore, a violation of federal regulations governing research on human subjects by recording Tor user data depends on what Tor user data they record.

INTRODUCTION

In 2008, researchers from the University of Colorado and University of Washington presented the results of their most recent project in a paper, entitled *Shining Light in Dark Places: Understanding the Tor Network,* at the Privacy Enhancing Technologies Symposium (PETS).[586] For their project, the researchers volunteered to use their servers at the University of

[586] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker, *Shining Light in Dark Places: Understanding the Tor Network* (2008).

Colorado as both Tor entry and exit nodes.[587] They hoped to discover demographic information about Tor users, analyze what type of Internet activities people engaged in over Tor, and develop a method for spotlighting misuses of Tor.[588] In order to acquire this information, the researchers recorded only the first 150 bytes of each data packet exiting their server.[589] This methodology raises major privacy concerns for Tor users. Tor's architecture is expressly designed to anonymize users' identities and Internet traffic. The methodology employed by these researchers creates several questions regarding its legality and raises ethical concerns as to whether their research violates federal protocols for research conducted on human subjects. Specifically, this section addresses its legality under the Wiretap Act and concludes that, while the Colorado researchers most likely did not violate the Wiretap Act, as the statute does not contemplate the type of information they intercepted, other researchers conducting similar experiments may violate the Act. It is less clear whether the researchers violated ethical protocols for research on human subjects.

THE WIRETAP ACT

Content and Non-Content Data

As explained in Section 1, the federal Wiretap Act prohibits the interception of communications in transit. Specifically, the Act states that "a person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication . . . shall be punished . . . "[590] The statute defines "intercept" as the "aural or other acquisition of the *contents* of any wire, electronic, or

[587] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker, *Shining Light in Dark Places: Understanding the Tor Network* (2008).
[588] *Id.*
[589] *Id.*
[590] 18 U.S.C.A § 2511(1)(a) (West 2008).

oral communication through the use of any electronic, mechanical, or other device."[591] The statute also defines "contents" as "any information concerning the substance, purport, or meaning of that communication."[592] As described in Section 1, determining whether something qualifies as content or non-content data requires nuanced analysis. Clearly, the body of an email contains "the substance, purport, or meaning" of a communication as the textual body of an email is the very thing the user intends to transmit. However, courts have not identified URLs as "content" under the Wiretap Act.[593] Similarly, IP addresses are not considered "content."[594] This data is automatically generated regardless of the user's intent.[595] As such, it does not constitute the "substance, purport, or meaning" of a communication.[596]

The researchers claim in their paper that they ran a program enabling them to capture only the first 150 bytes of each data packet going through their server.[597] This limitation allowed them to capture only application-level headers.[598] If true, it is unlikely that they violated the Wiretap Act. As stated previously, courts have consistently found that URLs and IP addresses, information contained within application-level protocol headers, do not qualify as "content"

---

[591] 18 U.S.C.A. § 2510(4) (West 2008) (emphasis added).
[592] 18 U.S.C.A. § 2510(8) (West 2008).
[593] *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F. Supp. 2d 434, 444 (D. Del. 2013). The court stated that no court has considered URLS as "content" under the Wiretap Act. According to the court, URLs are immutable transactional records that allow one to locate a document but do not include "the substance, purport, or meaning of an electronic communication" as required by the Wiretap Act. *Id.*
[594] *See In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F. Supp. 2d 434, 444 (D. Del. 2013); *In re* § 2703(d), 787 F. Supp. 2d 430, 436 (E.D. Va. 2011).
[595] *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012).
[596] The court relied on a Ninth Circuit ruling that found data automatically generated by a telephone call, like the time and duration of the call, did not constitute content under the Wiretap Act because it did not contain any information concerning the substance, purport or meaning of the communication. *Id.*
[597] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker, *Shining Light in Dark Places: Understanding the Tor Network* (2008).
[598] These "headers" refer to the first bytes of information in a data packet. The information contained in a packet's header allows servers to identify the type of data contained in the rest of the packet. It also determines where the server will send the data next. For a more detailed analysis of data packets, see *supra* note 12. Robert Ditzion, Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers, 41 AM. CRIM. L. REV. 1321, 1330 (2004).

under the statute.[599] This data is generated automatically and not through the intent of the Internet user.[600] Thus, it is not considered "content" for Wiretap Act purposes.[601] However, it isn't entirely clear what data the researchers actually collected. Their methodology indicates a purposeful attempt to avoid capturing content data and thus avoid liability under the Wiretap Act. If they successfully limited the captured data to the data outlined in their paper, it is unlikely that they violated the Act.

The Wiretap Act also makes illegal the *disclosure* of intercepted content data.[602] The researchers have not publicly disclosed the data they captured. Their refusal to publicize this data may reflect concern for the anonymity of Tor users, but also perhaps a fear of potential legal liability. If the researchers publicly disclose their data in the future and the disclosure reveals that the data in fact goes beyond application-level headers into content data, the researchers may fall within the reach of the Wiretap Act for both intercepting the contents of communication and for disclosing the intercepted content data. Additionally, an accidental or unsanctioned disclosure of the data could have negative legal implications for the researchers. If an independent party somehow obtained and disclosed the researchers' data, and the data contained content data, the independent party would be protected under the First Amendment so long as the speech involved "a matter of public concern."[603] However, establishing that an independent party unlawfully disclosed Tor user data recorded by academic researchers necessarily requires that the academic

[599] *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F. Supp. 2d 434, 444 (D. Del. 2013).
[600] *See*, *In re* Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014). *See also In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012).
[601] *Id.*
[602] The Act states that "any person who … *intentionally discloses, or endeavors to disclose*, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication." 18 U.S.C.A. § 2511(1)(c) (West 2008) (emphasis added).
[603] Bartnicki v. Vopper, 532 U.S. 514, 535 (2001). Whether participation in the Tor network for the purpose of academic research constitutes "a matter of public concern" is a question for a different project.

researchers unlawfully captured Tor user data under the Wiretap Act.[604] While the exact consequences of such a determination are unclear, any legal determination characterizing the researchers' conduct as unlawful will be detrimental to their interests to some degree.

Furthermore, one can imagine how less scrupulous researchers, or researchers seeking to analyze more than just demographic information, could eschew the data-limiting measures taken by the Colorado researchers. For example, if researchers captured the entire data packet and not just the first 150 bytes, perhaps to examine the body of an email sent by a Tor user, it would probably fall within the statute's definition of "content" as it cannot be created without the intent of the user. Capturing an entire packet increases the likelihood of capturing data a Tor user intended to communicate.

Consent Exemptions: Implied Consent

If one accepts *arguendo* that the researchers did in fact capture "content" data, it would not necessarily be dispositive of a statutory violation. The Wiretap Act contains a number of exemptions.[605] Notably, the consent exemption states that intercepting a communication "shall not be unlawful where such person is a party to the communication or where one of the parties to the communication has given prior consent . . . "[606] In order for the consent exemption to apply, the interceptor does not need to give express consent nor be an active participant in the conversation.[607] Rather, the interceptor's presence must merely be "apparent" to those individuals whose conversation is being intercepted. For example, if two people have a

[604] *See e.g.* Bartnicki v. Vopper, 532 U.S. 514 (2001). The court accepted for procedural purposes that an interception of content data constituted a violation of the act in order to determine whether an independent party violated the Wiretap Act by disclosing recorded content data. *Id.*
[605] 18 U.S.C.A. § 2511(2)(a-h) (West 2008).
[606] 18 U.S.C.A. § 2511(2)(d) (West 2008).
[607] Council on American-Islamic Relations Action Network, Inc. v. Gaubatz, 31 F.Supp.3d 237, 255 (D.C. Cir. 2014).

conversation, a third party standing nearby may not actively participate in the conversation, but their presence may still be apparent to the other two.[608] Courts have ruled that, based on the legislative history, the consent requirement is meant to be construed broadly.[609] However, courts have stressed that implied consent should not be "casually inferred" but instead it must be shown "convincingly" that the aggrieved party "knew about and consented to the monitoring despite the lack of formal notice."[610] Furthermore, it is not enough for the interceptor to merely demonstrate that an aggrieved party should have known their communications were being monitored.[611] In *United States v. Amen*, the court found that inmates implicitly consented to the recording of their phone calls over prison phones.[612] In making this determination, the court pointed to the Code of Federal Regulations which provides public notice that inmate telephone use is subject to limitations that the Warden deems necessary to ensure security. Moreover, a handbook given to all new inmates stated that prison phones are monitored and taped.[613]

It is highly unlikely that the academic researchers are covered by the Wiretap Act's implied consent exemption, as this would require demonstrating by a "convincing" degree that Tor users knew about and consented to the interception of their data by the academic researchers. The researchers may argue that Tor users should have known that their communications would hop through several distinct servers, as this mechanism is the very feature that allows Tor to anonymize its users. This anonymization process is the primary benefit of using Tor. The researchers may argue that a Tor user should reasonably expect that someone operating their own server as a relay is likely to access the information flowing through it at any given time.

---

[608] *See e.g.* Matter of John Doe Trader No. One, 894 F.2d 240, 244 (7th Cir. 1990). *See also* Grandbouche v. Adams, 529 F. Supp. 545, 548 (D. Colo. 1982).
[609] United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987).
[610] United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995).
[611] Jandak v. Village of Brookfield, 520 F.Supp. 815, 820 (N.D. Ill. 1981).
[612] United States v. Amen, 831 F.2d 373, 379 (2d Cir. 1987).
[613] *Id.*

However, even if the researchers argued these points successfully, they would likely fail under the rule described in *Jandak v. Village of Brookfield*. Merely showing that a Tor user should have known how Tor works and thus reasonably should have known their traffic would be monitored does not create implied consent.[614] Similarly, a showing that a Tor user knew that some node operators possessed, at the very least, the capability to monitor their Internet traffic would not be sufficient for implied consent.[615]

Consent Exemptions: Party to the Communication

Alternatively, the researchers could claim that they satisfied the consent exemption by demonstrating that, as server administrators, they operated the server through which Tor users sent their data and are thus entitled to capture the information. The consent exemption only requires that *one* party be a "party to the communication."[616] Instead of arguing that the Tor user gave implied consent, the researchers can claim that as a party to the communication, they gave unilateral consent to themselves to capture the data.[617] Again, in order for this argument to pass muster, the researchers run into a problem similar to the one created by implied consent.

Where implied consent requires demonstrating that the Tor user knew that they were being monitored, here the researchers would only need to demonstrate that the Tor user knew or should have known that their data would go through another server. One does not need to be "invited" into a communication in order to establish oneself as a party to a communication.[618] Alternatively, it is unclear what facts are sufficient to affirmatively establish oneself as a party.

---

[614] Jandak v. Village of Brookfield, 520 F.Supp. 815, 820 (N.D. Ill. 1981).
[615] Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).
[616] 18 U.S.C.A. § 2511(2)(d) (West 2008).
[617] 18 U.S.C.A. § 2511(2)(d) (West 2008). Federal law only requires that one party to the communication give consent as opposed to both parties. The Wiretap Act states, "Where such person is a party to the communication or where *one* of the parties to the communication has given prior consent . . . " *Id.* (emphasis added).
[618] Caro v. Weintraub, 618 F.3d 94, 97 (2d Cir. 2010).

In *Caro v. Weintraub*, the Second Circuit found that an uninvited party who recorded an oral conversation established himself as a party to the communication by "[speaking] up a few times and encouraging [the other party] to continue" even though the speaker did not communicate directly to the uninvited party.[619] *Caro* illustrates that a party can establish themselves as a party to the communication even when they are not invited to participate in the communication and are not the intended recipient of the communication. The uninvited party must do something to establish their presence, even if the application of the requirement is unclear as it pertains to Tor users and Tor researchers. Tor use may itself be enough to establish this requirement, as the very purpose of Tor is to anonymize users by sending their traffic through three separate nodes. While this fact fails to satisfy the Wiretap Act's implied consent exemption, it may be enough to establish the researchers' server as a party to a Tor user's communication. To that end, the front page of Tor's website, where one downloads the Tor Browser, provides sufficient information describing its three-hop structure.[620] This information may be enough to be considered "speaking up" under *Caro*.

Nevertheless, the circumstances in *Caro* are significantly different than the ones surrounding the researchers. An "unseen auditor" will not be able to exercise the exemption.[621] Unlike the party in *Caro*, the researchers never proactively announced their presence to the Tor users whose data they collected. Node operators are not cognizant of the contents of the Tor user's communication. In turn, this begs a question as to whether one can become a party to a communication if they do not inspect the contents of the communication when the sender of the communication knew or should have known the communication would be sent to the second party. Imagine a masked stranger hands someone else a letter for delivery to another masked

[619] Caro v. Weintraub, 618 F.3d 94, 97 (2d Cir. 2010).
[620] *Why Anonymity Matters,* TOR PROJECT, https://www.torproject.org (last visited March 8, 2015).
[621] Pitts Sales, Inc. v. King World Prods. Inc., 383 F. Supp. 2d 1354, 1361 (S.D. Fla. 2005).

stranger with explicit instructions not to open the letter. The "messenger" in this example, even though they posses the letter, never has access to the contents of the communication. Is the messenger thereby a party to the communication between the two masked strangers? The Ninth Circuit recently held in *In re Zynga Privacy Litig.,* that a transfer of data from one party to another party who only received header information did not constitute a communication under the Wiretap Act.[622] As this section argues, the data that the researchers state they captured does not qualify as content data because they only captured packet header information. However, unlike the receiving party in *Zynga,* the Tor users' entire packet, not just the header, went through the researchers' server.

