Copyright 2012 by Northwestern University School of Law
Northwestern University Law Review
Printed in U.S.A.
Vol. 106, No. 2

Notes and Comments

DMCA § 512 SAFE HARBOR FOR ANONYMITY NETWORKS AMID A CYBER-DEMOCRATIC STORM: LESSONS FROM THE 2009 IRANIAN UPRISING

Nassim Nazemi

ABSTRACT—In 2009, the world watched as Iranians took the online services that many have come to regard as tools of procrastination—services like Twitter, Facebook, and YouTube—and transformed them into tools of cyber-democratization. When the Iranian government banned foreign journalists, citizens disseminated cell phone footage of peaceful protests and the government's brutal response, keeping the world informed. But news did not escape Iran's borders unaided. Liberation technology, particularly the popular anonymity network "Tor," helped Iranian protesters bypass government censorship while remaining undetected. Today, the U.S.-based volunteers who comprise a significant segment of Tor's operator network face an uncertain legal landscape because Tor can facilitate copyright infringement. I foresee that Tor operators will soon find themselves defendants in copyright infringement actions arising from file-sharing activity, likely in connection with the BitTorrent protocol. The typical plaintiff's strategy of subpoenaing Internet service providers to identify users based on Internet Protocol address can mistakenly identify Tor operators who, because of the nature of this technology, will appear to be the sources of any infringing activity passing through their virtual tunnels. Using the Iranian uprising as case study, I argue that Tor operators should be shielded from secondary infringement liability so that they can continue to facilitate speech in censored nations, thereby improving U.S. access to world news and nurturing democratic habits abroad. Specifically, volunteer anonymity network operators should enjoy protection under the Digital Millennium Copyright Act (DMCA) § 512(a), a provision allowing safe harbor for transitory digital network communication providers.

AUTHOR—J.D. Northwestern University School of Law, 2012; M.A., The Chicago School of Professional Psychology, 2007; B.A., Northwestern University, 2000. I must thank Professor Jason DeSanto, for his wise and witty counsel; Corey McCaffrey, for his invaluable help; my fellow board members, for their thoughtful edits; Farid Kossari, for inspiring this work; Negin Nazemi, for blazing this trail; and my parents, for believing in me.

INTRODUCTION

In the summer of 2009, the world watched as Iranians took the online services that some of us have come to regard as tools of procrastination—services like Twitter, Facebook, and YouTube—and turned them into tools of cyber-democratization. The grassroots effort that came to be known as Iran's "Green Movement"[1] materialized from a flurry of tweets, status updates, and online videos. And when the Iranian government banned foreign journalists, ordinary citizens disseminated grainy cell phone footage of peaceful street protests and the government's brutal response, filling the void and keeping the world informed.[2] Iconic images like the blank and bloodied face of Neda Agha-Soltan captivated U.S. audiences and turned

[1] The Green Movement has its roots in Iranian presidential candidate Mir Hossein Mousavi's "green wave" campaign. *See* Hooman Majd, *Think Again: Iran's Green Movement*, FOREIGN POL'Y (Jan. 6, 2010), http://www.foreignpolicy.com/articles/2010/01/06/think_again_irans_green_movement. When Mousavi lost the bid in what most observers considered a rigged election favoring incumbent Mahmoud Ahmadinejad, the campaign transformed into an election protest. *Id.* Today, the Green Movement is increasingly viewed as an Iranian civil rights movement. *See, e.g.*, Hamid Dabashi, *Iran's Younger, Smarter Revolution*, DAILY BEAST (Jan. 2, 2010, 1:37 PM), http://www.thedailybeast.com/blogs-and-stories/2010-01-02/irans-younger-smarter-revolution/full ("For the last six months and since Day One of this uprising . . . I have consistently called and continue to call it a *civil-rights movement*."); Majd, *supra* ("With every instance of recent government tyranny, from show trials of opposition politicians and journalists to the beatings and murders of some demonstrators on Iran's streets, the movement has grown more steadfast in its demands for the rights of the people.").

