Washington University Global Studies Law Review

Volume 11 | Issue 3

2012

The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks

Keith D. Watson
Washington University School of Law

THE TOR NETWORK: A GLOBAL INQUIRY INTO THE LEGAL STATUS OF ANONYMITY NETWORKS

I. INTRODUCTION

On July 29, 2010, Jacob Appelbaum, the only known American member of the whistle-blowing organization WikiLeaks, was detained by U.S. agents as he attempted to reenter the country.[1] The agents frisked him, searched his bag, photocopied his receipts, and inspected his laptop.[2] Appelbaum was questioned about WikiLeaks, which leaked numerous classified government documents relating to the war in Afghanistan only days earlier.[3] The agents also questioned him about his views on the United States' involvement in Afghanistan and Iraq and his knowledge of the whereabouts of WikiLeaks founder Julian Assange.[4] Since then,

1. Nathaniel Rich, *The Most Dangerous Man in Cyberspace*, ROLLING STONE, Sept. 2, 2010, at 71.

2. *Id.*; Elinor Mills, *Researcher Detained at U.S. Border, Questioned About Wikileaks*, CNET (July 31, 2010), http://news.cnet.com/8301-27080_3-20012253-245.html.

3. Rich, *supra* note 1.

4. *Id.* Assange has become a lightning rod for the WikiLeaks cause. Federal prosecutors are exploring their options for convicting Assange and other WikiLeaks members on the basis of having "encouraged the theft of government property." Adam Entous & Evan Perez, *Prosecutors Eye WikiLeaks Charges*, WALL ST. J. (Aug. 21, 2010), http://online.wsj.com/article/SB10001424052748704488404575441673460880204.html. In January 2011, federal prosecutors subpoenaed Twitter for records of several individuals related to WikiLeaks, including: Assange and Appelbaum, Pfc. Bradley Manning (the alleged source of the Afghan War Logs leak and the "Collateral Murder" video), Rop Gonggrijp, and Birgitta Jonsdottir. *See* Scott Shane and John F. Burns, *Twitter Records in WikiLeaks Case Are Subpoenaed*, N.Y. TIMES, Jan. 9, 2011, at A1, *available at* http://www.nytimes.com/2011/01/09/world/09wiki.html?pagewanted=all. The subpoena was the first public evidence of a formal investigation into WikiLeaks. *Id.* Though the subpoena was filed under seal, Glenn Greenwald posted a copy of the subpoena on his blog; Salon has since removed the subpoena from its site, but it can be accessed through the Internet Archive's Wayback Machine. *See* http://web.archive.org/web/20110108131805/http://www.salon.com/news/opinion/glenn_greenwald/2011/01/07/twitter/subpoena.pdf [hereinafter Twitter Order]. The subpoena of Twitter records as well as the decision to keep the subpoena under seal was upheld by the court in the Eastern District of Virginia. *In re:* § 2703(d) Order; 10GJ3793, 787 F. Supp. 2d 430 (E.D. Va. 2011).

Due to increased political pressure and the fear of arrest following the arrest of Pfc. Bradley Manning, Assange cancelled his scheduled public appearances in the United States. *See* Declan McCullagh, *Feds Look for Wikileaks Founder at NYC Hacker Event*, CNET (July 16, 2010, 10:05 PM), http://news.cnet.com/8301-1009_3-20010861-83.html. Assange was scheduled to give the keynote address at the Hackers on Planet Earth ("HOPE") conference in New York City on July 16, 2010, but with the presence of Homeland Security agents at the event, conference attendees were warned Assange might remain abroad. *Id.* Assange is also under investigation for rape by Swedish authorities. These charges were initially alleged on August 20, 2010, and a warrant was then issued for Assange's arrest, but the warrant was dropped within twenty-four hours. David Batty, *Rape Warrant Against Wikileaks Founder Julian Assange Cancelled*, GUARDIAN.CO.UK (Aug. 21, 2010, 8:20 EDT), http://www.guardian.co.uk/media/2010/aug/21/julian-assange-wikileaks-arrest-warrant-sweden. Less

federal prosecutors have subpoenaed Twitter to obtain Appelbaum's records.[5] On November 28, 2010, WikiLeaks released over 250,000 confidential State Department cables.[6] These cables formed a secret history of U.S. diplomatic relations.[7] The State Department responded that it strongly opposed the leaks.[8] On October 22, 2010, WikiLeaks released the largest cache of classified military documents in U.S. history. The 391,832 reports ("The Iraq War Logs") documented numerous aspects of the Iraq War and occupation, including torture and abuse, official death counts, the military's reliance on contractors, details of civilian deaths, and Iran's involvement with Shiite militias in Iraq.[9] Prior to the Iraq War Logs

---

than two weeks later, however, the rape investigation was reopened due to new information. *Sweden Reopens Investigation into Rape Claim Against Julian Assange*, GUARDIAN.CO.UK (Sept. 1, 2010, 18:50 EDT), http://www.guardian.co.uk/media/2010/sep/01/sweden-julian-assange-rape-investigation. Assange contends that the rape charge is a politically-motivated smear campaign instigated by opponents of WikiLeaks. *Id.*

5. Twitter Order, *supra* note 4.

6. *See Secret U.S. Embassy Cables (Cablegate), 1966–2010*, WIKILEAKS (Nov. 28, 2010), http://mirror.wikileaks.info/wiki/Secret_US_Embassy_Cables_%28Cablegate%29,_1966-2010/; *see also State's Secrets*, N.Y. TIMES (Nov. 29, 2010), http://www.nytimes.com/interactive/world/states secrets.html (collecting leaked cables posted by the *New York Times*); *The US Embassy Cables*, GUARDIAN.CO.UK, http://www.guardian.co.uk/world/the-us-embassy-cables (last visited Feb. 29, 2012) (indicating additional leaked cables posted by the *Guardian*). For an overview of the contents of the leaks, see Scott Shane & Andrew W. Lehren, *Leaked Cables Offer a Raw Look Inside U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1, available at http://www.nytimes.com/2010/11/29/ world/29cables.html?_r=1.

7. Among the revelations, the cables revealed a stand-off between the United States and Pakistan over nuclear fuel, talks with South Korea about a unified Korean state, bargaining with other nations to take Guantanamo detainees off the United States' hands, China's global hacking efforts, details of extensive corruption in the Afghan government, and copious off-the-record gossip about world leaders. *See* Shane & Lehren, *supra* note 6.

8. Secretary of State Hillary Clinton called the leaks "an attack on the international community" and promised "that we are taking aggressive steps to hold responsible those who stole this information." Toby Harnden, *WikiLeaks: Hillary Clinton states WikiLeaks Release Is "an Attack,"* THE TELEGRAPH (Nov. 29, 2010), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/816 9040/WikiLeaks-Hillary-Clinton-states-WikiLeaks-release-is-an-attack.html. Meanwhile, Representative Peter King of New York called for WikiLeaks to be designated a "Foreign Terrorist Organization." *Id.* In February 2012, WikiLeaks revealed that the U.S. government had been pursuing a secret indictment against Assange since early 2011. *See Press Release, Stratfor Emails: U.S. Has Issued Secret Indictment Against Julian Assange*, WIKILEAKS (Feb. 28, 2012), http://wikileaks.org/Stratfor-Emails-US-Has-Issued.html.

9. *See The Iraq Archive: The Strands of a War*, N.Y. TIMES, Oct. 23, 2010, at A1, *available at* http://www.nytimes.com/2010/10/23/world/middleeast/23intro.html. The full storehouse of documents can be accessed at the War Logs web site. WARLOGS, http://warlogs.owni.fr (last visited Mar. 4, 2012). Selected documents, organized by subject matter, are available through the *New York Times* website. *Secret Dispatches from the War in Iraq*, N.Y. TIMES, http://www.nytimes.com/interactive/ world/iraq-war-logs.html (last visited Mar. 4, 2012). *See also Iraq: The War Logs*, GUARDIAN.CO.UK, http://www.guardian.co.uk/world/iraq-war-logs (last visited Mar. 4, 2012) (indicating additional leaked military documents posted by the *Guardian*). In light of the information contained in the reports, United Nations Rights Chief Navi Pillay has urged the United States and Iraq to "take necessary measures to investigate all allegations made in these reports and to bring to justice those

leak, WikiLeaks had posted around 90,000 reports relating to the United States's involvement in Afghanistan, which similarly provided details about civilian deaths, high-level corruption in the Afghan government, the fallibility of predator drones, and Pakistan's support of the Taliban.[10]