All Tor node operators, including the academic researchers, resemble the "messenger" in the example above. It does not appear that any court has analyzed this issue as it pertains to the "party to the communication" exemption. However, given the proscription against "unseen auditors," it seems likely that node operators need to at least take some proactive action equivalent to the "speaking up" in Caro. Thus, the mere existence of information explaining how the Tor network works on the Tor website probably does not suffice as a means to establish node operators as a party to every packet of data sent through their server.

Provider Exemption: Ordinary Course of Business

The Wiretap Act also provides an exemption for "an officer, employee, or agent of a *provider* of wire or electronic communication services . . . to intercept, disclose, or use that communication in the *normal course of his employment* while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of

[622] *In re* Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014).

the provider of the service."[623] Furthermore, a provider "shall not utilize [their] service [for] observing or random monitoring *except for mechanical or service quality control checks.*"[624] Determining whether this "provider exemption" applies to the researchers first requires knowing if Tor qualifies as a provider, a question discussed in Section 2. Of course, if Tor does not qualify as a provider, this exemption will not apply to the researchers. However, for the purpose of analyzing the provider exemption as it pertains to the academic researchers, Tor is presumed to qualify as a provider under the Wiretap Act.

As stated previously, the Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[625] The "provider exemption" prohibits any type of instrument, equipment or facility used by a provider "in the ordinary course of business" from being characterized as an "electronic, mechanical, or other device."[626] Thus, providers who seemingly intercept the content of communications, which would ordinarily be a violation of Wiretap Act, are exempted so long as they are able to establish that the interception occurred "in the ordinary course of business."[627]

Accordingly, courts have ruled that one of the basic services of a provider involves acquiring the content of communications.[628] However, every action that interests a company does not become a de facto "ordinary course of business."[629] In order to qualify as an ordinary course

---

[623] 18 U.S.C.A § 2511(2)(a)(i) (West 2008) (emphasis added). The courts have construed that when an employee of a provider is acting in the "normal course of his employment" implies that the provider is acting in the "normal course of business." *See e.g.* Hall v. EarthLink Network, Inc., 396 F.3d 500 (2d Cir. 2005).
[624] 18 U.S.C.A § 2511(2)(a)(i) (West 2008).
[625] 18 U.S.C.A. § 2510(4) (West 2008).
[626] Hall v. EarthLink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005).
[627] *Id.*
[628] *See* e.g. Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1251 (10th Cir. 2012). *See also* Defendant providers needed to intercept emails in order to maintain their email services. Hall v. EarthLink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005).
[629] Watkins v. L.M. Berrry & Co., 704 F.2d 577, 582 (11th Cir. 1983).

of business, the business reasons must be "legitimate"[630] or the actions must be "shown to be undertaken normally."[631] Recently, courts have read the exemption narrowly, allowing a provider to invoke the exemption only when they show "some link between the alleged interceptions at issue and its ability to operate the communication system."[632] In *In re Google Inc.*, a recent California District Court decision, the court required a nexus between the need to intercept the contents of a communication and the provider's ability to provide "the underlying service or good."[633] The court did not find a nexus between Google's interception of email content data and its ability to provide its email service.[634] Furthermore, the court stated that a provider cannot exercise the "ordinary course of business" exemption[635] when the provider's actions violate their own policies.[636]

Clearly, Tor not only has a "legitimate" interest in ensuring user data is not compromised as it flows through Tor node servers, but an essential interest. Consequently, the question may become whether a nexus exists between the data acquired by the Colorado researchers and Tor's ability to maintain its service. This nexus probably exists. One of the stated goals of the researchers was to develop a method for identifying misuses of Tor, such as routers logging exit traffic in order to capture passwords.[637] In their paper, they claim that they successfully identified at least one router operating in this manner. Allowing node operators to surreptitiously and

---

[630] Aria v. Mut. Cent. Alar Serv., Inc., 202 F.3d 553, 559 (2d Cir. 2000).
[631] Berry v. Funk, 146 F.3d 1003, 1009 (D.C. Cir. 1998).
[632] *In re* Google Inc., 13-MD-02430-LHK, 2013 WL 5423918 *10 (N.D. Cal. Sept. 26, 2013).
[633] The court adopted the D.C. Circuit's interpretation of 18 U.S.C.A. § 2511(2)(a)(i) and applied it to the provider exemption. *Id.* at 11.
[634] *Id.* at 11.
[635] *Id.* The court found that Google collected data outside the scope of what data Google's on Privacy Policy allowed it to collect.
[636] It is unclear what Tor's internal policies are concerning the acquisition of user data and whether a Tor Privacy Policy exists that expressly prohibits Tor or its agents from collecting user data or certain types of data. Clearly, under *In Re Google Inc.,* any policy that prevents Tor or its agents from collecting the data collected by academic researchers will be fatal to the "ordinary course of business" exemption. However, *In Re Google Inc.* is merely a District Court decision and it does not appear that as of this writing any appellate court has adopted this rule.
[637]Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker, *Shining Light in Dark Places: Understanding the Tor Network* (2008).

maliciously record user data seriously undermines Tor's ability to provide secure, anonymous browsing software. This anonymity is Tor's raison d'être. If Tor or Tor's agents, which may very well include academic researchers,[638] are not able to analyze the Tor network for misuses of Tor, what's to stop the proliferation of malevolent node operators? If left unchecked, one can easily see how a surfeit of malicious node operators, or even the suspicion of malevolent operators, undermines Tor's mission. An Internet user seeking enhanced anonymity will be less likely to use a provider's network if the provider cannot take necessary steps to eradicate threats to the user's privacy, especially when the "underlying good" offered by the provider is the anonymization being sought.

HUMAN RESEARCH

This research illuminates questions as to potential violations of the federal protocols concerning research on human subjects. The guidelines protecting research on human subjects conducted or funded by the United States Department of Health are codified in federal regulations referred to as the "Common Rule."[639] Institutions that receive federal funding when conducting research on human subjects must follow these guidelines. Furthermore, researchers are required to submit their research proposals to an Institutional Review Board (IRB) for approval prior to conducting the research.[640]

Like the Wiretap Act, the Common Rule contains several exemptions.[641] The most relevant is the exemption surrounding research involving the "collection or study of existing

[638] As discussed in Section 4, it is unclear whether relay operators are in fact agents of Tor. Agent implies that the relay operators may act on Tor's behalf, which relay operators cannot necessarily do. In the future, Tor may collaborate with researchers for the purpose of optimizing the network, in which case the researchers may become agents of Tor.
[639] 55 C.F.R. § 46.101(a)(1) (2005).
[640] *Id.*
[641] 55 C.F.R. § 46.101(b)(1-6) (2005).

data, documents, records, pathological specimens, or diagnostic specimens . . . if the information *is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects*."[642]

As stated previously, the researchers claim in their report to have only collected non-content application-level header data like IP addresses and URLS. The question then becomes whether this data constitutes personally identifiable information so as to satisfy the Common Rule exemption. IP addresses do not identify a person in the same way that Social Security numbers do. Instead, they are a unique series of numbers that are able to identify a computer when cross referenced with the owner's Internet service provider.[643] Courts have ruled that IP addresses are not personally identifiable because they refer to a computer and not a person.[644] It is worth noting that the Colorado researchers only submitted their proposal to their University's Institutional Review Board (IRB) after publishing their results. While the motivations for avoiding IRB pre-clearance are unclear, the University of Colorado determined that the researchers did not violate the Common Rule, nor did they violate any rules by submitting their proposal after completing their research.[645] The IRB stated that the research did not qualify as human subject research, nor did it involve the collection of personally identifying information.[646] According to the IRB, the researchers did not need to qualify for an exemption as their research did not involve human subjects, and even if it did involve human subjects it would have qualified under the exemption for lack of personally identifiable information.

---

[642] 55 C.F.R. § 46.101(b)(4) (2005) (emphasis added).
[643] See *supra*, note 10.
[644] Johnson v. Microsoft Corp., N. C06-0900RAJ, 2009 WL 1794400, at 4 (W.D. Wash. June 23, 2009).
[645] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker, *Response to Tor Study,* COLORADO UNIV., http://systems.cs.colorado.edu/mediawiki/index.php/Response_To_Tor_Study (last updated July 25, 2008).
[646] *Id.*

The University's argument is not entirely persuasive and if legally challenged may result in a different outcome. The Common Rule exemption specifically states that human subjects cannot be identified either directly *or* through identifiers linked to the subjects.[647] While IP addresses may not directly refer to a person, they are clearly linked to the owner to the degree that any piece of property is linked to an owner. In this case, the link between the property and the property owner is especially strong. People interact with computers in ways that are distinct from other pieces of property. Furthermore, law enforcement officers have been able to obtain "transactional," non-content information such as IP addresses, browsing history and the identities of people communicating over direct messages on Twitter using d orders.[648] The information, if captured by academic researchers and analyzed in the aggregate, could be used to directly identify a human being in violation of the Common Rule, if the information became publicly available through the actions of a law enforcement officer, or through the researchers' own disclosure or through unwarranted disclosure by an independent party.

CONCLUSION

The Colorado researchers did not violate the Wiretap Act because they did not collect "content" data. However, these specific researchers carefully devised their methodology to be in compliance with the Wiretap Act and took specific steps to avoid falling within its reach. Less disciplined researchers could easily, by virtue of negligence or misfeasance, capture Tor users' content data. Researchers may be considered unilaterally consented parties to the communication and be exempt from the Act. However, they more closely represent "unseen auditors" who are not entitled to invoke the exemption. Along the same blurry lines, Tor may be considered a

[647] 55 C.F.R. § 46.101(b)(4) (2005).
[648] *In re* Application of the United States for an Order Pursuant to 18 U.S.C. 2703(d), 830 F.Supp.2d 114, 133 (E.D.Va. 2011).

provider. This classification could offer protection under the Wiretap Act's provider exemption. However, as this manual intimates, Tor is not a provider and thus not able to invoke the provider exemption.[649] Nevertheless, the legality of the research does not necessarily speak to whether operating a Tor node in order to record Tor user data constitutes an ethical use of Tor technology. The Colorado case indicates that some Institutional Research Boards may not construe non-content data as personally identifiable information. Nevertheless, the researchers decision not to make the data they captured publicly available evinces their concern for its de-anonymizing power. While perhaps not technically an unethical use of human subjects for research under the Common Rule, it does seem unethical given Tor's function as an anonymization tool and this information's potential ability to de-anonymize Tor users. Regardless, researchers should be wary in using Tor for academic research purposes since they could potentially capture content data containing personally identifiable information in clear violation of the Common Rule.

[649] For more discussion on the topic see Sections 2,4, and 5.

Section 7

The Legality of Running a Tor Relay

Question Presented: Is it legal to operate a Tor exit or non-exit relay, and could Northeastern University run its own exit relay for academic research?

BRIEF ANSWER

Currently, law enforcement officers have not brought charges against relay operators for running a relay. Advocates such as the Electronic Frontier Foundation (EFF) claim that it is legal to run a relay. At this time, running a Tor relay is legal. In order for Northeastern to decide if running a relay would be in its best interest, it must weigh the low risk of legal prosecution against the benefit of the research obtained by running the relay.

INTRODUCTION

The operation of Tor relays by individual volunteers is the most essential aspect of the functionality of the Tor network. Therefore, determining the legality of running relays is an essential question that needs to be answered in order to alleviate the worries of volunteer relay operators. The United States Navy first developed the technology used by Tor in order to provide anonymity in military communications.[650] It was later adapted and made a publicly accessible proxy in July 1996.[651] The Tor network began with only five relays on a single operating system;[652] there are now 7,000 relays worldwide,[653] with just over 1,000 of those being exit relays.[654] The legality of running an anonymous Tor relay would affect many people across

[650] Paul Syverson, *Onion Routing: A Brief History,* http://www.onion-router.net/History.html (last visited Feb. 21, 2015).
[651] *Id.*
[652] *Id.*
[653] TOR PROJECT, https://metrics.torproject.org/relayflags.html (last visited Feb. 21, 2015).
[654] *Id.*

many jurisdictions. There are approximately 2.5 million users of Tor,[655] with only a fraction using it for illegal or illegitimate purposes. Unfortunately, these few users pose a threat to the relay operators, especially exit relay operators, by potentially making them subject to legal action. The harm created by those who utilize Tor for illegal purposes causes many relay operators to worry about their safety, and ultimately decide to no longer run relays.[656] Fewer relay operators leads to a less safe and less secure network, thereby impacting millions of users.[657]

LEGALITY OF RUNNING A TOR RELAY

There appears to be a consensus throughout the legal community that running Tor relays, exit and non-exit, is legal.[658] However, this issue has yet to be decided in a court of law. The Electronic Frontier Foundation (EFF) is a major driver in eliciting people to volunteer as relay operators.[659] The EFF also claims that the operation of a Tor relay is legal; however, they caution that the running of a Tor relay creates a certain legal uncertainty, as does all new technology.[660] When someone runs a relay, they functionally allow another individual to use their device to

[655] Because of the way the system works it makes it difficult to get perfectly accurate numbers, but this is the most accurate information they can gather. TOR PROJECT, https://metrics.torproject.org/userstats-relay-country.html (last visited Feb. 21, 2015).
[656] *See e.g.* Darlene Storm, *Fingered by IP: Does it take chutzpah to run a Tor exit relay?*, COMPUTERWORLD (Sep. 1, 2011, 2:00 PM), http://www.computerworld.com/article/2470970/endpoint-security/fingered-by-ip--does-it-take-chutzpah-to-run-a-tor-exit-relay-.html; *See also*, wtwu, *Passion and Dalliance blog: Why you need balls of steel to operate a Tor exit node*, Spy-Blog (Mar. 19, 2009 11:14 AM), http://p10.hostingprod.com/@spyblog.org.uk/blog/2009/03/passion-and-dalliance-blog-why-you-need-balls-of-steel-to-operate-a-tor-exit-nod.html; *See also*, Mike Masnick, *ICE Screws Up, Seizes Tor Exit Node; Vows Not to Learn From Its Mistake*, techdirt (Aug. 26, 2011 6:30 PM), https://www.techdirt.com/articles/20110825/13360915683/ice-screws-up-seizes-tor-exit-node-vows-not-to-learn-its-mistake.shtml.
[657] ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/torchallenge/what-is-tor.html (last visited Feb. 21, 2015); *See also* TOR PROJECT, https://metrics.torproject.org/userstats-relay-country.html (last visited Feb. 21, 2015).
[658] TOR PROJECT, *The Legal FAQ for Tor Relay Operators*, https://www.torproject.org/eff/tor-legal-faq.html.en (last visited Feb. 21, 2015).
[659] The Electronic Frontier Foundation started a drive to try to get more people to volunteer to be relay operators; called the Tor Challenge. ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/torchallenge/what-is-tor.html (last visited Feb. 21, 2015).
[660] TOR PROJECT, *The Legal FAQ for Tor Relay Operators*, https://www.torproject.org/eff/tor-legal-faq.html.en (last visited Feb. 21, 2015).

access the Internet. If a user does something illegal while being routed through a relay, the operator of that relay could potentially be prosecuted for those actions.[661] Although this has not happened to date, it is uncertain if someone will be prosecuted solely for running a Tor relay in the future.

Even though relay operators have not been charged for the crimes of others using their relays, they could be arrested and have their relay-running device, such as a computer or a server, confiscated for an extended period of time.[662] These instances are rare and are usually exclusive to individuals running exit relays.[663] If the government chose to prosecute relay operators, the one way they could do so would be under the Federal Statute on "Aiding and Abetting."[664] Even so, courts have held that the government would have to prove that the relay operator acted with the same criminal intent as the perpetrator of the crime.[665] This would be very difficult to prove as oftentimes relay operators are not even aware if their relays are being used to access illegal or illegitimate content. Another way relay operators could be attacked is under federal copyright law.[666] To prove this, the government or the plaintiff would have to show

---

[661] TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 21, 2015).
[662] *See e.g.* Darlene Storm, *Fingered by IP: Does it take chutzpah to run a Tor exit relay?*, COMPUTERWORLD (Sep. 1, 2011, 2:00 PM), http://www.computerworld.com/article/2470970/endpoint-security/fingered-by-ip--does-it-take-chutzpah-to-run-a-tor-exit-relay-.html; *See also*, wtwu, *Passion and Dalliance blog: Why you need balls of steel to operate a Tor exit node*, Spy-Blog (Mar. 19, 2009 11:14 AM), http://p10.hostingprod.com/@spyblog.org.uk/blog/2009/03/passion-and-dalliance-blog-why-you-need-balls-of-steel-to-operate-a-tor-exit-nod.html; *See also*, Mike Masnick, *ICE Screws Up, Seizes Tor Exit Node; Vows Not to Learn From Its Mistake*, techdirt (Aug. 26, 2011 6:30 PM), https://www.techdirt.com/articles/20110825/13360915683/ice-screws-up-seizes-tor-exit-node-vows-not-to-learn-its-mistake.shtml.
[663] TOR PROJECT, *The Legal FAQ for Tor Relay Operators*, https://www.torproject.org/eff/tor-legal-faq.html.en (last visited Feb. 21, 2015).
[664] 18 U.S.C.A. § 2 (West 1951).
[665] Certiorari was denied by the United States Supreme Court on this issue in 1991 and courts have followed this interpretation of 18 U.S.C.A. § 2 in the First, Second, Seventh, and Eleventh Circuits. For more analysis on this issue *see* United States v. Loder, 23 F.3d 586, 590-91 (1st Cir. 1994).
[666] 17 U.S.C.A. § 102 (West 1976).

that the IP address is a plausible connection to the copyright infringement.[667] These very stringent standards have led to no one being prosecuted for solely running a Tor relay as of yet.

Exit Relay Operators

Exit relay operators expose themselves to the greatest likelihood of criminal prosecution. Even the EFF does not run an exit relay, and they caution against running one from a private residence.[668] Given that the exit relay is the last relay in the system, the relay operator's IP address is the one that is associated with the particular activity on the Internet.[669] Thus, if someone were to access something illegal, the exit relay operator would then be associated with that illegal activity via their IP address.

If law enforcement was monitoring incoming requests to a particular website containing illegal materials, they could track it back to the exit relay operator. If law enforcement were to obtain a search warrant based on the Internet activity, they could potentially prosecute the relay operator for items found on the premises during the search.[670] This is called the "good-faith exception." When law enforcement, with good faith reliance upon a legally acquired warrant, finds any evidence, even of a different crime, they would be able to present the evidence in court.[671] For example, someone could be running an exit relay legally, but due to activities associated with their IP address, they could have law enforcement officers come to their home

[667] Ashcroft v. Iqbal, 129 S. Ct. 1937, 1940 (2009); *See also*, Bell Atl. Corp. v. Twombly, 127 S. Ct. 1955, 1965 (2007).
[668] TOR PROJECT, *The Legal FAQ for Tor Relay Operators*, https://www.torproject.org/eff/tor-legal-faq.html.en (last visited Feb. 21, 2015).
[669] TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 21, 2015).
[670] *See e.g.* Massachusetts v. Sheppard, 468 U.S. 981, 987-88 (1984); *See also* United States v. Leon, 468 U.S. 897, 956 (1984).
[671] TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 21, 2015).

and search the premises. If law enforcement discovered illegal song downloads on the computer, the relay operator could be charged with copyright infringement.[672]

As a result of this possible scenario, the EFF and Tor both warn volunteers running exit relays by suggesting that they run the relays as safely as possible to protect themselves from harassment and potential legal trouble.[673] However, even if an individual were to follow all of the guidelines to running an exit node, there is no guarantee that they will not be prosecuted.

Non-Exit Relay Operator

A middle, or non-exit, relay operator has minimal legal risk associated with running a relay.[674] The operator of a middle relay is so far removed from the final step and the actual Internet activity that it would be next to impossible to connect them to a crime.[675] It would also be extremely difficult to identify anyone running a middle relay and difficult to determine whether the signal in question came from their relay.[676] The legality may be the same as that of the exit relay operator, but the likelihood of prosecution is so remote that there has not even been a case where someone has been arrested while running a middle relay.

NORTHEASTERN'S LIABILITY WHEN RUNNING A TOR RELAY

As Section 6 outlined, researchers at the University of Colorado analyzed the Tor network in order to examine Tor users' Internet activity. They wanted to discover Tor user demographic information. In the study, the researchers ran their own exit relay using university

---

[672] Lost three computers external hard drives, CDs, notebooks and various papers. Kim Zetter, *Tor Researcher Who Exposed Embassy E-mail Passwords Gets Raided by Swedish FBI and CIA*, WIRED (Nov. 14, 2007, 4:13 PM), http://www.wired.com/2007/11/swedish-researc/.
[673] Mike Perry, *Tips for Running an Exit Node with Minimal Harassment*, TOR PROJECT (Jun. 30, 2010), https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment.
[674] TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 21, 2015).
[675] *Id.*
[676] *Id.*

servers to monitor the data running through it.[677] As explained in the previous section, this study raised various legal questions under the Federal Wiretap Act.[678] The Electronic Frontier Foundation (EFF) advises people not to monitor Tor user traffic when running an exit relay because it can subject node operators to legal action under the Wiretap Act.[679] Also, there are institutional regulations that must be cleared before a university should begin any kind of research. If Northeastern University ("Northeastern") wanted to conduct a similar experiment, the researchers would first need to obtain approval from the school's Institutional Review Board.[680] Then, they would need to obtain approval from the Office for Information Security Department because the study involves the school's Internet network.[681] As stated in the previous section, the research team at the University of Colorado finely tailored their monitoring to make sure that they did not access any *content data*.[682] In order to avoid legal liability under the Federal Wiretap Act and the Common Rule, researchers at Northeastern would want to implement the same procedure.[683] Northeastern would still be opening itself up to possible law enforcement action, just as any other exit relay operator, which could possibly lead to temporary confiscation of its servers or any and all electronic devices associated with the relay.[684] Although

[677] For more information on the researcher's methods and goals, see Section 6.
Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker, *Shining Light in Dark Places: Understanding the Tor Network* (2008).
[678] 18 U.S.C. § 2511 (2008).
[679] TOR PROJECT, *The Legal FAQ for Tor Relay Operators*, https://www.torproject.org/eff/tor-legal-faq.html.en (last visited Feb. 21, 2015).
[680] Section 6 discusses the Institutional Review Board requirements as governed by the Code of Federal Regulations.
[681] 45 C.F.R. § 46.101(a)(2). *See also* "Use of University Systems to Host Non-University Activities - Use of University information systems for hosting non-University activities must have the explicit written authorization of the Office of the Provost or its designee." OFFICE OF INFORMATION SECURITY, *Policy on Appropriate Use of Computer and Network Resources*, 4 (March 5, 2014).
[682] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker, *Shining Light in Dark Places: Understanding the Tor Network* (2008).
[683] 18 U.S.C. § 2511 (2008).
[684] House and car searched even took his fertilizer. Alex "Yalla" Janßen, *Tor madness reloaded*, Blog of too many things (Sep 16, 2007), http://itnomad.wordpress.com/2007/09/16/tor-madness-reloaded/.

this did not happen to the University of Colorado, and instances are very rare, this would still be a risk for any university to take upon itself.

Northeastern's Responsibility to Law Enforcement

This type of research could become useful to law enforcement agencies to be able to de-anonymize users or to gather more information on the type of people using Tor. Northeastern would not be required to provide their research to law enforcement officers without a proper warrant because of the right to privacy implicit in the Fourth Amendment.[685] Northeastern is able to voluntarily provide the research if so desired and if it is allowed under the University's privacy policy.[686] In a recent incident, the Massachusetts Institute of Technology provided information to law enforcement willingly, which led to the prosecution of one of its students.[687] If Northeastern did not want to hand over the data, or could not under their policy, law enforcement would have to produce a judicial search warrant. Northeastern could not stop law enforcement officers from obtaining any and all information as indicated in the warrant.[688] This could lead to significant damage to the anonymity of the Tor network and could possibly be very costly to Northeastern. This did not occur in the University of Colorado study, nor is it a regular occurrence for exit relay operators.

---

[685] U.S. CONST. AMEND. IV.
[686] Northeastern University, *Professional Standards and Business Conduct Policy*, Section IX, (Jan. 2002).
[687] See the story of Aaron Swartz, where MIT willfully handed over the information to the authorities. Marcella Bombardieri, *The inside story of MIT and Aaron Swartz*, BOSTON GLOBE, (March 30, 2014), http://www.bostonglobe.com/metro/2015/03/29/the-inside-story-mit-and-aaron-swartz/YvJZ5P6VHaPJusReuaN7SI/story.html.
[688] Boston College had done research on the IRA including interviews with dissidents in Ireland promising not to release the interviews until after the interviewees' deaths. UK through the US got a subpoena and acquired access to some of the interviews. More about this issue in Question 8. *In re* Request from the United Kingdom Pursuant to the Treaty between the Gov't of the U.S. & the Gov't of the United Kingdom on Mut. Assistance in Criminal Matters in the Matter of Dolours Price, 718 F.3d 13, 26 (1st Cir. 2013).