The Pentagon forcefully condemned the Afghan and Iraq War leaks The Defense Department press secretary Geoff Morrell officially responded, "We deplore WikiLeaks for inducing individuals to break the law, leak classified documents and then cavalierly share that secret information with the world, including our enemies. . . . This security breach could very well get our troops and those they are fighting with killed."[11]

Response from media pundits has been varied. Christian Whiton, a Fox News contributor and former State Department adviser, has called for WikiLeaks and those who help run it to be designated "enemy combatants" and tried for espionage.[12] On the opposite side of the geopolitical equation, Iran has also condemned WikiLeaks, questioning its intentions and vowing to "confront this mischievous act."[13]

Appelbaum, whom *Rolling Stone* magazine dubbed "the most dangerous man in cyberspace,"[14] is the leading developer and advocate of Tor, a free, open-source software that allows users to keep their Internet usage anonymous.[15] Tor is an essential aspect of WikiLeaks' mission, allowing leakers to hide their identities while uploading mass quantities of

---

responsible for unlawful killings, summary executions, torture and other serious human rights abuses." *UN Urges US and Iraq to Probe Wikileaks Torture Claims*, BBC NEWS (Oct. 26, 2010), http://www.bbc.co.uk/news/world-middle-east-11632839. Similarly, Manfred Nowak, the UN's chief investigator of torture, called on the Obama administration to investigate any torture claims that arise out of the Iraq War Logs. Jamie Doward, *Iraq War Logs: Obama Must Investigate Torture Claims, Says UN Envoy*, GUARDIAN.CO.UK (Oct. 23, 2010, 7:51 EDT), http://www.guardian.co.uk/world/2010/oct/23/obama-investigate-war-logs-torture.

10. *Afghan War Diary, 2004–2010*, WIKILEAKS (July 25, 2010), http://mirror.wikileaks.info/wiki/Afghan_War_Diary_2004-2010/. For an overview of the contents of the Afghan War Leaks, *see* Nick Davies & David Leigh, *Afghanistan War Logs: Massive Leak of Secret Files Exposes Truth of Occupation*, GUARDIAN, July 25, 2010, at 1, *available at* http://www.guardian.co.uk/world/2010/jul/25/afghanistan-war-logs-military-leaks.

11. *Iraq War Logs: The Defense Department's Response*, N.Y. TIMES, Oct. 23, 2010, at A9, *available at* http://www.nytimes.com/2010/10/23/world/middleeast/23response.html.

12. Christian Whiton, Op-Ed, *Why Do We Keep Ignoring the WikiLeaks Threat?*, FOXNEWS.COM (Oct. 25, 2010), http://www.foxnews.com/opinion/2010/10/25/christian-whiton-wiki-leaks-ignore-threat-obama-democrats-congress-iraq-war.

13. *Iran Slams 'Mischievous' WikiLeaks*, NEWS24.COM (Oct. 26, 2010, 17:05), http://www.news24.com/World/News/Iran-slams-mischievous-WikiLeaks-20101026.

14. Rich, *supra* note 1.

15. *See Tor: Overview*, TOR PROJECT, http://www.torproject.org/about/overview.html.en (last visited Mar. 4, 2012); *see also* Richard Abbott, *An Onion a Day Keeps the NSA Away*, 13 No. 11 J. INTERNET L. 22, 22 (2010) (explaining Tor and exploring some legal issues related to its operation).

classified documents to WikiLeaks' servers. Because such massive leaks of confidential government documents could expose whistle-blowers to severe penalties, including espionage,[16] these releases would not have been feasible without some means of achieving anonymity.

This Note seeks to provide an overview of the Tor anonymity network and its legal status under several different regimes of Internet control explores its treatment in four countries. Part II discusses Tor generally. Part III explores the treatment of Tor in the countries of the United States, China, Saudi Arabia, and the United Arab Emirates.[17] This discussion offers illuminating case studies on the issues that Tor faces. Part IV analyzes the internet kill switch and U.S. law, including considerations of how other countries monitor the Internet as described in the previous parts. In Part V, the Note concludes.

II. TOR GENERALLY

Tor is not just used to leak highly classified government documents. The Tor software has been downloaded over 36 million times in the last year alone.[18] It has received grants from Google, Human Rights Watch, and even the U.S. military.[19] According to Tor's website, the Tor network

16. The Espionage Act criminalizes the disclosure of classified information "relating to national defense." 18 U.S.C. § 793(d)-(e) (2006). Bradley Manning, the alleged leaker of the "Collateral Murder" video released by WikiLeaks, has been charged under § 793(e) of the Espionage Act. *Army Charges Manning with Leaking Intelligence*, ARMY NEWS SERVICE (Feb. 24, 2012), http://www.defense.gov/news/newsarticle.aspx?id=67319. Additionally, Manning was arraigned on twenty-one other charges, including aiding the enemy in violation of Article 104 of the Uniform Code of Military Justice ("UCMJ"), sixteen charges under Article 134 of the UCMJ, five charges of theft of public property or records in violation of 18 U.S.C. § 641, two charges of fraud and related activity in connection with computers in violation of 18 U.S.C. § 1030(a)(1), and five charges under Article 92 of the UCMJ. *Id.*

Furthermore, WikiLeaks' potential liability under the Espionage Act has also been discussed and remains a contentious issue. *See* Mark Fenster, *Disclosure's Effects: WikiLeaks and Transparency*, 97 IOWA L. REV. 753 (2012); Yochai Benkler, *A Free Irresponsible Press: WikiLeaks and the Battle Over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311 (2011); Molly Thebes, Note, *The Prospect of Extraditing Julian Assange*, 37 N.C. J. INT'L & COM. REG. 889 (2012); Josh Chafetz, *Congress's Constitution*, 160 U. PA. L. REV. 715 (2012).

17. A complete analysis of the legal status of anonymity networks is outside the scope of this Note. Rather, countries have been chosen to provide a broad overview of various approaches to Internet regulation and the legal effect of such regulation on the Tor anonymity network. It is important to note, however, that even in countries in which operating Tor is completely legal, users may encounter legal issues. *See infra* note 41 and accompanying text.

18. Rich, *supra* note 1, at 72.

19. *Id.* at 72. Despite its perceived rebel status, Tor's development was initially sponsored by the U.S. Naval Research Lab., *Tor: Sponsors*, TOR PROJECT, http://www.torproject.org/about/sponsors.html.en (last visited Jan. 16, 2011). Additionally, Tor is currently used by a branch of the Navy in intelligence gathering while deployed in the Middle East. *See Tor: Overview*, *supra* note 15.

has several users: private individuals to protect their online activity; businesses to keep data confidential, research competition, and facilitate internal accountability; journalists to protect anonymous sources and sensitive research; and activists to "report abuses from danger zones."[20] Tor is even employed by law enforcement to surveil web sites without leaving an imprint as well as by a branch of the Navy for open-source intelligence gathering.[21] Despite its reputation as a tool for radicals, dissidents, and criminals, Appelbaum promotes Tor as an essential tool for life in the "Internet Age":

> Tor shouldn't be thought of as subversive. It should be thought of as a necessity. Everyone everywhere should be able to speak and read and form their own beliefs without being monitored. It should get to a point where Tor is not a threat but is relied upon by all levels of society.[22]

Anonymity can also be an extremely important tool for political dissidents living under oppressive regimes. Egypt provides an especially notable recent example. Tor experienced a huge spike in Egyptian users during the Egyptian Revolution of 2011.[23] In the days leading up to the protests on

---

20. *Who Uses Tor?*, TOR PROJECT, https://www.torproject.org/about/torusers.html.en (last visited Mar. 23, 2012). Tor claims that the variety of people who use its network is part of what makes it so secure. *Id.* By creating a disparate body of users, activity cannot be easily localized to one particular area or group of people, thereby maintaining the secrecy of all its users. *See Tor: Overview*, *supra* note 15.

21. *See Tor: Overview*, *supra* note 15. In fact, Tor was originally developed by the Naval Research Lab ("NRL") for use by military field personnel. *Id.* Because a network that only included military personnel would be completely ineffective (since any person using the network would be immediately identified as "military"), NRL released Tor as open-source software. TIM JORDAN, HACKING: DIGITAL MEDIA AND TECHNOLOGICAL DETERMINISM 75 (Polity Press 2008).

22. Rich, *supra* note 1.

23. *Recent Events in Egypt*, TOR PROJECT (Jan. 29, 2011), https://blog.torproject.org/blog/recent-events-egypt. During the 2010—2011 protests in Tunisia, Tor also noted a huge spike in usage within the country after President Zine El Abidine Ben Ali lifted Tunisia's hugely censorious Internet strictures. *Update on Tor Usage in Tunisia*, TOR PROJECT (Jan. 13, 2011), https://blog.torproject.org/blog/update-tor-usage-tunisia. Previously, OpenNet Initiative had reported that Tunisia strongly censors Internet content—including Tor, as well as sites like YouTube and Flickr—while concealing its filtering activities with fake error messages. *Tunisia*, OPENNET INITIATIVE (Aug. 7, 2009), http://opennet.net/research/profiles/tunisia. All Internet providers were required to submit their IP addresses to the government on a regular basis. *10 Worst Countries to be a Blogger*, COMM. TO PROTECT JOURNALISTS (Apr. 30, 2009, 12:01 AM), http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php. Furthermore, a report by the Committee to Protect Journalists identified Tunisia as the seventh worst country in which to be a blogger. *Id.* The report notes that at least two bloggers have been jailed for their work, while others have been the target of surveillance, electronic sabotage, and restrictions on freedom of movement. *Id.*, *see also* Kamel Labidi, *After CPJ Letter, Tunis Grants Journalist Freedom to Travel*, COMM. TO PROTECT JOURNALISTS (Mar. 30, 2009, 5:23 PM ET), http://cpj.org/blog/2009/03/after-cpj-letter-tunis-grants-journalist-freedom-t.php (outlining the harsh

January 25, 2011, during which thousands of people demonstrated against the government in Cairo's Tahrir Square, the number of Egyptians using Tor quadrupled.[24] This increase in usage was particularly significant because, as many media outlets have reported, the Internet was integral in helping organize the protests.[25] Two days later, President Hosni Mubarak completely shut off the access to the Internet for the entire country.[26]

Tor is also appealing to Internet users in free countries who do not wish to expose their activities to the world at large.[27] Additionally, Tor states that its network is used by corporations "to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers."[28] Furthermore, it can be a useful tool for journalists to protect the identities of confidential sources.[29] However, many have also complained that anonymity networks provide a safe haven for criminal activity.[30]

---

treatment of journalist and human rights lawyer Mohamed Abbou); Joel Campagna, *Tunisia Report: The Smiling Oppressor*, COMM. TO PROTECT JOURNALISTS (Sept. 23, 2008, 8:23 PM ET), http://cpj.org/reports/2008/09/tunisia-oppression.php (detailing Tunisia's oppression of dissidents under President Ben Ali's reign).

24. *Directly Connecting Tor Users*, TOR PROJECT, http://metrics.torproject.org/users.html?graph=direct-users&start=2011-01-01&end=2011-02-15&country=eg&dpi=72#direct-users (last visited Feb. 15, 2011); *see also Recent Events in Egypt*, TOR PROJECT, https://blog.torproject.org/blog/recent-events-egypt (last visited Feb. 15, 2011) (noting the spike in Egyptian Tor users and outlining the issues faced by Internet users during the Internet shutdown). According to the *Boston Globe*, Tor received over 120,000 download requests from January 26 to January 29, most of them from Egypt. Farah Stockman, *Foreign Activists Stay Covered Online: Mass. Group's Software Helps Avoid Censorship*, BOSTON GLOBE (Jan. 30, 2011), http://www.boston.com/news/world/africa/articles/2011/01/30/mass_groups_software_helps_avoid_censorship/.

25. *See, e.g.*, Jennifer Preston, *Movement Began with Outrage and a Facebook Page That Gave It an Outlet*, N.Y. TIMES, Feb. 6, 2011, at A10, *available at* http://www.nytimes.com/2011/02/06/world/middleeast/06face.html?scp=7&sq=egypt%20twitter%20facebook%20internet&st=cse.

26. Matt Richtel, *Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts*, N.Y. TIMES, Jan. 29, 2011, at A13, *available at* http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?scp=1&sq=egypt%20cuts%20off%20most%20internet%20and%20cell%20services&st=cse. Some Egyptians were able to continue accessing the Internet through the ISP Noor, which stayed operational for three days after the shut-off, as well as through dial-up connections. Mark Hachman, *Egypt's Last ISP, Noor Group, Vanishes from 'Net*, PCMAG.COM (Jan. 31, 2011, 8:41 PM EST), http://www.pcmag.com/article2/0,2817,2379016,00.asp. When Egypt's Internet access was restored five days after the initial shutdown, the digital free speech think tank Citizen Lab was still encouraging Egyptians to use Tor. *See* Andy Greenberg, *Mubarak's Digital Dilemma: Why Egypt's Internet Controls Failed*, FORBES (Feb. 2, 2011), http://blogs.forbes.com/andygreenberg/2011/02/02/mubaraks-digital-dilemma-why-egypts-internet-controls-failed/.

27. Tor promotes itself as a tool for regular Internet users to prevent being tracked by web sites and to subvert their ISP's content restrictions. *See Tor: Overview*, *supra* note 15.

28. *Id.* Tor also notes that some corporations use its network as a more secure alternative to VPN clients. *Id.*

29. *Id.* Independent Media Center (a.k.a. Indymedia), a global network of independent journalists, recommends that its members use Tor to protect their identities. *Id.* Online News Association, an organization for digital journalists, provides training on its web site for reporters looking to use Tor. Lucas Timmons, *Free Network Helps Keep You, Your Data and Sources Safe*, ONLINE NEWS ASS'N (Mar. 1, 2012), http://journalists.org/2012/03/01/free-network-helps-keep-you-

Tor allows users to send data over the Internet anonymously by shielding the source's location. This is accomplished by a complex encryption network that dissociates Internet communication from its source's IP address. Tor achieves user anonymity through so-called "onion routing,"[31] which bounces all communications routed through the Tor network to various different "nodes" before delivering them to their destination.[32] These "nodes" are proxy servers scattered across the globe. Tor users connect to the network by first pulling in a list of nodes from a directory server.[33] The user's computer then accesses the Tor network through a random node.[34] The user's information is then routed through a random series of relay nodes before finally routing to an exit node, which sends the user's information to the actual Internet.[35] What is significant about the Tor network is that each node communicates only with the nodes immediately preceding and following it in the chain. Therefore, the user's computer has direct contact with only the first node in the chain, and the actual Internet communicates only with the exit node.[36] The entry node does not know the ultimate destination of the data, and the exit node is unaware of the data's origin.[37] Because exit nodes are the only nodes that communicate directly with the public Internet, any traffic routed through

---

your-data-and-sources-safe/.

30. For example, in 2011, efforts by the "hacktivist" group Anonymous brought down Freedom Hosting, a hosting service that hosted over forty child pornography sites. Sean Gallagher, *Anonymous Takes Down Darknet Child Porn Site on Tor Network*, ARS TECHNICA (Oct. 23, 2011), http://arstechnica.com/business/news/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.ars. Anonymous also released the account details of 1,589 users of Lolita City, one of the largest child pornography sites operated on the Tor network. *Id.*

Tor responds to the charge that its network shelters criminals:

> Tor aims to provide protection for ordinary people who want to follow the law. Only criminals have privacy right now, and we need to fix that. Some advocates of anonymity explain that it's just a tradeoff—accepting the bad uses for the good ones—but there's more to it than that. Criminals and other bad people have the motivation to learn how to get good anonymity, and many have the motivation to pay well to achieve it. Being able to steal and reuse the identities of innocent victims (identify [sic]theft) makes it even easier. Normal people, on the other hand, don't have the time or money to spend figuring out how to get privacy online. This is the worst of all possible worlds.

Abuse FAQ, TOR PROJECT, http://www.torproject.org/docs/faq-abuse.html (last visited Jan. 16, 2011).

31. The name "Tor" was originally chosen to stand for "The Onion Router," although the name is no longer an acronym. *See* Abbott, *supra* note 15, at 1.

32. *Tor: Overview*, *supra* note 15; *see also* Abbott, *supra* note 15, at 22–23 (providing additional explanation of Tor's decentralized structure).

33. Abbott, *supra* note 15.

34. *Tor: Overview*, *supra* note 15.