CONCLUSION

The courts have not yet directly addressed the question of the legality of running a Tor relay and the attendant risks associated with running a Tor relay. Given that current law enforcement officers do not bring charges against relay operators for solely running a relay, and advocates such as the Electronic Frontier Foundation claim that it is legal,[689] the implication would be that running a Tor relay is legal. Even if the government were to bring charges against a relay operator, their case under either the Federal Statute on "Aiding and Abetting" or copyright infringement laws would be very difficult to prove.[690] In order for Northeastern University, as a private organization, to decide if running a relay is in its best interest, it must weigh the low risk of legal prosecution against the benefit of the research obtained by running the relay. If Northeastern University approves of the research, the Institutional Review Board would need to approve it as well and make sure that it does not conflict with any university policies. As demonstrated by the lack of prosecution, running a Tor middle or exit relay appears to be legal. The operator may be opening themselves up to other liabilities and even possible intrusion by law enforcement, but the societal benefit of running a Tor relay outweighs these risks.

[689] TOR PROJECT, *The Legal FAQ for Tor Relay Operators*, https://www.torproject.org/eff/tor-legal-faq.html.en (last visited Feb. 21, 2015).
[690] 18 U.S.C.A. § 2 (West 1951). *See also*, United States v. Loder, 23 F.3d 586, 590-91 (1st Cir. 1994).

Section 8

The Constitutionality of Anti-Harassment Laws

Question Presented: Are anti-harassment laws constitutional? Is there a way to resolve the conflict between anti-cyberstalking laws and First Amendment rights?

BRIEF ANSWER

Anti-harassment laws are constitutional, and can be effective tools for combating cyberstalking, online threats, and the escalation of those acts into violence.

The perception that anti-harassment and anti-stalking laws conflict with the First Amendment comes from a fear that the language of these laws is overly broad. Those in power could abuse the laws in order to suppress speech, or otherwise chill the expression of free speech. This potential conflict can be resolved, however, by looking to case law to establish in which contexts these laws are used. In recent cases such as *United States v. Cassidy*,[691] *United States v. Sayer*,[692] *United States v. Osinger*,[693] and *United States v. Petrovic*,[694] a clear pattern emerges where the freedom of speech remains protected, while harassers and cyberstalkers are still successfully prosecuted.

INTRODUCTION

As technology has advanced at a rapid pace over the last 20 years, online harassment and cyberstalking have not only become widespread issues, but increasingly powerful methods for abusers to control victims. Prosecutors, law enforcement officers, and advocates have had

[691] United States v. Cassidy, 814 F.Supp.2d 574 (D.Md.2011).
[692] United States v. Sayer, 748 F.3d 425 (1st Cir. 2014).
[693] United States v. Osinger, 753 F.3d 939 (3rd Cir. 2014).
[694] United States v. Petrovic, 701 F.3d 849 (8th Cir. 2012).

difficulty keeping pace with the ways abusers use technology to harass, stalk, surveil, intimidate, or even impersonate victims.

In the past, technological harassment and stalking largely took place over the Internet, such as on social media websites or via obtaining information about a target for abuse through search engines. Increasingly, abusers have repurposed computer monitoring software that was originally developed for parents to monitor their children's online activities as tools to monitor victims' computer use.[695] An abuser can use keystroke logging hardware to keep records of a victim's every computer message.[696] In addition to controlling laptop and computer use, abusers are able to stalk and harass a victim through phone use by bombarding the victim's phone with calls and text messages, impersonating a victim, or using Global Positioning System (GPS) technology to monitor a victim's physical location at all times.[697] Finally, an abuser can also harass a victim without ever contacting them by creating websites intended to embarrass or humiliate the victim, or by making abusive, but vague, public statements online that they know the victim will eventually see or hear about.[698]

It is clear technology can give abusers a great deal of control over a victim; the above is not an exhaustive list of the methods abusers will use. When this abuse is put in the context of the cycle of violence, and the way in which abusive relationships usually escalate before reaching physical violence, it becomes clear there is a substantial government interest to intervene. Thus, Congress has updated laws like the Violence Against Women Act (VAWA) to specifically prevent online harassment and cyberstalking.[699]

---

[695] George LeVines, *As domestic abuse goes digital, shelters turn to counter-surveillance with Tor*, BETA BOSTON, (May 7th, 2014), http://www.betaboston.com/news/2014/05/07/as-domestic-abuse-goes-digital-shelters-turn-to-counter-surveillance-with-tor/.
[696] *Id.*
[697] *Id.*
[698] *Id.*
[699] 42 U.S.C. §§ 13701-14040 (2008).

Many free speech advocates have expressed concerns regarding the breadth of the language in these acts.[700] They view the language as vague, and argue the stalking and anti-harassment statutes are unconstitutional limits on free speech, with potential for abuse by the government. This belief became more widespread after, in *United States v. Cassidy*, a Maryland man successfully appealed his conviction under the federal cyberstalking statute.[701] While the court did not strike the law down, it held the application of the law in that case was unconstitutional.[702]

This section of the manual will seek to reconcile anti-harassment laws and First Amendment rights, with the goal of ensuring the laws on hand protect both victims of abuse and the right to free speech.

ANALYSIS

Language of the federal statutes regarding online harassment and cyberstalking

The Violence Against Women Reauthorization Act of 2013 (VAWA 2013) expanded 18 USC § 2261A to include a provision on cyberstalking.[703] The language in the cyberstalking subsection regarding the intent of the accused is nearly identical to the subsection regarding more traditional forms of stalking.[704] Section 2261A(1), regarding traditional forms of stalking, addresses whoever "travels in interstate or foreign commerce . . . with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate

[700] Gabe Rottman, *New Expansion of Stalking Law Poses First Amendment Concerns*, Blog of Rights (Mar. 12, 2013, 1:55 PM), https://www.aclu.org/blog/free-speech/new-expansion-stalking-law-poses-first-amendment-concerns.
[701] United States v. Cassidy, 814 F.Supp.2d 574, 576 (D.Md.2011).
[702] *Id.* at 588.
[703] 18 U.S.C.A. § 2261(A) (West 2013).
[704] *Id.* § 2261(A)(1).

another person."[705] Similarly, Section 2261A(2), regarding cyberstalking, addresses whoever "with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce."[706] The VAWA appears to be the statute under which most accused abusers are charged.

Free speech advocates have argued that the language in statutes like this is unconstitutionally overbroad, specifically infringing on the First Amendment right to freedom of speech.[707] In a letter to the House of Representatives in May of 2012, the American Civil Liberties Union stated its opposition to the then-House version of the VAWA 2013, stating that "without bright lines delineating lawful speech from unlawful 'true' threats, vague or overbroad statutes criminalizing speech that could be construed as 'harassing,' 'intimidating,' or that is claimed to cause 'serious' or 'substantial' emotional distress, have a significant chilling effect on protected speech."[708]

The Electronic Frontier Foundation (EFF) voiced similar concerns in a January 2015 blog post addressing online harassment. In the post, the EFF noted it "will continue to be a staunch advocate for free speech and privacy online" and "remain critical of new regulation."[709] However, the EFF also expressed a clear desire to work with advocates and legislators to craft

[705] 18 U.S.C.A. § 2261(A)(1) (West 2013).
[706] 18 U.S.C.A. § 2261(A)(2) (West 2013).
[707] Gabe Rottman, *New Expansion of Stalking Law Poses First Amendment Concerns*, Blog of Rights (Mar. 12, 2013, 1:55 PM), https://www.aclu.org/blog/free-speech/new-expansion-stalking-law-poses-first-amendment-concerns.
[708] Letter from Laura W. Murphy, Director, and Vania Leveille, Senior Legislative Counsel, *to members of the United States House of Representatives*, AMERICAN CIVIL LIBERTIES UNION WASHINGTON LEGISLATIVE OFFICE (May 16, 2012), https://www.aclu.org/files/assets/aclu_letter_re_hr_4970_-final-5-16-12_-final.pdf.
[709] Nadia Kayyali and Danny O'Brien, *Facing the Challenge of Online Harassment*, DEEPLINKS BLOG (January 8, 2015), https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment.

legislation that protects free speech rights as well as victims of online abuse, stating "there's nothing inconsistent about loving free speech and speaking out against harassment."[710]

Facial Challenges to the Constitutionality of a Law

A court can strike down a criminal conviction on constitutional grounds if either the statute as applied to the case at hand is unconstitutional or if the statute is unconstitutional on its face. If the court deems the statute unconstitutional as applied to the case at hand, the statute remains in effect though the conviction is overturned.[711] If the court deems the statute facially unconstitutional, it strikes down the statute in addition to overturning the conviction.[712] There are several ways in which a court may strike down a statute as facially unconstitutional, including vagueness, content-bias, and overbreadth.[713] The cases below are primarily concerned with overbreadth challenges. The relevant standard for review, as set forth by the Supreme Court in *Virginia v. Hicks*, is that "rarely, if ever, will an overbreadth challenge succeed against a law or regulation that is not specifically addressed to speech or to conduct necessarily associated with speech (such as picketing or demonstrating)."[714]

Successful overbreadth challenges can come from traditional First Amendment protections

In *United States v. Cassidy*, the defendant was charged under the federal stalking statute for making abusive and harassing comments online to a public figure. In a rather unusual story, the defendant, William Cassidy, had joined a Buddhist sect claiming to be a "tulku," a high-ranking spiritual figure in Buddhism. When other members doubted his claim and he was forced

[710] Nadia Kayyali and Danny O'Brien, *Facing the Challenge of Online Harassment*, DEEPLINKS BLOG (January 8, 2015), https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment.
[711] United States v. Cassidy, 814 F.Supp.2d 574, 576 (D.Md.2011).
[712] Virginia v. Hicks, 539 U.S. 113, 118 (2003).
[713] *Id*. at 118.
[714] *Id*. at 124.

to leave the group, Cassidy made crude and inflammatory remarks about the sect's leader on Twitter and several blogs; Cassidy was charged under 18 USC § 2261A for the remarks.[715]

The United States District Court of Maryland granted Cassidy's motion to dismiss. The court agreed with Cassidy that, as applied to his case, the statute infringed on his First Amendment right to criticize a public figure (the religious sect leader).[716] The court applied intermediate scrutiny in the case and ruled that, as applied in *Cassidy*, the statute did not survive intermediate scrutiny.[717] This demonstrates that a traditional First Amendment defense to an attempted suppression of speech can overcome the cyberstalking statute. Notably, however, the court chose to not reach the facial validity of the cyberstalking provision of the stalking statute.[718]

Unsuccessful overbreadth challenges show the statute can still protect victims of abuse

While the decision in *Cassidy* alarmed supporters of the Violence Against Women Act, subsequent cases have shown the decision is a relatively narrow one.

In *United States v. Petrovic*, the defendant mailed dozens of nude photographs of his ex-wife to her family, co-workers, and other people in her community; he also launched a website where anyone could view nude pictures and videos of her.[719] The defendant made a similar overbreadth challenge as the defendant in *Cassidy*, but on appeal, the Eighth Circuit rejected the challenge, ruling,

> Section 2261A(2)(A) is directed toward "course[s] of conduct," not speech, and the conduct it proscribes is not "necessarily associated with speech." Because the statute requires both malicious intent on the part of the defendant and substantial

[715] United States v. Cassidy, 814 F.Supp.2d 574, 576 (D.Md.2011).
[716] *Id.* at 582.
[717] *Id.* at 587.
[718] *Id.* at 587.
[719] United States v. Petrovic, 701 F.3d 849, 852 (8th Cir. 2012).

> harm to the victim . . . "[i]t is difficult to imagine what constitutionally-protected . . . . speech would fall under these statutory prohibitions. Most, if not all, of the [statute's] legal applications are to conduct that is not protected by the First Amendment."[720]

In *United States v. Sayer*, the defendant posted nude pictures of his ex-girlfriend to involuntary pornography[721] websites along with her name and address, encouraging strangers to come to her home.[722] The defendant also filed an overbreadth challenge, arguing that as applied to his case, the statute violated his fundamental right to free speech.[723] On appeal, the First Circuit Court of Appeals rejected the argument, stating

> the interstate stalking statute, which prohibits a course of conduct done with 'intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate, or cause substantial emotional distress' clearly targets conduct performed with serious criminal intent, not just speech that happens to cause annoyance or insult.[724]

Finally, in *United States v. Osinger*, the defendant sent videos of his ex-girlfriend engaged in explicit sexual acts to her family, her boss, and her co-workers at her new job.[725] The defendant also filed an overbreadth challenge, and like the previous two cases, the court denied on appeal.[726] The Third Circuit Court of Appeals cited to *Petrovic*, stating "we agree with the Eighth Circuit's rationale that, because 18 USC § 2261A proscribes harassing and intimidating conduct, the statute is not facially invalid under the First Amendment."[727]

---

[720] United States v. Petrovic, 701 F.3d 849, 856 (8th Cir. 2012). (Quoting United States v. Bowker, 372 F.3d 365, 379 (6th Cir. 2004).)
[721] This memo uses the term "involuntary pornography" rather than "revenge pornography" as a reflection of the fact that many people whose images are posted on these have had the pictures stolen, rather than someone posting them in revenge. For more discussion of involuntary pornography, see Section 9.
[722] United States v. Sayer, 748 F.3d 425, 428 (1st Cir. 2014).
[723] *Id.* at 435.
[724] *Id.* at 435.
[725] United States v. Osinger, 753 F.3d 939, 941 (3rd Cir. 2014).
[726] *Id*. at 950.
[727] *Id.* at 944.