35. Abbott, *supra* note 15.

36. *Id.*

37. *Id.*

the Tor network is traceable only to the exit node.[38] Each communication is encrypted in a new layer of code before passing to the next node.[39] The communication is eventually ensconced in several layers of code, which are then "peeled away" by the exit node, hence the onion metaphor.[40]

Thus, Computer A submits data through the Tor network, the communication will pass through the network and exit onto the actual Internet through the exit node, Computer B. Any data sent by Computer A will appear to anyone tracing the communication as if it has come from Computer B.[41] This essentially allows the user of Computer A to surf the

38. *Id.*

39. *Id.*

40. Tor is not infallible, however. Researchers at the University of Regensburg, Germany, found that a computer on the same network as an exit node—including, potentially, the exit node's ISP—could eavesdrop on the Tor traffic being routed through that node. Dominik Herrmann, Rolf Wendolsky & Hannes Federrath, *Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïves-Bayes Classifier*, CCSW 09: PROCEEDINGS OF THE 2009 ACM WORKSHOP ON CLOUD COMPUTING SECURITY (Nov. 13, 2009), *available at* http://epub.uni-regensburg.de/11919/1/authorsversion-ccsw09.pdf; *see also* John Borland, *Flaws Spotlighted in Tor Anonymity Network*, WIRED (Dec. 27, 2010), http://www.wired.com/threatlevel/2010/12/flaws-spotlighted-in-tor-anonymity-network/ (reporting on the findings of the Regensburg researchers). By capturing packet stream of this traffic and comparing the data with a "fingerprint" database detailing how sites look when accessed through Tor, the eavesdropper could theoretically trace the data back to its source. This method would only work if the eavesdropper has some idea of what sites the target might be visiting. *Id.* Otherwise, it would have no data to build a proper "fingerprint" database. *Id.* Users can effectively circumvent any "fingerprint" eavesdropping by simply sending more than one request at a time, thereby obfuscating the source data.

This flaw in the Tor network was exploited by the "hacktivist" group Anonymous in 2011 when they hacked several child pornography sites operating on the so-called "darknet." Gallagher, *supra* note 30. The "darknet" refers to sites which operate entirely on the Tor network and are visible only to Tor users. *Id.* Such sites are given .onion domain names. *Id.* While the IP addresses of these "darknet" sites are concealed, they have a digital fingerprint that can be used to identify services hosted on a single server and track visits to that site. *Id.* Anonymous targeted a "darknet" hosting service named Freedom Hosting, which hosted over 40 child pornography sites, including Lolita City, which, according to Anonymous, is "one of the largest child pornography websites to date, containing more than 100GB of child pornography." Anonymous took down the hosting service and released account details of 1,589 users. *Id.*

41. This means that users who host exit nodes are taking a risk of being contacted by authorities for any illegal activity conducted through their node. *See* Abbott, *supra* note 15, at 26. A recent incident from Germany illustrates the dangers of hosting an exit node. Germany engages in only very minor regulation of the Internet and virtually no regulation of anonymity networks or proxy servers. However, a recent crackdown on child pornography and terrorism led authorities to seize several computers running Tor nodes. *Tor Madness Reloaded*, ITNOMAD, http://itnomad.wordpress.com/2007/09/16/tor-madness-reloaded (last visited Oct. 31, 2010).

German blogger ITNomad recounts an incident in which his computer was seized by German authorities after a Tor user posted a threat on a German copper forum called copzone.de about his purported plan to plant a bomb in the Department of Work. *Id.* ITNomad recalls that the police searched his house, placed him in handcuffs and took him to the police station for interrogation. *Id.* Realizing that the blogger was merely running a Tor node, all charges were dropped, but due to the event, ITNomad stopped running the node. *Id.* In an earlier incident, German authorities raided seven data centers in search of child pornography trafficking or evidence thereof, seizing a total of ten

Internet with complete anonymity, assuming the user never submits any information that is linked to her identity, such as accessing her standard e-mail account.

Anonymous Internet usage is attractive for a number of different people. As discussed above, anonymity is essential for whistleblowers to reveal classified documents without surrendering their identities. Anonymity is also highly attractive to people living under oppressive regimes.[42] Tor not only allows users to communicate controversial opinions and information without the fear of reprisal, it can also be used to bypass highly restrictive Internet firewalls, such as those employed in China, Saudi Arabia, and the United Arab Emirates.[43] By linking to the Tor network and choosing an exit node in a country that does not restrict Internet usage, users can access sites that are completely blocked in their home countries.[44] But Tor also has a reputation as a safe haven for criminal activity, especially child pornography.[45]

Both the alleged criminality of Tor, and its potential to subvert oppressive regimes, has made it a potential threat to a number of governments around the world. Tor offers users enhanced privacy and the ability to circumvent their own governments' Internet restrictions. Legal treatment of Tor within a country reflects differing attitudes toward the Internet, privacy, and criminal prosecution.

III. SURVEY OF THE TREATMENT OF TOR IN DIFFERENT COUNTRIES

This Note explores the legal status of Tor in four countries—the United States, China, Saudi Arabia, and the United Arab Emirates. These nations were chosen for their diversity of approaches to Internet regulation and, in

servers in the process, some of which were acting as Tor exit nodes. Anders Bylund, *TOR Anonymizing Proxy Servers Seized During German Child Porn Investigation*, ARS TECHNICA (Sept. 11, 2006), http://arstechnica.com/software/news/2006/09/7709.ars. These examples point out many of the challenges facing those who work to facilitate Tor. Running an exit node opens an individual up to involvement with the police. Often, as was the case with ITNomad, the hassle and legal costs of dealing with Tor-related charges and investigations will be enough to convince a facilitator to quit running his node.

42. *See supra* notes 23–26 and *infra* Part III.B–D.

43. *See infra* Part III.B–D.

44. *See Tor: Overview*, *supra* note 15; Abbott, *supra* note 15. In such instances, Tor is essentially being employed as a proxy server. Abbott, *supra* note 15, at n.5.

45. *See supra* notes 30 and 40; Jennifer B. McKim, *Privacy Software, Criminal Use*, BOSTON.COM (Mar. 8, 2012), http://articles.boston.com/2012-03-08/business/31136655_1_law-enforcement-free-speech-technology (discussing various criminal uses of Tor); Ryan Naraine, *Hacker Builds Tracking System to Nab Tor Pedophiles*, ZDNet (Mar. 6, 2007), http://www.zdnet.com/blog/security/hacker-builds-tracking-system-to-nab-tor-pedophiles/114 (discussing a hacker working to track pedophiles on Tor).

the case of the latter three, for the potential lessons they hold for the changing face of Internet law in the United States.

A. United States

Currently, the United States has no laws that specifically restrict Tor. Thus, the Tor network seems to be perfectly legal in the United States.[46] This legality is the opinion of the open-Internet advocacy group Electronic Frontier Foundation: "[W]e believe that running a Tor relay-including an exit relay that allows people to anonymously send and receive traffic-is lawful under U.S. law."[47]

However, there is some question whether Tor users might be subject to the Digital Millennium Copyright Act ("DMCA") for copyright infringement conducted through the Tor Network.[48] Tor operators claim that Tor is protected because it is a transitory network that does nothing more than move traffic around the net, thus falling under the DMCA's "safe harbor" provisions.[49] The question is whether Tor violates

46. If Tor is used to commit illegal acts, then the Tor user is still liable for the underlying acts, but not for his use of Tor.

47. ELECTRONIC FRONTIER FOUNDATION, *The Legal FAQ for Tor Relay Operators*, TOR PROJECT, http://www.torproject.org/eff/tor-legal-faq.html.en (last updated Aug. 24, 2011). This Legal FAQ was authored by the Electronic Frontier Foundation (EFF), a nonprofit activist organization that seeks to promote civil liberties online and open Internet. *See About EFF*, EFF, http://www.eff.org/about (last visited Jan. 16, 2011). EFF advocates on behalf of Tor, encouraging people to run Tor relay nodes. *See The EFF Tor Challenge*, EFF, https://www.eff.org/torchallenge (last visited Mar. 27, 2011).

48. Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2860 (1998) (codified as amended throughout multiple sections of 17 U.S.C.).

49. Digital Millennium Copyright Act, 17 U.S.C. § 512 (2010). Often, users who run exit nodes will receive notifications regarding copyright infringement. *See Five Years as an Exit Node Operator*, TOR PROJECT (Nov. 11, 2008), https://blog.torproject.org/blog/five-years-exit-node-operator. DMCA complaints are so common that Tor provides a boilerplate response, authored by EFF, on its website for exit node operators who are contacted by their Internet service providers. Electronic Frontier Foundation, *Response Template for Tor Relay Operator to ISP*, TOR PROJECT (May 31, 2011), https://www.torproject.org/eff/tor-dmca-response.html. Under § 512(a), the first of four safe harbor provisions in the DMCA, "transitory digital network communications" are immune from money damages for copyright infringement claims when the following five conditions are met:

> (1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
>
> (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
>
> (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
>
> (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or

"§ 512(i)'s mandate that all such networks not interfere with 'standard technical measures,' which § 512(i)(2) describes as 'technical measures that are used by copyright owners to identify or protect copyrighted works.'"[50] Because the DMCA was not intended to cover and did not anticipate anonymity networks like Tor, it seems unlikely that a court would apply its provisions to Tor.[51] Furthermore, one might question whether an exit node facilitator could face liability for child pornography charges. There would seem to be liability under 18 U.S.C. § 2252 if someone knowingly facilitated the downloading of child pornography,[52] but the whole point of Tor is that exit-node facilitators do not know what is being routed through their computers.[53]

---

network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

§ 512(a). Additionally, to be eligible for any of the safe harbors, a service provider must have "reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers . . . ." § 512(i)(1)(A); *see also* RIAA v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003) (holding that the DMCA prohibited copyright owners from issuing subpoenas to ISPs which do not store infringing material on their servers but rather act merely as "conduits" for Internet traffic); RIAA v. Charter Comm., 393 F.3d 771 (8th Cir. 2005) (affirming the judgment of the D.C. Circuit). As for what constitutes a reasonable policy, EFF claims that any policy which terminates subscribers for repeat infringement should be sufficient. *See* EFF, *supra* note 47. EFF claims not only that the ISP falls under the "conduit" safe harbor but that a Tor node facilitator does as well. *Id.* This latter contention may be more difficult to sustain. While node facilitators are somewhat analogous to ISPs in that they merely act as a passageway through which outside Internet traffic is routed, individual node facilitators lack the ability to terminate Tor users who employ their node for copyright infringement. Thus, it is possible that they lack the ability to formulate a reasonable policy that would qualify it for the "conduit" safe harbor provision.

50. *See* Abbott, *supra* note 15, at 25 (quoting 17 U.S.C. § 512(i)(2)).

51. *See id.* at 25–26.

52. 18 U.S.C. § 2252 (2010). Particularly relevant is § 2252(a)(4)(B), which creates culpability for any person who:

[K]nowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.

§ 2252(a)(4)(B).

53. Prosecution under § 2252 for possession of child pornography requires knowledge of the images. *See* Lori J. Parker, Annotation, *Validity, Construction, and Application of Federal Enactments*

Threats of laws more specific to Tor loom in the United States. Significantly, President Obama has proposed measures that would inhibit Internet privacy, including anonymity networks like Tor. According to the *New York Times*, "[e]ssentially, officials want Congress to require all services that enable communications—including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype—to be technically capable of complying if served with a wiretap order."[54] Currently, these formats are very difficult for the government to monitor.[55] While there is not yet any draft of potential statutory language, one of the government's primary goals appears to ensuring government access to all peer-to-peer communication, regardless of whether it is conducted over a landline-telephone, cellphone, BlackBerry, Voice Over Internet Provider (VoIP),[56] or other means.[57]

B. China

At the opposite end of the Tor-regulation spectrum from the United States, China's regulation of the Internet is notoriously stringent and broad-ranging.[58] China's regulation is primarily accomplished through

---

Proscribing Obscenity and Child Pornography or Access Thereto on the Internet, 7 A.L.R. Fed. 2d 1, IV.A (2005). Thus, a Tor node facilitator who does not realize that someone is using his or her node to download illegal materials would not be liable. *See supra* note 41 and accompanying text. But if the authorities discover that illegal materials are being downloaded through the user's computer, the user will likely face significant challenges. *Id.*

54. Charlie Savage, *U.S. Is Working to Ease Wiretaps on the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=1&_r=1&hp; Charlie Savage, *Officials Push to Bolster Law on Wiretapping*, N.Y. TIMES, Oct. 19, 2010, at A1, *available at* http://www.nytimes.com/2010/10/19/us/19wiretap.html?src=twrhp. The Internet "kill switch" was eventually dropped from the Senate's bi-partisan 2012 cyber security bill. *See* Scott J. Shackleford, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 STAN. L. REV. ONLINE 106, 108 (2012), http://www.stanfordlawreview.org/sites/default/files/ online/articles/64-SLRO-106.pdf.

55. *Id.* Indeed, as it is currently structured, Tor has no way of monitoring traffic through its network. *See Abuse FAQ*, *supra* note 30. Unlike an ISP, which routes all subscribers' Internet traffic through centralized servers, which allow for Internet activity to be easily traced back to its source, Tor is decentralized by design. *Id.* While it might be technically possible for Tor to design a backdoor through which to monitor traffic, doing so would significantly weaken the network by creating a vulnerable point which hackers could target. *Id.*

56. VoIP is a general term for any technology that allows communication through an Internet provider, including popular services such as Skype. *See* Glenn Greenwald, *The Obama Administration's War on Privacy*, SALON (Sept. 27, 2010, 5:28 AM CST), http://www.salon.com/news/opinion/glenn_greenwald/2010/09/27/privacy/index.html.

57. *See* Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, *supra* note 54.

58. China also has the largest number of Internet users in the world, with 298 million Internet users, an increase of 42% from 2007 to the end of 2008. CHINA INTERNET NETWORK INFORMATION

extensive filtering of content.[59] Tor is illegal under Revised Provisional Regulations Governing the Management of Chinese Computer Information Networks Connected to International Networks, which reads, "[c]omputer information networks conducting direct international networking shall use the international access channels provided by the national public telecommunications networks of the Ministry of Posts and Telecommunications. No units or individuals shall set up by themselves or use other access channels for international networking."[60] Thus, people in China can only legally access the Internet by going through the government's public channels, which heavily censor content according to eleven proscribed content categories.[61] This system of Internet control is often referred to as the "Great Firewall of China."[62] China's regulation of the Internet thus seeks to create an absolute bottleneck for all traffic to international sites.[63]

CENTER, THE TWENTY-THIRD STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA 3 (2009), http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf. More astoundingly, in this same time period over 90% of these users had broadband access, a spike of over 100 million. *Id*. at 14.

59. China bans eleven types of content, for which it is illegal either to produce or disseminate. These are:

> (1) violating the basic principles as they are confirmed in the Constitution; (2) jeopardizing the security of the nation, divulging state secrets, subverting of the national regime or jeopardizing the integrity of the nation's unity; (3) harming the honor or the interests of the nation; (4) inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples; (5) disrupting national policies on religion, propagating evil cults and feudal superstitions; (6) spreading rumors, disturbing social order, or disrupting social stability; (7) spreading obscenity, pornography, gambling, violence, terror, or abetting the commission of a crime; (8) insulting or defaming third parties, infringing on the legal rights and interests of third parties; (9) inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order; (10) conducting activities in the name of an illegal civil organization; and (11) any other content prohibited by law or rules.

Provisions of the Administration of Internet News Information Services (promulgated by the State Council Information Office and the Ministry of Information Industry, Sept. 25, 2006), art. 19, *translated in Human Rights and Rule of Law—News and Analysis*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA (June 6, 2006), http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

60. Revised Provisional Regulations Governing the Management of Chinese Computer Information Networks Connected to International Networks (originally promulgated on February 1, 1996 by State Council Decree No. 195 and revised by the State Council on May 20, 1997), art. 6, *translated in Codes & Statutes—Computer and Internet Law*, EASTLAW.NET, http://www.eastlaw.net/service/datacnlaw/code/computer/no195.htm (last visited May 12, 2012).

61. *See* Provisions on the Administration of Internet News Information Services, *supra* note 59, art. 19.

62. *See* ANGELA ROMANO, *Asia*, *in* PUBLIC SENTINEL: NEWS MEDIA & GOVERNANCE REFORM, 353, 360 (Pippa Norris ed., 2010). China's national firewall is officially known as the Golden Shield Project. According to Romano, the Great Firewall is "arguably . . . the best-honed system for monitoring and censoring the Internet to restrict dissidence and suppress alternative views." *Id.* at 360.

63. *Id.* China has received extensive international criticism for its rigorous censorship of Internet

Tor frustrates this objective by allowing users to bypass the Great Firewall entirely by routing their traffic through exit nodes located outside of the country.[64] Tor would allow, for example, users to connect to the unfiltered version of google.com, rather than its heavily filtered counterpart, google.cn.

In 2009, China blocked access to all Tor entrance nodes by simply blocking the IP addresses affiliated with these nodes through its Great Firewall.[65] These efforts blocked about eighty percent of Tor's entrance relays.[66] Tor has attempted to circumvent these IP blocks by providing bridge nodes.[67] Unlike the normal entrance relays, bridge nodes are kept confidential, so their IP addresses cannot be blocked by Chinese authorities.[68] According to Tor:

> Right now, China is the main place in the world that filters connections to the Tor network. So bridges are useful a) for users in China, b) as a backup measure in case the Tor network gets blocked in more places, and c) for people who want an extra layer of security because they're worried somebody will recognize that it's a public Tor relay IP address they're contacting.[69]

---

content. *Id.* In particular, the International Olympic Committee lodged complaints, prompting China to promise unfettered Internet access to journalists covering the 2008 Beijing Olympics. *Id.* However, while China did allow access to previously blocked sites such as BBC.com, China actually increased barriers to web content on certain topics, including the Tibetan uprisings. *Id.*

64. Used in such a way, Tor is basically acting as a proxy server. Chinese officials attempt to block proxy servers. *See China*, OPENNET INITIATIVE (June 15, 2009), http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf ("[T]he major exceptions to the focus on [filtering] politically sensitive topics specific to China in 2008 were circumvention tools and pornography. A portion, though not a majority, of proxy tools and anonymizers in both the Chinese . . . and English languages . . . was blocked. The circumvention tool Psiphon is also blocked, along with the Citizen Lab at the University of Toronto and the Information Warfare Monitor, sister institutions engaging in research on circumvention and surveillance."). Use of proxy servers is banned under Revised Provisional Regulations Governing the Management of Chinese Computer Information Networks Connected to International Networks. *See* discussion, *supra* note 59.