This pattern of cases shows that, despite the ruling in *Cassidy*, the clear trend indicates that the anti-cyberstalking statute is constitutional under the First Amendment, and advocates can be assured that law enforcement can successfully prosecute abusers under the statute. The connecting theme is that the statute prohibits a "course of conduct," not specifically speech, and so speech that is traditionally protected under the First Amendment will not be threatened.

Reconciling the unsuccessful overbreadth challenges with the concerns of free speech advocates through statutory definitions

While courts since *Cassidy* have been clear on the constitutionality of the statute and the proper application of it, free speech advocates may remain concerned as the dicta of the decisions does not necessarily preclude government infringement on free speech. As a hypothetical, a businessperson engaged in aggressive negotiations may be charged with intimidating the other party, when they really only intended to improve their bargaining position, as the statute bars attempts to "intimidate." A second hypothetical could involve authorities charging protesters under the "harass" clause of the statute for engaging in a protest against a corporation with aggressive online posts about the corporation.

A potential solution, then, is to provide definitions of certain terms in the statutes themselves to ease the concerns of free speech advocates. In *Osinger*, for example, the court dismissed the defendant's argument that the statute was unconstitutionally vague because,

> contrary to Osinger's argument, "harass" and "substantial emotional distress" are not esoteric or complicated terms devoid of common understanding . . . ("Black's Dictionary . . . defines harassment as 'words, conduct, or action (usu. repeated or persistent) that, being directed at a specific person, annoys, alarms, or causes substantial emotional distress in that person and serves no legitimate purpose . . .' ")[728]

[728] United States v. Osinger, 753 F.3d 939, 945 (3rd Cir. 2014).

If the legislators incorporated the definition from Black's Dictionary into the statute itself, it would go a long way towards easing the fears of free speech advocates. In particular, the definition states that harassment is conduct that "serves no legitimate purpose," which would preclude the two hypotheticals above, as courts would consider the business negotiations and the protest to be speech, not courses of conduct, and so they would not be in violation of the statute.[729] On the other hand, courts would still convict the defendants in *Petrovic*, *Sayer*, and *Osinger* under the statute, as their course of conduct did not serve any legitimate purpose.

CONCLUSION

In conclusion, advocates and attorneys for victims of online harassment and cyberstalking are potential allies to free speech advocates, and the conflict between the two on the current statutory language is resolvable. Through methods such as relying on traditional First Amendment protections and implementing statutory definitions, it is possible to protect free speech while still protecting the victims of abuse the statutes were designed to protect.

[729] BLACK'S LAW DICTIONARY (10th Ed. 2014).

Section 9

How to Handle Misused Technology

Question Presented: If citizens misuse technology, or other goods or services, should that technology or those goods or services be outlawed? Will outlawing technology eliminate abuses? How would you defend against a PinkMeth-type lawsuit?

BRIEF ANSWER

This section will first discuss why technologies, Tor and others, should not be eliminated despite misuses to which citizens subject them. This section will then describe why outlawing technologies will not eliminate abuses. Finally, this section will describe the *PinkMeth* case, and how an organization like Tor could defend against a similar type of lawsuit.

INTRODUCTION

Citizens misuse technology all of the time. That misuse does not mean that those services should be outlawed. Today, the rapidly evolving Internet is commonly misused, but there are plenty of other technologies, goods, and services that are used with bad intentions. As a society, we have made decisions to continue the use of certain technologies, despite their misuses, because the social utilities and economic benefits are so great that we do not want to make the sacrifice of not being able to use those products.

MISUSED TECHNOLOGIES, AND GOODS OR SERVICES, SHOULD NOT BE OUTLAWED DESPITE MISUSES, BUT COULD BE REGULATED

Tor is vital to a plethora of services such as communication, political discourse, and cultural development, and as such, it should not be eliminated despite how it is misused. Currently, there are many products that are still used in society, despite their misuses, such as guns, vehicles, phones, etc. A clear example of societal interests outweighing the costly misuses

can be seen in the case of transportation, and more specifically vehicles. Society needs vehicles and the benefits they provide. Vehicles and other methods of transportation are also commonly misused. They are used in a variety of crimes, including kidnapping, drug dealing, and car bombings.[730] Even when vehicles are used as intended, they can be deadly. In 2013 alone, it is estimated that there were 32,719 deaths from motor vehicle crashes.[731] Despite these misuses, no one would argue that as a society we should give up vehicles because they are dangerous. The United States government has enshrined the importance of vehicles in the law. Title 49 of the United States Code Annotated states, "The national objectives of general welfare, economic growth and stability, and security of the United States require the development of transportation policies and programs."[732] Clearly, there are many misuses that surround vehicles, but as a society we still rely on, and indeed protect their use, because their social utility has revolutionized modern society.

Society has decided not to ban vehicles, but instead has put in place laws giving vehicles less protection in some circumstances to reduce misuses. In *United States v. Howard*, the court said, "all searches require a warrant unless they are made pursuant to a small set of narrow exceptions, of which the automobile exception is one."[733] Under this exception a vehicle can be searched without a warrant when "agents have probable cause to believe the vehicle contains contraband or evidence of a crime."[734] Instead of banning technologies like vehicles, laws have been adopted to decrease misuses by giving enforcement officers greater freedom to conduct

[730] *See e.g.,* United States v. Singh, 483 F.3d 489, 489 (7th Cir. 2007) (vehicle used to transport victim while being kidnapped). *See also* United States v. One 2001 Mercedes Benz ML 320, 668 F. Supp. 2d 1132, 1132 (E.D. Wis. 2009) *as amended* (Oct. 16, 2009) (vehicle used to transport marijuana).
[731] INSURANCE INSTITUTE FOR HIGHWAY SAFETY, http://www.iihs.org/iihs/topics/t/general-statistics/fatalityfacts/state-by-state-overview (last visited Feb. 21, 2015).
[732] 49 U.S.C.A. § 101 (West 2014).
[733] United States v. Howard, 489 F.3d 484, 496 (2d Cir. 2007).
[734] United States v. Tamari, 454 F.3d 1259, 1261 (11th Cir. 2006).

searches. Tor can also be misused, but instead of banning Tor, statutes and regulations should be used to cut down on misuses.

The United States government has made it clear that they want to promote the Internet and the services it provides.[735] It is the policy of the United States "to promote the continued development of the Internet and other interactive computer services and other interactive media."[736] Similarly, in 2010 the Federal Communications Commission (FCC) adopted the Open Internet Order.[737] Transparency, no blocking, and no unreasonable discrimination are three rules the Order adopted to continue to promote "freedom and openness of the Internet."[738] This policy, similar to that of transportation, makes it clear that we have a societal interest in the benefits and utilities that Internet services provide. Congress has found that the Internet offers a forum for "political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[739] The Internet is an essential forum for these activities to take place. The United States has further made it their policy "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools."[740]

Tor gives users a place to be anonymous. Anonymity is crucial for political discourse, unique opportunities for cultural development, improving economic activities, and other intellectual activity. The Electronic Frontier Foundation (EFF) has recommended using Tor "as a

---

[735] There have been laws passed, such as the Child Online Protection Act (COPA), which has since been struck down, that have recognized potentially dangerous threats that occur on the Internet. 47 U.S.C.A. § 231 (West 1998). The government recognizes that there are dangers that accompany the Internet in statutes like COPA, and yet they still have made it their policy to promote Internet services. The government's continued promotion of the Internet is evidence that the benefits of the Internet outweigh the misuses.
[736] 47 U.S.C.A. § 230 (West 1998).
[737] *In the Matter of Preserving the Open Internet Broadband Industry Practices*, FEDERAL COMMUNICATIONS COMMISSION 17906-17908 (Dec. 21, 2010), https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf.
[738] *Id*.
[739] 47 U.S.C.A. § 230 (West 1998).
[740] *Id*.

mechanism for maintaining civil liberties online."[741] Courts have found that the "ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals to express themselves freely without fear."[742] In *McIntyre v. Ohio Elections Comm'n*, the court stated, "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind."[743] The government wants to promote the Internet and its services because the forum provides for intellectual activity that our society values.

The Internet has also revolutionized economic activity. Just as vehicles give people more freedom to live where they desire, commute more easily, and increase economic activity immensely, the Internet allows people to telecommute. The Internet helps further the expansion of international economic markets. Intellectual activity, political discourse, economic activity, and cultural development are strengthened by the anonymity that Tor provides. Tor's anonymity services create a space where survivors of domestic violence can voice their survival stories online, and where political dissidents can illuminate human rights violations that are occurring around the world.

Tor is misused, as are many Internet services. Tor is not the problem; Tor is a technology. Certain citizens misuse Tor; other citizens rely on Tor for their safety. Everyday citizens, militaries, journalists, law enforcement officers, activists, business executives, and other groups all use, and rely on, Tor.[744] The consequences of banning Tor, solely because it is misused, would be to deprive citizens of a crucial tool to speak anonymously on the Internet. Banning Tor would be a mistake and would not eliminate abuses. To cut down on misuses the government should regulate Tor. With technologies that are commonly misused, such as vehicles, the

[741] TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 21, 2015).
[742] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (US. Super. Ct. 1995).
[743] Talley v. California, 362 U.S. 60, 64 (US. Super. Ct. 1960).
[744] TOR PROJECT, https://www.torproject.org/about/torusers.html.en (last visited Feb. 21, 2015).

government has adopted special laws to cut down on the abuses.[745] The Internet is rapidly evolving and the government will need to adopt laws that regulate the misuses. Regulating Tor is an effective way to continue to promote anonymity and the open Internet, while also reducing the misuses.

OUTLAWING TECHNOLOGY WILL NOT ELIMINATE ABUSES

Banning Tor will not eliminate the abuses that the government is trying to protect against. One abuse, which has resulted in lawsuits involving Tor, has focused on those who post involuntary pornography online. Involuntary pornography involves someone obtaining private photos, and posting them online with the personal information of the individual in the photos. These abuses existed well before Tor was used. The misuses exist because of human behavior, not because of the technologies. Instead of banning Tor, the government should regulate the human behavior that is at the root of the misuse by attaching strict penalties to abuses.

In 1984, there was a lawsuit involving a woman whose private photograph was stolen and sent to Hustler Magazine.[746] Hustler then published the photograph in their magazine with the woman's personal information.[747] Despite Hustler's "safeguards" to obtain the information with permission, they were still found to have acted negligently.[748] This is very similar to what involuntary pornography websites do today. While Hustler's intent to obtain the permission of the person differed from involuntary pornography websites,[749] the idea behind posting private

[745] United States v. Tamari, 454 F.3d 1259, 1264 (11th Cir. 2006).
[746] Wood v. Hustler Magazine, Inc., 736 F.2d 1084, 1085 (5th Cir. 1984).
[747] *Id*. at 1086.
[748] *Id*. at 1085.
[749] Hustler sent a letter to the address that was listed with the photographs that were sent in, asking yes or no questions to obtain permission to use the photographs. In this case, there was a fake address listed and the person who stole the photographs filled out the letter and sent the form back to Hustler.

photos with private information is similar.[750] These abuses that occur using Tor exist because of citizens misusing the technology. The citizens that cause the misuses should be punished, not the technologies.

The act of being anonymous online should not be punished, but any criminal actions that occur while using Tor should be. Instead of banning Tor because citizens misuse it, regulations that enhance criminal liability when using Tor should be used as a deterrent method. If misuses occur while someone is using Tor, and that individual's liability is enhanced, the misuses that occur using that service should decrease. Enhancement statutes exist throughout the country as discussed in Section 10.[751] Enhancement statutes could be adopted in regards to misuses that occur when using Tor to deter citizens from partaking in those activities.

Abuses such as involuntary pornography websites existed well before Tor, and will continue to exist even if Tor was banned. The technologies are not the problem; the citizens misusing the technologies are the problem. At a certain point, society has to choose what should be banned. Clearly, not everything that contributes to crime should be prohibited. Guns, cars, cell phones, ski masks, hats, gloves, and cash all contribute to crime but no one would argue that society should eliminate those things. Items that provide benefit and utility to society should not be banned just because they are abused and cannot be banned without devastating effects.