65. David Talbot, *China Cracks Down on Tor Anonymity Network*, TECH. REV. (Oct. 15, 2009), http://www.technologyreview.com/web/23736.

66. *Tor Partially Blocked in China*, TOR PROJECT (Sept. 27, 2009), https://blog.torproject.org/blog/tor-partially-blocked-china.

67. *Id.* According to Abbott, *supra* note 15, bridge nodes have been very successful in providing Chinese users access to Tor. Tor's data bears this out. *See China Blocking Tor: Round Two*, TOR PROJECT (Mar. 11, 2011), https://blog.torproject.org/blog/china-blocking-tor-round-two. In March, 2010, China improved its method of blocking Tor, making access to public nodes virtually impossible. *Id.* However, most Tor users in the country were able to switch to non-public bridge nodes. *Id.* In turn, China's Great Firewall started to block some of the most popular bridge nodes. *Id.*

68. While it is generally true that bridge nodes cannot be blocked by the Great Firewall, the most popular ones are sometimes discovered by Chinese officials and can then be blocked. *Id.*

69. *Tor FAQ: Should I Be a Normal or a Bridge Relay?*, TOR PROJECT, https://www.torproject

So far, China has dealt with Tor by blocking access to entrance node IP addresses,[70] but if users continue to circumvent this bulwark by linking up with the Tor network through bridge nodes, China could feel the need to take more proactive measures. Targeting exit node facilitators would be impossible because, due to China's extensive Internet restrictions, exit node facilitators are unlikely to exist within the country.[71] Instead, because China has the power and self-granted authority to remotely access all individuals' computers and monitor their activity,[72] a more effective strategy would be to prosecute people simply for running Tor software on their computers.

Unlike the United States, China has ensured the legal means to very well eliminate the use of Tor within the country.

C. Saudi Arabia

Saudi Arabia, like China, routes all Internet traffic through its national network.[73] Saudi Arabia also filters some sites, especially those with "immoral" content, such as pornography, gambling, and religious

---

.org/docs/faq.html.en#RelayOrBridge (last visited Mar. 28, 2012).

70. *See Tor Partially Blocked in China*, *supra* note 66.

71. *See* Kent, *View Tor Nodes in Google Earth*, CYBER SECURITY & PROFOUND SUBMERSION (Oct. 4, 2010), https://b.kentbackman.com/2010/10/04/view-tor-exit-nodes-in-google-earth/ (finding no exit nodes operating in mainland China).

72. Article 14 authorizes Chinese officials to obtain full access to any sensitive information they wish: "Providers of internet information services and internet access providers shall maintain these records for 60 days, and shall make them available to all relevant government agencies examining them pursuant to law." State Council Order No. 292 (adopted at the 31st Executive Meeting of the State Council on September 20, 2000; promulgated by Decree No. 292 of the State Council of the People's Republic of China as of September 25, 2000), art. 14, *translation in Measures for Managing Internet Information Services*, CHINA CULTURE, http://www1.chinaculture.org/library/2008-02/06/content_23369.htm (last visited May 12, 2012). Finally, Article 15 defines what information must be restricted:

> IIS providers shall not produce, reproduce, release, or disseminate information that . . . endangers national security, . . . is detrimental to the honor and interests of the state, . . . undermines social stability, . . . undermines the state's policy towards religions, . . . other information prohibited by the law or administrative regulations.

Id. art. 15.

73. *See Internet Filtering in Saudi Arabia in 2004*, OPENNET INITIATIVE, http://opennet.net/studies/saudi#toc1a (last visited Mar. 4, 2012). "Since its creation in 1998, the state-run Saudi Telecom Company (STC) had been the sole provider of telecom services. However, in an effort to join the World Trade Organization (WTO), the government opened the telecommunication sector to competition in 2002." *Id.*; *see also Saudi Arabia's Telecom Sector Growing Rapidly*, KHALEEJ TIMES ONLINE (Mar. 24, 2008), http://www.khaleejtimes.com/DisplayArticleNew.asp?xfile=data/business/2008/March/business_March715.xml&section=business&col (reporting that Saudi Arabia's telecom revenues are growing at an average annual rate of 15%).

conversion.[74] The Saudi government also focuses its Internet regulation heavily on quashing dissent, prohibiting the publication or accessing of "anything contrary to the state or its system."[75] According to OpenNet Initiative, Saudi Arabia has also extensively filtered sites that provide tools to circumvent its national network, including Tor.[76] While Saudi Arabia's ban on anonymity networks is partially intended to give teeth to its censorship efforts, the government has also made clear that it is interested in surveillance.[77] Saudi Arabia's interest in surveillance seems to be fundamentally linked to the religious and anti-dissident agenda of its Internet censorship.[78]

---

74. *Introduction to Content Filtering*, INTERNET SERVICES UNIT, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm (last visited Mar. 4, 2012).

75. The Saudi government bans nine content categories, for which publication and access is prohibited. These are:

> (1) Anything contravening a fundamental principle or legislation, or infringing the sanctity of Islam and its benevolent Shari'ah, or breaching public decency; (2) Anything contrary to the state or its system; (3) Reports or news damaging to the Saudi Arabian armed forces, without the approval of the competent authorities; (4) Publication of official state laws, agreements or statements before they are officially made public, unless approved by the competent authorities; (5) Anything damaging to the dignity of heads of states or heads of credited diplomatic missions in the Kingdom, or harms relations with those countries; (6) Any false information ascribed to state officials or those of private or public domestic institutions and bodies, liable to cause them or their offices harm, or damage their integrity; (7) The propagation of subversive ideas or the disruption of public order or disputes among citizens; (8) Anything liable to promote or incite crime, or advocate violence against others in any shape or form; and (9) Any slanderous or libelous [sic] material against individuals.

Arab Media: Saudi Internet Rules, COUNCIL OF MINISTERS RESOLUTION (Feb. 12, 2001), http://www.al-bab.com/media/docs/saudi.htm.

76. *See Internet Filtering in Saudi Arabia*, *supra* note 73. Such measures to block anonymity networks are especially injurious in Saudi Arabia, which has actively pursued bloggers who speak out against the Saudi government. In 2008, clerics called for harsh punishment, including flogging for bloggers who advocated for reform of the Saudi government and death for owners of TV stations that air what is perceived as immoral material. Kamel Labidi, *Saudi Prince Threatens Sports Commentators*, COMM. TO PROTECT JOURNALISTS (Jan. 27, 2009), http://cpj.org/blog/2009/01/saudi-prince-threatens-sports-commentators.php. The Saudi government also imprisoned blogger Fouad al-Farhan without charge for several months in 2007 and 2008 for promoting reform and the release of political prisoners. *See* Katherine Zoepf, *Saudis Confirm Detention of Blogger of Social Issues*, N.Y. TIMES, Jan. 2, 2008, at A4, *available at* http://www.nytimes.com/2008/01/02/world/middleeast/02saudi.html?ei=5065&en=bf9af2ff6de9aeb0&ex=1199854800&partner=MYWAY&pagewanted=print. Such activities have led the Committee to Protect Journalists to name Saudi Arabia the fifth worst country in which to be a blogger. *10 Worst Countries to be a Blogger*, COMM. TO PROTECT JOURNALISTS (Apr. 30, 2009), http://www.cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php.

77. Pursuant to this goal, Saudi Arabia not only monitors Internet traffic, it monitors the activity of patrons at physical Internet cafés as well. Helmi Noman, *Restriction on Internet Use in the Middle East on the Rise: Internet Cafés in Saudi Must Install Hidden Cameras*, OPENNET INITIATIVE (Apr. 16, 2009), http://opennet.net/blog/2009/04/restriction-Internet-use-middle-east-rise-Internet-caf%C3%A9s-saudi-must-install-hidden-came. In March 2009, the Ministry of Internet ordered Internet cafés to install hidden cameras and provide a record of names and identities of their customers. *Id.*

78. *Internet Filtering in Saudi Arabia*, *supra* note 73.

The Tor site is blocked in Saudi Arabia; however, circumvention appears to be relatively common in the country.[79] Accordingly, usage of Tor in Saudi Arabia has been steadily increasing since late 2009.[80]

D. United Arab Emirates

The United Arab Emirates has a more moderate yet still restrictive approach. The United Arab Emirates leads the Middle East in adoption of information and communication technology.[81] Internet use has skyrocketed in the past decade.[82] The Internet is regulated in the U.A.E. by the Telecommunications Regulatory Authority ("TRA").[83] The TRA is responsible for producing the Internet Access Management ("IAM") policy, which outlines prohibited online content categories for ISPs.

The content categories prohibited include Internet tools for bypassing blocked content.[84] This block, of course, applies to Tor as well as any

79. *See Directly Connecting Tor Users*, TOR METRICS, https://metrics.torproject.org/users.html?graph=direct-users&start=2009-01-01&end=2011-01-18&country=sa#direct-users (last visited Mar. 4, 2012) (showing that Saudi Arabia has the tenth highest number of directly connecting Tor users in the world).

80. Direct connections have increased from around 1000 in late 2009 to over 4000 in early 2011. *See, e.g.*, *Directly Connecting Tor Users*, TOR METRICS, https://metrics.torproject.org/users.html?graph=direct-users&start=2009-01-01&end=2011-01-18&country=sa#direct-users (last visited Mar. 4, 2012).

81. *See* Tom Gara, *UAE Leads Region in IT, Says Report*, THE NATIONAL (Apr. 16, 2009), http://www.thenational.ae/article/20090416/BUSINESS/448045865/-1/ART.

82. *Internet Users (Per 100 People)*, WORLD BANK, http://data.worldbank.org/indicator/IT.NET.USER.P2 (last visited Apr. 3, 2012) (showing Internet usage has risen from 23.6% in 2000 to 78% in 2011). Furthermore, over 40% of Internet users in the United Arab Emirates are female, the highest proportion of female users in the Gulf Cooperation Council. *See* Neeraj Gangal, *UAE Has Most Female Internet Users in GCC*, ITP.NET (Sept. 25, 2009), http://www.itp.net/573940-uae-has-most-female-internet-users-in-gcc.

83. *See Internet Filtering in the United Arab Emirates in 2004–2005: A Country Study*, OPENNET INITIATIVE, http://opennet.net/studies/uae (last visited Mar. 4, 2012).

84. *Id*. Other categories of regulated content include: content for learning criminal skills and illegal drugs; content containing pornography and nudity; gambling sites; sites for hacking and malicious codes; content offensive to religions, phishing Internet sites; Internet content that downloads spyware; web sites providing unlicensed voice over Internet protocol ("VoIP") service; terrorism content; and prohibited top level domain, apparently a reference to the top level domain of Israel (.il), which is blocked in the UAE. *Id*. Until recently, VoIP was completely banned in the United Arab Emirates, and Skype, one of the most popular worldwide VoIP providers, is still banned. *See UAE Legalises VoIP, But Skype Still Banned*, EXPATS IN KUWAIT (Mar. 15, 2010), http://www.expatsinkuwait.com/news/86-it/1619--uae-legalises-voip-but-skype-still-banned .html. In a similar move, the United Arab Emirates came very close to banning BlackBerry services within its borders. Barry Meier & Robert F. Worth, *Emirates to Cut Data Services of BlackBerry*, N.Y. TIMES, Aug. 2, 2010, at A1, *available at* http://www.nytimes.com/2010/08/02/business/global/02 berry.html?scp=2&sq=uae%20blackberry&st=cse. This plan was scrapped only days before the ban was set to go into effect, although it was unclear if Research In Motion, the manufacturer of BlackBerry, had made any concessions to bring the phone in-line with the U.A.E. Internet regulations. Bettina Wassener, *United*

software that allows an Internet user in the United Arab Emirates to access banned content by linking to a proxy server located in another country.[85] Accordingly, the Tor site is blocked, as are all sites that provide a list of proxy servers.[86]

The United Arab Emirates' objective in banning anonymity networks is twofold. First, anonymity networks allow users to access blocked content, such as pornography and sites detailing how to conduct criminal activity. Second, anonymity networks also allow Internet users to evade government monitoring.

The United Arab Emirates openly engages in Internet monitoring.[87] The Dubai police force engages an around-the-clock policing unit to monitor Internet activity.[88] This unit, known as the "e-police," investigated 222 crimes in 2008.[89] The United Arab Emirates has thus developed an

---

Arab Emirates Drops BlackBerry Threat, N.Y. TIMES, Oct. 9, 2010, at B2, *available at* http://www.nytimes.com/2010/10/09/technology/09blackberry.html?scp=4&sq=uae%20blackberry&st=cse. Greenwald and Jardin both noted that the United Arab Emirate's reasons for banning some VoIP providers is similar to the Obama administration's rationale for requesting backdoor entry into VoIP and BlackBerries in the United States. *See* Greenwald, *supra* note 56; Xeni Jardin, *Obama Administration Wants Encryption Backdoors for Domestic Surveillance*, BOING BOING (Sept. 27, 2010, 11:53 AM), http://www.boingboing.net/2010/09/27/obama-administration.html.

85. *Internet Filtering in the United Arab Emirates*, *supra* note 83. For a differing approach, consider Thailand. Although Thailand engages in some Internet censorship, the government does not ban the use of circumvention tools altogether. *See* Computer Crime Act, B.E. 2550, art. 5-8 (2007), unofficial translation available at http://www.prachatai.com/english/node/117 (outlawing access to a computer system or data which is protected by a specific access prevention measure, but not specifically banning the use of proxies). According to Information and Communications Technology ("ICT") Minister Sitthichai Pookaiyaudom, "I don't think the intent of the law is to prosecute anonymous proxy use. If you use proxies to access legal sites, then it is fine. If you use proxies to access bad sites, then that is illegal. Whether you use proxies or not is beside the point." Don Sambandaraksa, *Setting the Record Straight*, BANGKOK POST (May 30, 2007), http://www.bangkokpost.com/opinion/opinion/246430/setting-the-record-straight. Despite the ICT Minister's statement that proxies are legal, many circumvention tools are targeted by Thailand's official filtering. *Thailand*, OPENNET INITIATIVE (May 9, 2007), http://opennet.net/research/profiles/thailand. However, filtering circumvention tools appears to be a lower priority than other targets, such as pornography. *Id.*

86. It is unclear whether the United Arab Emirates bans specific IP addresses or just the Tor website.

87. *See Internet Filtering in the United Arab Emirates*, *supra* note 83. "The authorities have established committees and electronic surveillance departments to monitor objectionable Internet activities." *Id.*

88. Andy Sambidge, *Dubai's e-Police Probe 222 Internet Crime Cases*, ARABIAN BUSINESS (Oct. 30, 2008), http://www.arabianbusiness.com/dubai-s-e-police-probe-222-Internet-crime-cases-83845.html.

89. *Id.* The e-police prosecuted eighty-seven cases involving fraud and financial crimes, thirty-eight illegal hacking cases, and ninety-two cases of defamation and extortion. *Id.* Internet monitoring also allowed the government to track down individuals offering cheap, illegal VoIP services from their apartments. *Id.* Thus, the government has used its monitoring capabilities in order to prosecute cases of individuals selling services that are illegal because they evade monitoring.

Internet regime that not only seeks to eliminate certain types of content but also enhances the government's ability to surveil its citizens.

IV. INTERNET KILL SWITCH AND U.S. LAW

If the United States increases regulations of Tor, similar to China, Saudi Arabia, and the United Arab Emirates, and enacts the "internet kill switch," might those users who run exit nodes be liable for illegal activity that is routed through their node? Recall that for anyone investigating this illegal activity, the communication will appear as if it had come directly from the exit node's IP address. The IP addresses of exit nodes are publicly available.[90] Meaning, if a user employs Tor to download illegal child pornography, this action will look like it came from the exit node's IP address and authorities could easily trace it to the owner of the exit node.[91] There has not yet been a case dealing with the legality of running a Tor exit node.[92] However, some Tor exit node facilitators have received DMCA notices from their ISPs, universities, and similar organizations.[93] Tor and the Electronic Frontier Foundation strongly contend that such users have no legal liability for such activity.[94] In fact, pursuant to this belief, EFF itself runs an exit relay node.[95]

If the new provisions have the effect of banning anonymity networks that completely hide the user's identity, then this could effectively outlaw Tor. However, because exit and entrance nodes are located all around the globe, it would be essentially impossible to completely shut down Tor.[96]

---

90. *See* Abbott, *supra* note 15, at 27.