Tor contributes to the government's goals of expanding the Internet. That alone is enough of a reason for Tor to continue to exist, despite the abuses. Some may argue that Tor is to the Internet what tinted windows are to cars, and should be banned or regulated the same way as tinted windows.[752] Tor is not like tinted windows. Being anonymous and hidden in a car does

[750] Wood v. Hustler Magazine, Inc., 736 F.2d 1084, 1094 (5th Cir. 1984).
[751] Sarah French Russell, *Rethinking Recidivist Enhancements: The Role of Prior Drug Convictions in Federal Sentencing*, 43 UC DAVIS L. REV. 1137, 1137-38 (2010).
[752] FLA. STAT. ANN. § 316.2953 (West 1999).

not promote the same interests as being anonymous online. Tor is crucial in giving citizens the ability to participate in political discourse, unique opportunities for cultural development, improving economic activities, and other intellectual activity. Like every other technology, Tor can be misused by citizens. Banning Tor will not eliminate abuses. Eliminating Tor simply eliminates one technology, and citizens will abuse other technologies that are at their disposal. Unless society wants to eliminate technology altogether, abuses will exist. Regulations should be implemented that enhance penalties when people abuse Tor to cut down on misuses. The justifications for eliminating Tor due to its misuses are not strong enough given the massive social benefits it provides.

DEFENSE AGAINST PINKMETH-TYPE LAWSUITS

Recently, Tor was involved in a lawsuit against PinkMeth, an involuntary pornography website. In the *PinkMeth* case, Shelby Conklin sued PinkMeth.com and Tor for posting pornographic pictures and personal information about her on the PinkMeth website.[753] Tor was named in the lawsuit because the plaintiff claimed that Tor and PinkMeth conspired to commit certain torts against her. [754] PinkMeth attempted to retain Tor as a co-defendant in the lawsuit by claiming Tor allowed users to post nude photographs anonymously, and because a link was provided on the site that allowed people to access PinkMeth on a secure network using Tor.[755] There was a final judgment of $1,000,000.00 awarded to Shelby Conklin against PinkMeth.com.[756] Tor was dropped from the lawsuit, but it is still important to examine how to

[753] Helen Lupercio, *RE: Shelby Conklin VS Pinkmeth.Com aka pinkmethuylnenlz.onion.lt and The Tor Project Inc. PinkMeth Summons and Complaint*, (2014), http://www.scribd.com/doc/233081133/233038130-Pink-Meth-Summons-and-Complaint.
[754] *Id*. at 8.
[755] *Id.* at 8.
[756] JasonLeeVanDyke, *Final Judgment - Shelby Conklin v. PinkMeth.com, et al.*, Scribd. (Nov 13, 2014), http://www.scribd.com/doc/246495441/Final-Judgment-Shelby-Conklin-v-PinkMeth-com-et-al.

defend against a similar lawsuit. The Communications Decency Act (CDA)[757] states "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[758]

In order to be protected by this statute, Tor needs to be considered an "interactive computer service." The statute defines an interactive computer service as any service that "provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[759] Tor is a service that provides people with access to content on the Internet. It is very likely that Tor would fall inside the definition set forth in the statute. The only other definition within the statute that might possibly apply to Tor is the access software provider definition. Access software providers are similar to interactive computer services, in that they provide software that allows people to have control over the content on their computers. The statute provides that the term "'interactive computer service' means any information service, system, or access software provider."[760] Access software providers are included in the definition of interactive computer services, so Tor should receive the same protection regardless of which definition is adopted.

Courts in the past have found that third party websites that allow other users to upload information can be categorized as interactive computer services.[761] In *Klayman v. Zuckerberg*, the plaintiff sued Facebook because of information that was posted by one of its users.[762]

---

[757] For the remainder of the Memorandum, I will refer to the immunity that providers of interactive computer services receive, under the CDA. The citations that follow that act will be to 47 U.S.C.A. § 230 (West 1998), as that is the codified version of CDA.
[758] 47 U.S.C.A. § 230 (West 1998).
[759] *Id.*
[760] *Id.*
[761] Klayman v. Zuckerberg, 753 F.3d 1354, 1355 (D.C. Cir. 2014).
[762] *Id*.

Facebook quickly deleted the offensive information.[763] Despite its speed, the plaintiff still filed a lawsuit.[764] The court dismissed the lawsuit against Facebook because they found that Facebook is protected under the Communications Decency Act.[765] If Tor is able prove that it falls under the definition of an interactive computer service, it too should be protected in suits like the *PinkMeth* case. One safeguard that Tor could use is to block access to offensive materials as it becomes aware of them. This becomes tricky because of the anonymity, but it was something that the Court noted in the Facebook lawsuit.

In a similar lawsuit, a class of women sued Texxxan.com, another involuntary pornography site.[766] GoDaddy, an interactive computer service, was also named in the lawsuit.[767] The trial court initially denied GoDaddy's motion to dismiss because the CDA does not preempt state law intentional torts.[768] On appeal, the court reversed and said that GoDaddy was an interactive computer service under Section 230 of the Telecommunications statute, not an information content provider.[769] The court held that "with regard to the material published on the websites, plaintiffs cannot maintain claims against GoDaddy that treat it as a publisher of that material."[770] The same rationale can also be applied in a case against Tor, like the *PinkMeth* suit. Tor has a much stronger argument than GoDaddy, since GoDaddy actually hosts content, while Tor just provides a temporary channel. Tor does not host any material; therefore, that argument cannot be made against it.

---

[763] Klayman v. Zuckerberg, 753 F.3d 1354, 1355 (D.C. Cir. 2014).
[764] *Id.*
[765] *Id.*
[766] GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 753 (Tex. App. 2014).
[767] *Id.*
[768] *Id.* Plaintiffs also asserted "GoDaddy is not entitled to immunity under section 230 of the CDA because the underlying content is unlawful or not entitled to First Amendment protection." *Id*. at 755.
[769] An information content provider is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C.A. § 230 (West 1998).
[770] *GoDaddy.com, LLC* at 759.

The government has a policy interest in protecting Tor. Under Section 230, the government has made it clear that they want to support Tor.[771] One suggestion for a form of self-regulation is adopting a code of conduct to ensure that providers of Internet services are acting in accord with social responsibility.[772] A representative group of Internet service agencies could be formed to adopt the code of conduct, which would allow those services to further the goals of the government in regards to the Internet, while acting in agreement with social standards.[773] The government should not provide any disincentives for an organization like Tor to exist, because Tor is advancing the government's goals in regards to the Internet. Instead of banning Tor the government may encourage it to remove offensive material as they discover it, but overall Tor is an organization that should be supported.

CONCLUSION

Tor gives users the ability to interact online with anonymity. That anonymity gives citizens the chance to communicate openly and freely, partake in unique cultural development, and exercise a freer form of speech. The government supports the Internet because it gives users a platform to participate in crucial forms of communication. Tor helps the government accomplish their goals for the Internet, but just like most other technologies, it can be misused. Under the Communications Decency Act, Tor is protected from what users post using its program.[774] It would be a mistake to ban Tor just because of the misuses. Citizens find ways to

[771] *See e.g.,* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (purpose of the CDA was to maintain "the robust nature of Internet communication"). *See* also 800-JR Cigar, Inc. v. GoTo.com, Inc., 437 F. Supp. 2d 273, 295 (D.N.J. 2006). (the purpose of the Communications Decency Act is to promote self-regulation of Internet service providers).
[772] Dr. Marcel Machill, Jens Waltermann, *Self-regulation of Internet content: towards a systematic, integrated and international approach*, CENTER FOR DEMOCRACY AND TECHNOLOGY (1999), https://www.cdt.org/files/speech/BertelsmannProposal.pdf.
[773] *Id.*
[774] 47 U.S.C.A. § 230 (West 1998).

abuse whatever technologies exist. Tor provides great social utility and has many benefits, and should therefore exist despite the misuses.

Section 10

Cyberharassment and the Wider Prospects of Sentencing Enhancements for Tor Users

Question Presented: What Constitutes Online Harassment? Does using Tor create enhanced penalties for users?

BRIEF ANSWER

Cyberharassment is harassment in the online environment. In many ways traditional harassment statutes have been modified to incorporate terminology that captures advances in communication technology. In other instances statutes remain sufficiently broad in that they do not have updated terminology, but can ostensibly capture cyberharassment as well. There is currently no available evidence that Tor use is being considered for enhanced penalties.

INTRODUCTION

This section introduces two related but not necessarily interconnected topics. It will first define the phenomenon of online harassment (cyberharassment) and trace its development as a legal concept at the state level. In the process, it will compare state laws that specifically address cyberharassment and those that do not. Secondly, the possibility of Tor creating enhanced penalties for users who may theoretically undergo criminal prosecution will be examined. This section draws an analogy between enhanced penalties for crimes committed anonymously and enhanced penalties for crimes committed anonymously using Tor. The likelihood of existing legislation creating enhanced penalties is slim. However, future legislation may create enhanced penalties for Tor use.

WHAT CONSTITUTES ONLINE HARASSMENT?

The Evolution of Cyberharassment at the State Level

Cyberharassment has emerged as a legal concept from traditional statutory definitions of harassment that have been further sculpted through common law. This section will analyze the current state of harassment law, and how existing laws are being expanded to address the growing concerns surrounding cyberharrassment. It will provide an overview of statutory recommendations expressed through the Model Penal Code, and specifically analyze two existing state laws, to provide an understanding of the state of cyberharassment policies in the U.S.

In part, cyberharassment has developed because of the ubiquitous nature of the Internet, computers, and smartphones. A recent study by the Pew Research Center has found that, "40% of Internet users have personally experienced online harassment, from the mild to the severe; [and] 73% have witnessed it occur to others."[775] Online harassment often takes the forms of name-calling, intentional embarrassment, and physical threats.[776] Online harassment enables an increased level of anonymity for the perpetrator. In many cases, state legislatures have had to quickly adapt their laws to changing technology to address these contemporaneous versions of more traditional crimes.[777] Cyberharassment is but one example of an old crime which has thrived in its new online environment.

---

[775] Maeve Duggan, *Online Harassment,* PEW RESEARCH CENTER, (October 22, 2014), http://www.pewinternet.org/2014/10/22/online-harassment.
[776] *Id*. at pg. 6.
[777] Andrew Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law To Include Electronic Communications*, 74 MO. L. REV. 379, 382 (2009).

In 1962 the American Law Institute fashioned a Model Penal Code (MPC) in an effort to "serve as a basis for comprehensive legislative reform in every American jurisdiction."[778] The primary goal of the MPC was to provide a basic standard to assist lawmakers in the drafting of legislation to ensure a level of continuity across the nation's many jurisdictions. The MPC defines harassment in the following way:

> Section 250.4. Harassment
>
> A person commits a petty misdemeanor if, with purpose to harass another, he:
> (1) makes a telephone call without purpose of legitimate communication; or
> (2) insults, taunts, or challenges another in a manner likely to provoke violent or disorderly response; or
> (3) makes repeated communications anonymously or at extremely inconvenient hours, or in offensively coarse language; or
> (4) subjects another to an offensive touching; or
> (5) engages in any other course of alarming conduct serving no legitimate purpose of the actor.[779]

While the MPC has fulfilled its purpose as a statutory prototype, advances in technology have necessitated changes in the statutory language of state laws. "In 1978, state legislatures began enacting computer crime statutes, beginning with Arizona and Florida. Since then, every state has enacted some form of computer-specific criminal legislation."[780] A comprehensive effort to combat online harassment is evident nationwide; although each state addresses the problem differently.

> Massachusetts specifically addresses cyberharassment:
> Section 43A. (a) Whoever willfully and maliciously engages in a knowing pattern of conduct or series of acts over a period of time directed at a specific person, which seriously alarms that person and would cause a reasonable person to suffer substantial emotional distress, shall be guilty of the crime of criminal harassment … The conduct or acts described in this paragraph shall include, but not be limited to, conduct or acts conducted by mail or by use of a telephonic or

[778] Kadish, Schulhofer, Steiker, Barkow, *Criminal Law and its Processes: Cases and Materials*, 1191, 9th Ed. (2012).
[779] Kadish, Schulhofer, Steiker, Barkow, *Criminal Law and its Processes: Cases and Materials*, 1250, 9th Ed. (2012).
[780] Chris Kim, Barrie Newberger, Brian Shack, *Computer Crimes*, 49 AM. CRIM. L. REV. 443, 443 (2012).

> telecommunication device or electronic communication device including,…but not limited to, electronic mail, internet communications, instant messages or facsimile communications.[781]

Conversely, New Mexico does not specifically address cyberharassment:

> **(A)** Harassment consists of knowingly pursuing a pattern of conduct that is intended to annoy, seriously alarm or terrorize another person and that serves no lawful purpose. The conduct must be such that it would cause a reasonable person to suffer substantial emotional distress.
> **(B)** Whoever commits harassment is guilty of a misdemeanor.[782]

There are notable differences between states such as Massachusetts, which specifically identify harassment via email and the Internet, and states like New Mexico, which do not. However, the lack of specificity in certain harassment statutes, such as New Mexico's, could provide the flexibility necessary to criminalize online harassment. New Mexico's statute does not explicitly preclude prosecuting online harassment. The MPC's statutory harassment model provides similar flexibility.