91. *See id.* at 24 (explaining Tor's operations under the section titled "Circuit Building").

92. *See* Electronic Frontier Foundation, *Legal FAQ*, *supra* note 47.

93. *Id.*

94. *Id.* EFF notes that no one has yet been sued for running a Tor node. *Id.* However, EFF also makes no promise that Tor node facilitators cannot be held legally accountable:

> All new technologies create legal uncertainties, and Tor is no exception. Presently, no court has ever considered any case involving the Tor technology, and we therefore cannot guarantee that you will never face any legal liability as a result of running a Tor relay.

Id.

95. *Id.* ("EFF believes so strongly that those running Tor relays shouldn't be liable for traffic that passes through the relay that we're running our own middle relay.").

96. Due to the decentralized nature of Tor, a total shutdown could be achieved only by disabling each individual node. *See generally Tor: Overview*, *supra* note 15 (explaining Tor's decentralized networking architecture); Abbott, *supra* note 15 (same). Even then, new nodes could start running Tor and thus rehabilitate the network. *Tor: Overview*, *supra* note 15 (explaining Tor's decentralized networking architecture); Abbott, *supra* note 15 (same).

On the other hand, if the United States does not want to explicitly ban anonymity networks, it could instead provide a back-door entrance for government surveillance of nearly all other online communication services, including VoIP, BlackBerry, and peer-to-peer networks. Such surveillance would almost certainly have the effect of driving criminal activity to anonymity networks, which would only make them more controversial. At that point the U.S. government might consider adopting measures similar to Saudi Arabia's and China's, which block access to the Tor site and most likely create liability for exit node facilitators. Such a move could be extremely detrimental to online privacy and might even raise some Fourth Amendment issues.[97]

The United States' goal to ensuring government access to all peer-to-peer communication could also have major implications for Tor. According to some commentators, including Glenn Greenwald of Salon and Xeni Jardin of Boing Boing, the goal of these proposed provisions is to provide government access to any and all online communication.[98] Greenwald, Jardin, and others have also noted that adoption of such provisions would essentially copy the more invasive Internet regulation laws found in the United Arab Emirates and Saudi Arabia,[99] both of which are classified as practicing "substantial filtering" of political websites, according to OpenNet Initiative.[100] Tor states that it has not yet been asked to create backdoor access into the Tor network.[101] Tor has vowed that if it is mandated to provide a backdoor for government surveillance, it will

97. *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) (providing a theoretical framework for application of the Fourth Amendment to the Internet, arguing in favor of (1) a distinction between content and non-content information and (2) mandatory search warrants for protected Internet communication); Mike McNerney, *Warshak: A Test Case for the Intersection of Law Enforcement and Cyber Security*, 2010 U. ILL. J.L. TECH. & POL'Y 345 (2010) (calling for updated laws and judicial norms to protect privacy on the Internet); Laura J. Tyson, Comment, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257 (2010) (arguing against the rigid application of the third-party doctrine to Internet cases); Eric R. Diez, Comment, *"One Click, You're Guilty": A Troubling Precedent for Internet Child Pornography and the Fourth Amendment*, 55 CATH. U. L. REV. 759 (2006) (discussing the role of child pornography cases in the erosion of online 4th Amendment rights); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (identifying "digital dossiers"—companies' online collections of users' personal information—as a major Fourth Amendment concern).

98. Greenwald, *supra* note 56 ("[T]he U.S. Government is taking exactly the position of the UAE and the Saudis: no communications are permitted to be beyond the surveillance reach of U.S. authorities."); Jardin, *supra* note 84.

99. Greenwald, *supra* note 56; Jardin, *supra* note 84.

100. *See Internet Filtering in Saudi Arabia*, *supra* note 73.

101. *Tor FAQ: Is There a Backdoor in Tor?*, TOR PROJECT, https://www.torproject.org/docs/faq#Backdoor (last visited Mar. 4, 2012).

refuse to do so.[102] Tor also claims that it has received legal advice that a request for a back-door entrance is unlikely and, if such a request were made, it could be successfully challenged in U.S. courts.[103]

V. CONCLUSION

The question remains, what lessons can be drawn from the global treatment of anonymity networks? Anonymity networks are not targeted without reason. Anonymity networks are challenged and dealt with only when they conflict with the larger objectives of a nation's Internet regulation regime. China's robust and broad-ranging Internet policy regards any and all attempts to evade its centralized control of the Internet as an affront. Thus, anonymity networks are targeted because they allow users to evade the centralized firewall. The United Arab Emirates sees its role in Internet regulation in a somewhat more limited way. Its primary objectives are to (1) filter immoral, illegal, and prurient content; and (2) facilitate government surveillance of its citizens. Anonymity networks frustrate both of these goals, so their usage is banned. Saudi Arabia filters content for both moral reasons and to prevent anti-government dissent; however, unlike the United Arab Emirates, its surveillance efforts are fairly primitive, and correspondingly, Tor is widely used within the country.

The government surveillance objective of the United Arab Emirates is especially instructive for the United States. While the United States filters very little content on the Web, it has shown an increasing interest in the ability to monitor Internet communications. Insofar as anonymity networks frustrate this goal, they may run into increasing pressure from the federal government. The United States currently stands at something of a crossroads in terms of its control over the Internet. More and more, anonymity networks seem to be bumping up against the United States' interest in law enforcement, prevention of terrorist attacks, and stopping leaks of classified documents. While Tor makes claims that its network does not actually promote bad activity,[104] it is important to note that

102. *Id.*

103. *Id.* The source of, and basis for, this legal advice is unclear. Tor merely attributes the advice to "some smart lawyers." This opinion most likely comes from the Electronic Frontier Foundation ("EFF"), which has authored a Legal FAQ on Tor and which itself hosts a Tor node. *See* Electronic Frontier Foundation, *Legal FAQ*, *supra* note 47.

104. *See Tor: Overview*, *supra* note 15.

massive leaks of classified government documents would be virtually unfeasible without some kind of anonymity network.[105]

As more and more communication is conducted online, law enforcement and intelligence gathering authorities will find it increasingly useful to access online communications. It seems unlikely that the United States would ban anonymity networks outright, and such a move would raise major right-to-privacy concerns.[106] However, just as all telephone landlines can be tapped,[107] it is quite possible that the United States will seek to require anonymity networks to provide a backdoor entrance to these communications.[108] While such a move would be less intrusive than the United Arab Emirates' total ban on proxy servers, the rationale behind such a move is largely the same, that no communication should be unattainable by the government. In terms of liability for using Tor, it would be more likely for the United States to move toward allowing usage of anonymity networks but creating independent liability for the use of Tor to commit illegal acts.[109]

Requiring a backdoor into anonymity networks like Tor would be a significant infringement on individual privacy, which is completely unwarranted. To take this approach would be to essentially mirror the repressive tactics of the United Arab Emirates and Saudi Arabia. Furthermore, adopting regulations which would inhibit the privacy of anonymity networks would deprive journalists, corporations, whistleblowers, and non-governmental organizations of a powerful tool. There is also value in Tor for the average Internet user who does not wish to have his or her every move tracked by various websites. While it is

105. It is impractical to physically transport hundreds of thousands of classified documents. If leakers are going to reveal secret documents, they are only going to do so via some kind of secure private Internet connection to protect themselves.

106. *See* discussion *supra* note 97.

107. Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1021 (1994). Specifically, § 103 requires phone companies to ensure that all of its phone lines are able to be "expeditiously" tapped. 47 U.S.C. § 1002.

108. CALEA has been expanded by the FCC to include mobile phones and VoIP. 47 C.F.R. § 1.20000–1.20008 (2010). For further discussion of this rule, see Communications Assistance for Law Enforcement Act, 69 Fed. Reg. 56956 (FCC Sept. 23, 2004) (proposed rule).

109. Perhaps more relevant on a local level in the United States is the German example, in which ignorance of Tor on the part of law enforcement creates difficulties for those who would help facilitate the Tor network. *See supra* note 40 and accompanying text. The fear of persecution and the hassles of dealing with law enforcement (or one's ISP) will often be enough to dissuade many from assisting the Tor network.

undeniable that Tor provides some level of shielding for those who wish to carry out illegal activity, that is not in itself a reason to deny privacy for others.

Keith D. Watson[*]

---

* J.D. (2012), Washington University in St. Louis School of Law; B.A. (2008), Truman State University. The author would like to thank the staff of the *Global Studies Law Review* for their helpful edits. The author is particularly grateful to Julia Walcott and Anna Erwin, both of whom have provided invaluable assistance on this Note.