A lack of specificity within a state harassment statute can afford some prosecutorial flexibility, but it can also conflict with the Supreme Court's *void for vagueness* doctrine, requiring that laws not be substantially overbroad.[783] Under the *void for vagueness* doctrine, statutes that "fail to provide to the kind of notice that [would] enable ordinary people to understand what conduct it prohibits are unconstitutional."[784] A statute that fails to define key terms can be challenged for being overbroad.[785]

---

[781] MASS. GEN LAWS ch. 265, §43A (2015).
[782] N.M. STAT. ANN. § 30-3A-2 (West 2014).
[783] Henderson, *supra* note 777, at 387.
[784] Tyler Newby, *The Impact Of Recent Cyberstalking And Cyberharassment Cases: Leading Lawyers On Navigating Privacy Guidelines And The Legal Ramifications Of Online Behavior. Developments in Cyberstalking And Cyberharassment Law: What Attorneys Need To Know*, WL 1600592 (2014). (Quoted in City of Chicago v. Morales, 527 U.S. 41, 56 (1999).)
[785] *Id.* 7.

States are still working to address cyberharassment. For example, the National Conference of State Legislatures (NCSL) is compiling information on cyberharassment.[786] Its website collects and displays information from across the many U.S. jurisdictions to increase familiarity with state harassment laws. According to NCSL:

> Cyberharassment usually pertains to threatening or harassing email messages, instant messages, or to blog entries or websites dedicated solely to tormenting an individual. Some states approach cyberharrassment by including language addressing electronic communications in general harassment statutes, while others have created stand-alone cyberharassment statutes[787]

The pervasive nature of the Internet, coupled with the multitude of tools used to access it, have created challenges for online harassment legislation. However, regarding harassment and its evolution into what we call cyberharrassment today, existing laws appear to have been relatively easily adapted to the new online world.[788] Otherwise, these laws may exist with enough flexibility to meet the new challenges resulting from technological advances, but this flexibility can come at a cost. There are drawbacks. The Supreme Court's *void for vagueness* doctrine could invalidate a harassment statute that lacks specificity, like New Mexico's statute.[789] Despite the best efforts of state legislatures to combat online harassment, criminals and those who wish to exploit quickly developing technologies will attempt to remain one step ahead.

DOES USING TOR CREATE ENHANCED PENALTIES FOR USERS?

Sentencing enhancements are used by the legal system to address aggravating circumstances that may arise during the commission of a crime. The 2014 United States

---

[786] NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx (last visited Feb. 27, 2015).
[787] NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx (last visited Feb. 27, 2015).
[788] Andrew Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law To Include Electronic Communications*, 74 MO. L. REV. 379, 382 (2009).
[789] Andrew Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law To Include Electronic Communications*, 74 MO. L. REV. 379, 387 (2009).

Sentencing Commission Guidelines Manual outlines suggested federal criminal enhancements.[790] During a robbery, for example, "Possession or use of a weapon, physical injury, and unlawful restraint sometimes occur."[791] Many state enhancement guidelines have a similar framework and operate with similar goals.[792]

This part will provide an overview of sentencing enhancements. Next it will draw an analogy to current anonymity curbing laws and apply this to Tor. This part will conclude with a discussion of potential future legislation that could undermine the Tor's anonymity.

There are a number of enhancements that increase penalties for certain crimes. For example sentencing enhancements can be attached to (1) recidivism,[793] (2) hate crimes,[794] and (3) the commission of a crime within a school zone.[795] Currently, "All fifty states have some form of enhancement statutes, and state sentencing guidelines regimes across the country contain enhancement provisions."[796]

Enhancement statutes increase a sentence according to the manner in which a crime is committed.[797] The Supreme Court has held that enhancements are constitutional and do not

[790] USSC, *Guidelines Manual,* (2014). The USSC is an independent agency within the Judicial branch. Its principal purposes are: (1) to establish sentencing policies and practices for the federal courts, including guidelines to be consulted regarding the appropriate form and severity of punishment for offenders convicted of federal crimes; (2) to advise and assist Congress and the executive branch in the development of effective and efficient crime policy; and (3) to collect, analyze, research, and distribute a broad array of information on federal crime and sentencing issues, serving as an information resource for Congress, the executive branch, the courts, criminal justice practitioners, the academic community, and the public. The U.S. Sentencing Commission was created by the Sentencing Reform Act provisions of the Comprehensive Crime Control Act of 1984.
[791] USSC, *Guidelines Manual*, § 2B3.2 Pg. 117 (2014).
[792] NATIONAL CENTER FOR STATE COURTS, *State Sentencing Guidelines: Profiles and Continuum* (2008).
[793] Sarah French Russell, *Rethinking Recidivist Enhancements: The Role of Prior Drug Convictions in Federal Sentencing*, 43 UC DAVIS L. REV. 1137, (2010).
[794] Hate crimes have been widely challenged as unconstitutional (Examples incl: TX. GA.)
[795] PRISON POLICY INITIATIVE, http://www.prisonpolicy.org/zones.html (last visited, Mar. 8, 2015).
[796] Sarah French Russell, *Rethinking Recidivist Enhancements: The Role of Prior Drug Convictions in Federal Sentencing*, 43 UC DAVIS L. REV. 1137, 1137-38 (2010).
[797] United States v. Watts, 519 U.S. 148, 154 (1997).

constitute double jeopardy.[798] There is little evidence that sentencing enhancements could attach to Tor use.[799]

How has Anonymity been previously addressed?

Many states have anonymity preventing legislation on the books. For instance, Florida's statute concerns criminal anarchy, treason, and other crimes against public order states. The Florida statute creates penalties for when a person wears a mask, hood, or other device:

> (3) With the intent to intimidate, threaten, abuse, or harass any other person; or
> (4) While she or he was engaged in conduct that could reasonably lead to the institution of a civil or criminal proceeding against her or him, with the intent of avoiding identification in such a proceeding.[800]

Law enforcement and prosecutors at the state and federal level are increasingly aware of the attractiveness of anonymity networks to criminal enterprises.[801] While Tor use hasn't worked its way into the realm of sentencing enhancement, those who choose to use the network for nefarious purposes have recently drawn fire as evidenced in a complaint filed by the federal government in the Southern District of New York.[802] The complaint seeks the forfeiture of all assets of 27 named websites (and others yet to be named) that operate on the Tor network,

---

[798] Witte v. United States, 515 U.S. 389, 400 (1995).
[799] These cases stand for the contention that Tor use has not created sentencing enhancements *See e.g.* U.S. v. Brown, U.S. Dist., M.D. Tenn., Nashville WL 5846382 (2014). *See also* United States v. Pierce, 2014 U.S. Dist. LEXIS 108171 (D. Neb. July 28, 2014). *See also* United States v. Berger, 2012 U.S. Dist. LEXIS 111806 (N.D. Fla. June 12, 2012). *See also* FTC v. Asia Pac. Telecom, Inc., 788 F. Supp. 2d 779 (N.D. Ill. 2011). *See also* SEC v. Shavers, 2014 U.S. Dist. LEXIS 130781 (E.D. Tex. Sept. 18, 2014). *See also* United States v. Ulbricht, 2014 U.S. Dist. LEXIS 93093 (S.D.N.Y. 2014). *See also* United States v. McGrath, 2014 U.S. Dist. LEXIS 12304 (D. Neb. Jan. 31, 2014). *See also* United States v. Reibert, 2014 U.S. Dist. LEXIS 181252 (D. Neb. Dec. 12, 2014). *See also* United States v. Williams, 592 F.3d 511 4th Cir. Va. (2010).
[800] FLA. STAT. TITLE XLVI CHAPTER 876.12-876.15 (2014).
[801] 2014 WL 5788806 (S.D.N.Y.) (Trial Pleading) United States District Court, S.D. New York.
[802] Complaint WL 5788806 (S.D.N.Y.) United States District Court, S.D. New York.
United States of America, v. Any and all Assets of the Following Dark Market Websites Operating on the Tor Network (2014).

"including but not limited to the '.onion' addresses of the websites, the servers hosting the websites, and any bitcoins or other digital currency residing on those servers."[803]

It could be argued that anonymity provokes questions regarding the intentions of those who wish to remain unknown. Historical racial tension in the south provided support for laws penalizing disguising oneself. In the past, intimidation by groups like the Ku Klux Klan provided rationale for such laws.[804] However, these laws have not always withstood constitutional challenges regarding freedom of expression and free speech.[805] For example, Florida Supreme Court struck down a statute similar to the statue above for being overbroad.[806]

Currently many states prohibit identity concealment through the use of a mask for a variety reasons.[807] However, it is worth asking if laws designed to prevent anonymity for legitimate reasons in the past, may be used to erode online anonymity in the future. If there is a link between the contemporary concerns, terrorism and online criminal behavior, to historical concerns, then online anonymity provided by Tor, might similarly undergo increased legal scrutiny.

CONCLUSION

Online anonymity is concerning to governments because of the current climates of international terrorism and cybercrime, despite online anonymity's multitude of beneficial uses. However, at this time, governments have not prosecuted users who simply seek to remain anonymous online. Nor is there indication that enhanced penalties will attach to users of Tor that

---

[803] Complaint WL 5788806 (S.D.N.Y.) United States District Court, S.D. New York.
United States of America, v. Any and all Assets of the Following Dark Market Websites Operating on the Tor Network (2014).
[804] State v. Miller, 260 Ga. 669 (1990).
[805] Church of the Am. Knights of the KKK v. Kerik, 232 F. Supp. 2d 205 (S.D.N.Y. 2002).
[806] Robinson v. State, 393 So. 2d, 1076 (Fla. 1980).
[807] *See e.g.* MGL. ALM GL CH. 268, § 34. *See also* W. VA. CODE § 61-6-22. *See also* CAL PEN CODE § 185. *See also* N.C. GEN. STAT. § 14-12.8.

step outside the confines of the law. Despite this, keeping a keen eye toward proposed legislation will be beneficial going forward. Currently, it appears that past identity concealment legislation is not being adapted to the Internet, but that is not to say that in the future anonymity will not be eroded through different means.[808]

[808] Future research should consider the interest the U.S. government and the states express in further regulation of the Internet. The questions for future research should include: does there seem to be an incremental shift in favor of more governmental control? Is there a detectable pattern that has been previously used to implement increased regulation outside of the Internet? How will the individual anonymity of users online be preserved or eroded?

Section 11

Lawsuits against Backpage and their Applicability to Tor

Question Presented: How might recent Backpage lawsuits be used to erode freedom of the press and freedom of speech and what ulterior motives can drive efforts to abridge those freedoms? What effect would closing Backpage have on eliminating child exploitation? If a Backpage-type argument was used to try to shut down Tor, how would you argue against it?

BRIEF ANSWER

In several recent lawsuits, Backpage successfully claimed immunity from prosecution for hosting illegal third party content under Section 230 of the Communications Decency Act (CDA).[809] The CDA grants online service providers broad immunity against claims based on third-party content. Jurisdictions have also stated that statutes criminalizing the unknowing advertisement of commercial sexual abuse of a minor are likely in violation of the First Amendment. Closing Backpage would not make a significant difference in the fight against child exploitation. In fact, it might hinder law enforcement efforts to prevent it. The CDA covers interactive computer services, which includes Tor. If Tor faced litigation for hosting illegal third party content, Tor would be immune from prosecution under the CDA. Additionally, Tor's lack of scienter would potentially grant it First Amendment protection.

INTRODUCTION

The 2014 Backpage lawsuit involves two underage women who were forced into prostitution. Traffickers used Backpage.com, an online classifieds section, to advertise the women. The women filed suit in October 2014 against Backpage for hosting their

[809] 47 U.S.C. § 230(c)(1) (1998).

advertisements.[810] Although this case is still ongoing, there are fully litigated lawsuits against Backpage with similar fact patterns as the 2014 case.[811] In these lawsuits, Backpage has successfully claimed immunity from prosecution under Section 230 of the CDA.[812] In *M.A. v. Vill. Voice Media Holdings*, Backpage successfully moved to dismiss the case when the court held that the operating a website, without creating the content, is covered under CDA.[813] In *Backpage.com, LLC v. McKenna*, the court held that that a statute that criminalized advertising commercial sexual abuse of a minor was preempted by the CDA. In dicta, the court also stated that were they prosecuted under such a statute, it would violate the scienter requirement of the First Amendment.[814]

This section will begin by analyzing § 230 of the Communications Decency Act. It will then explore First Amendment protections for interactive computer services. Next, it will examine attempts to use a Backpage lawsuit to erode the CDA and First Amendment free speech protections. Finally, this section will discuss the potential effect that closing Backpage would have on child sexual exploitation, and Tor's defenses against a potential Backpage-type lawsuit.

IMMUNITY PROVIDED BY SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

The CDA provides online service providers broad immunity from claims based on illegal third party content. In enacting this legislation Congress granted an immunity to interactive

[810] Doe (1) et al v. Backpage.com, LLC et al.
[811] M.A. v. Vill. Voice Media Holdings, 809 F. Supp. 2d 1041 (E.D. Mo. 2011). *See e.g.* Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262 (W.D. Wash. 2012). *See also* Backpage.com, LLC v. Hoffman, No. 13-CV-03952 DMC JAD, 2013 WL 4502097 (D.N.J. Aug. 20, 2013). *See also* Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805 (M.D. Tenn. 2013).
[812] M.A. v. Vill. Voice Media Holdings, 809 F. Supp. 2d 1041 (E.D. Mo. 2011). *See e.g.* Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262 (W.D. Wash. 2012). *See also* Backpage.com, LLC v. Hoffman, No. 13-CV-03952 DMC JAD, 2013 WL 4502097 (D.N.J. Aug. 20, 2013). *See also* Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805 (M.D. Tenn. 2013).
[813] M.A. ex rel. P.K. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041, 1050 (E.D. Mo. 2011).
[814] Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1277 (W.D. Wash. 2012).

computer services unavailable to other information mediums such as television, radio and print media.[815] Tor is considered an interactive computer service. The term interactive computer service "means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet."[816] Congress created the CDA to promote the continued development of the Internet and interactive computer services and to preserve the vibrant and competitive free market on the Internet.[817] Congress also created the CDA in order to encourage interactive computer services to self-police themselves for illegal content.[818] For further information on the background of the CDA, see Section 9.

Backpage's knowledge of potentially illegal content does not make Backpage liable for hosting that content

Backpage's awareness of illegal advertisements created by third parties and hosted on Backpage's classifieds section will have no bearing on their immunity from liability under the CDA, even though they have dealt with this issue in the past. Advertisements posted by a third party will not be classified as the interactive service provider's own speech merely because the interactive service provider had notice of the advertisement's illegal content.[819] The legislature articulated that withholding this immunity could cause websites to overly censor their hosted third party content in an attempt to avoid prosecution. This exaggerated level of self-censorship would directly contradict the principle aims of the CDA, as the CDA seeks to promote the continued development of the Internet.[820]

[815] Blumenthal v. Drudge, 992 F. Supp. 44, 49 (D.D.C. 1998).
[816] 47 U.S.C. § 230(f)(2) (1998).
[817] 47 U.S.C. § 230(B)(1)-(2) (1998).
[818] Batzel v. Smith, 333 F.3d 1018, 1028 (9th Cir. 2003).
[819] Universal Commun. Sys. v. Lycos Inc., 478 F.3d 413, 420 (1st Cir. 2007).
[820] *Id.*

Backpage's creation of an "erotic services" category does not make Backpage liable for the hosted third party content

The "erotic services" category on Backpage's website does not create a potential for liability when third parties post advertisements in that category. In *Dart v. Craigslist, Inc.*, the court found § 230 immunity protected a website from claims that the website facilitated prostitution.[821] Craigslist created an "erotic services" category, but their users created the content of the advertisements and selected the categories in which their advertisements would appear.[822] The court in *Dart* held that the word-search function provided by Craigslist did "not cause or induce anyone to create, post, or search for illegal content."[823] Despite the fact that the website built and operated the "erotic services" category, the website still did not create the illegal content, and thus was not liable.[824]

Backpage profiting from illegal advertisements does not make them liable for the content in those advertisements

Even though Backpage earns revenue from the illegal advertisements and provides tools to increase their reach and usability, it maintains immunity under the CDA.[825] In *Goddard v. Google*, the court held that "the fact that a website elicits online content for profit is immaterial; the only relevant inquiry is whether the interactive service provider 'creates' or 'develops' that content."[826]

[821] Dart v. Craigslist, Inc., 665 F. Supp.2d 961 (N.D. Ill. 2009).
[822] *Id.*
[823] *Id.* at 969.
[824] Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007).
[825] Goddard v. Google, Inc., No. C 08-2738JF(PVT), 2008 WL 5245490, at *3 (N.D. Cal. Dec. 17, 2008).
[826] *Id.*

Thus, interactive computer services like Backpage are immune from prosecution under the CDA even if they (1) know they are hosting illegal content, (2) make special categories and create tools that facilitate access to illegal content, and (3) profit from that content.

FIRST **AMMENDMENT PROTECTIONS PROVIDED TO INTERACTIVE SERVICE PROVIDERS**

Although the Communications Decency Act provides immunity to interactive service providers in terms of hosted illegal third party content, Congress can amend the legislation in the future. Consequently, it is vital that Backpage, and by extension Tor, has First Amendment protections, which Congress cannot nullify without violating the Constitution.

Courts have not definitively decided the First Amendment issue. The immunities provided to interactive service providers by the CDA preempt any binding decisions under the First Amendment. Due to the CDA, no case explicitly states that a statute criminalizing the advertisement of commercial sexual abuse of a minor by an interactive service provider violates the First Amendment. In *Backpage.com, LLC v. McKenna*, *Backpage.com, LLC v. Cooper*, and *Backpage.com, LLC v. Hoffman*, the court held that such a statute is likely in violation of the First Amendment even though the CDA preempts the issue.[827] In *Backpage.com, LLC v. Cooper*, Backpage sued the Attorney General of Tennessee. Tennessee enacted a new law criminalizing the advertisement of the commercial sexual abuse of a minor. When prosecuted under this statute, an interactive computer service like Backpage could be found liable despite lack of knowledge that the advertisement depicted a minor.[828] Because a defendant does not need to know of the hosted content's illegality, the courts in *Cooper* and *McKenna* found that the state

[827] Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262 (W.D. Wash. 2012). *See e.g.* Backpage.com, LLC v. Hoffman, No. 13-CV-03952 DMC JAD, 2013 WL 4502097 (D.N.J. Aug. 20, 2013). *See also* Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805 (M.D. Tenn. 2013).
[828] Tenn. Code Ann. § 39-13-315 (West 2012).

laws likely violated the Constitution as they didn't fulfill the scienter requirement of the First Amendment due to the lack of the required mens rea.[829]

Given these rulings, the First Amendment will likely protect interactive service providers like Backpage and Tor in the absence of CDA protection. However, the immunities for interactive service providers found in the CDA preempt any court from deciding this issue.

HOW IS THE RECENT BACKPAGE LAWSUIT BEING USED TO ERODE THE FREEDOM OF THE PRESS AND FREEDOM OF SPEECH AND WHAT ULTERIOR MOTIVES CAN DRIVE EFFORTS TO ABRIDGE THOSE FREEDOMS?

The recent lawsuits against Backpage.com have attempted to eliminate CDA and First Amendment protections given to online content hosts against illegal third party content. The CDA was created in order to ensure information could be freely disseminated, but it is facing challenges on the grounds that it protects websites disseminating illegal sexual material. The Electronic Frontier Foundation (EFF) fights to prevent laws from unintentionally infringing on free speech rights. In 2012, the EFF assisted Backpage and the Internet Archive, a website that hosts copies of webpages in certain moments in time. They filed an injunction to prevent the enactment of a new law in the state of Washington, Wash. S.B. 6251, which targeted indirect publication and dissemination of any underage commercial sex act.[830] The court found that the Washington law was in direct violation of the CDA and likely violated the First Amendment. Due to this, the law was not implemented, and Backpage and the Internet Archive were granted the injunction they sought.

Those who are trying to abridge freedom of speech are able to frame issues in agreeable terms, which critics have a hard time arguing against. There are many historical examples, most

[829] Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1284 (W.D. Wash. 2012); *See also* Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805, 830 (M.D. Tenn. 2013).
[830] Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1268 (W.D. Wash. 2012).

recently, when legislators used terrorism and homeland security as the basis to justify increased surveillance and decreased privacy rights as embodied in the Patriot Act.[831] Because of the national sentiment after the attacks on September 11, 2001, legislation was passed that decreased privacy and due process rights in the United States.[832] Similarly, national security was also used as a justification for Japanese internment and the Red Scare.

If those attempting to abridge the freedom of speech of online interactive service providers are able to revoke the CDA immunity, it is likely but uncertain the First Amendment would provide protection to those service providers.

CLOSING BACKPAGE WILL NOT SIGNIFICANTLY REDUCE CHILD SEXUAL EXPLOITATION

Closing Backpage will not make a significant impact on the fight to eliminate child sexual exploitation. The history of child sexual exploitation is long, with protests against child prostitution organized by Josephine Grey dating back to the 1800s.[833] Today, roughly 1.8 million children in the United States have been victims of sexual assault[834] and an estimated 100,000 American juveniles are prostituted every year.[835]

Closing Backpage would hamper law enforcement efforts to prevent child sexual exploitation. Law enforcement is able to monitor the advertisements on Backpage and other large

---

[831] UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, PL 107–56, October 26, 2001, 115 Stat 272.
[832] Brett Burney, *The Patriot Act,* GP SOLO MAGAZINE, (July/Aug. 2007), http://www.americanbar.org/content/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/patriot_act.html.
[833] *Josephine Butler 1828-1906*, HERSTORIA (July, 5 2012), http://herstoria.com/?p=450.
[834] Kilpatrick, D., R. Acierno, B. Saunders, H. Resnick, C. Best, and P. Schnurr, *"National Survey of Adolescents," Charleston, SC: Medical University of South Carolina, National Crime Victims Research and Treatment Center,* (1998).
[835] Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1267 (W.D. Wash. 2012).

websites that offer erotic service listings like MyRedBook.com.[836] These are valuable resources for law enforcement because the websites are visible and can be monitored.[837] Closing Backpage and similar websites would push advertisements for child sexual exploitation to new, possibly more obscure websites.[838] This would hamper law enforcement efforts to arrest the traffickers responsible and rescue the underage victims.

In 2009, Craigslist eliminated the "erotic services" section of its website and then a year later eliminated its "adult services" section which had replaced it. This closing only had a minimal impact on the number of online escort advertisements because the traffic migrated from Craigslist to other websites.[839] One of the websites with the largest spikes in traffic after the closure was Backpage.[840] If Backpage were shut down, the long-term effect would be minimal. Traffic would shift to other online classified websites and the government would have to initiate a constant process of shutting them down, leading to a "whack-a-mole" situation. By shutting down Backpage, the public would be losing services, and law enforcement efforts would be hampered. Similarly, if Tor were shut down, the public would be losing access to valuable services like anonymity software.

Assuming Backpage is protected under the First Amendment, if the government tried to shut down Backpage through legislative action, the regulation would need to meet strict scrutiny. Strict scrutiny must be "such that it is narrowly tailored to promote a compelling government

---

[836] Mark Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, USC ANNENBERG CENTER ON COMMUNICATIONS LEADERSHIP & POLICY RESEARCH SERIES ON TECHNOLOGY AND HUMAN TRAFFICKING, (Nov. 2012) at 30.
[837] *Id.*
[838] *Id.*
[839] *Backpage.com, LLC v. McKenna*, 881 F. Supp. 2d at 1282-83; Mark Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, USC ANNENBERG CENTER ON COMMUNICATIONS LEADERSHIP & POLICY RESEARCH SERIES ON TECHNOLOGY AND HUMAN TRAFFICKING, (Nov. 2012) at 27.
[840] Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805, 815 (M.D. Tenn. 2013).

interest."[841] While curtailing child sexual exploitation is a certainly a compelling government interest, the government must not restrict speech any further than necessary to achieve its goal in order to ensure "that legitimate speech is not chilled or punished."[842] In a strict scrutiny test, the regulation must be the "least restrictive means among available, effective alternatives."[843] The government has the burden to prove that a plausible and less restrictive alternative to closing down Backpage would be "ineffective to achieve its goals."[844] This would be very difficult because there are many alternatives that can achieve the same goal without restricting free speech to the same degree.

Closing Backpage would not have a major impact on child sexual exploitation. By losing a highly visible website, law enforcement would lose a valuable tool in identifying underage victims and the web traffic from Backpage would migrate to other websites. Also, assuming that Backpage has protection under the First Amendment, the government would have a high degree of difficulty overcoming the strict scrutiny standard needed to enact legislation to shut down Backpage.

IF A BACKPAGE-TYPE ARGUMENT WAS USED TO TRY TO SHUT DOWN TOR, HOW WOULD YOU ARGUE AGAINST IT?

There are many differences between the services that Tor and Backpage offer. Backpage is an online classifieds website, while Tor is a program that provides online anonymity services. Despite the two companies' differences, Tor would still be considered immune from prosecution under the Communications Decency Act.

[841] Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805, 837 (M.D. Tenn. 2013).
[842] Ashcroft v. Am. Civil Liberties Union, 542 U.S. 656, 666 (2004).
[843] *Id.*
[844] United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 816 (2000)

If Tor was facing litigation for allowing access to or hosting illegal third party content, they would likely be immune from prosecution under the CDA because their status as an interactive computer service qualifying them for immunity. Tor has a stronger argument regarding its own immunity under the CDA than Backpage, because Tor's services are more closely aligned with the legislative intent of the CDA.[845] Congress created these immunities to promote the continued development of the Internet and to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services.[846] Tor, a provider of secure encrypted Internet access, provides anonymous free speech, which better exemplifies the CDA's goals than Backpage, which simply hosts online classifieds.

Overall, Tor is covered under the CDA because it is an interactive computer service. Thus, if it was facing litigation for facilitating access to illegal third party content, Tor could successfully claim immunity and would also potentially be protected under the First Amendment for lack of scienter.

[845] 47 U.S.C. § 230(B)(1)-(2) (1998).
[846] *Id.*

INDEX

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X