[2] *See, e.g.*, Jessica Reed, *Updated: Citizen Journalism Round-up*, GUARDIAN (June 15, 2009, 10:00 AM), http://www.guardian.co.uk/commentisfree/2009/jun/15/iran-election-protests-blogs.

legions of casual observers into activists.[3]

Separated by oceans, continents, and a language barrier, these newly minted activists seized on technology to bridge the gap. Liberation technology[4]—specifically, tools allowing censorship bypass[5] and user anonymity—delivered a sort of twenty-first-century Underground Railroad. One tool in particular, an anonymity network called Tor,[6] quickly emerged as a powerful ally to Persian Samizdat, helping Iranian protesters bypass government censors while remaining safely anonymous.[7] Tor allowed Iran's cyber-dissidents to voice their unmistakable demands for freedom and to share with the outside world their firsthand accounts of the government's brutal response—all without revealing their online identities.

Today, the U.S.-based volunteers that comprise a significant segment of Tor's operator network[8] face an uncertain legal landscape[9] because Tor is

---

[3] *See* Monica Hesse, *Facebook's Easy Virtue*, WASH. POST, July 2, 2009, at C1 (noting that social media activism surged following Neda's death but suggesting that many of these activists may lack the commitment necessary to effect tangible change); Jessica Ravitz, *Neda: Latest Iconic Image to Inspire*, CNN WORLD (June 24, 2009), http://articles.cnn.com/2009-06-24/world/neda.iconic.images_1_neda-agha-soltan-tiananmen-square-iran.

[4] Larry Diamond defines "liberation technology" as "any form of information and communication technology . . . that can expand political social, and economic freedom." Larry Diamond, *Liberation Technology*, J. DEMOCRACY, July 2010, at 69, 70. He includes in this definition things like computers, the Internet, and social networking websites. *Id.* To his list, I add censorship-bypass tools and anonymizers.

[5] As used in this Comment, the term "bypass" indicates software and online services that enable Internet users to circumvent online censorship. Although "circumvention" is the term more often employed in information-technology circles, I avoid it in an effort to minimize confusion with "circumvention" as a legal term of art in the copyright context. *See, e.g.*, Digital Millennium Copyright Act, Pub. L. No. 105-304, § 103, 112 Stat. 2860, 2863 (1998) (codified at 17 U.S.C. § 1201 (2006)) (creating liability for "[c]ircumvention of copyright protection systems").

[6] Tor describes itself as "free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis." *Anonymity Online*, TOR PROJECT, https://www.torproject.org (last visited July 2, 2012).

[7] Although this Comment focuses on the role of anonymity networks in enabling Iran's protesters-turned-journalists to disseminate information to a world audience without fear of government reprisal, a separate benefit of anonymity lies beyond its scope: the role of anonymity in helping foreign activists organize and disseminate information *among themselves*. This latter benefit was never realized in Iran, where the news-disseminating power of social networking instead backfired against activists and exposed them to the Iranian regime. *See* Evgeny Morozov, *Iran: Downside to the "Twitter Revolution,"* DISSENT, Fall 2009, at 10, 12 ("[B]oth Twitter and Facebook give Iran's secret services superb platforms for gathering open source intelligence about the future revolutionaries, revealing how they are connected to each other. . . . Once regimes used torture to get this kind of data; now it's freely available on Facebook.").

[8] Most Tor operators are located in the United States and Germany. Damon McCoy et al., *Shining Light in Dark Places: Understanding the Tor Network*, *in* PRIVACY ENHANCING TECHNOLOGIES 63, 64 (Nikita Borisov & Ian Goldberg eds., 2008). Tor's architecture is such that its volunteer-run network could remain operational even after a complete shutdown of The Tor Project, Inc., the entity that presently funds and develops Tor software. This Comment's inquiry is therefore cabined to the potential liability of Tor's volunteer operators rather than that of The Tor Project.

amenable to both legal and illegal usage. As countersurveillance expert Richard Abbott has observed, "[m]any dismiss [Tor] as a den of thieves and pedophiles" while "[o]thers describe it as a beacon of democracy able to free the individual from oppression."[10] This Comment ponders the "den of thieves" allegation and considers one particular form of theft, copyright infringement. I argue that Tor *operators*—individuals who donate computer resource and bandwidth to make the Tor network possible—should not be held secondarily liable for the infringing activities of Tor *users*—individuals who send Internet traffic through the Tor network in an effort to mask their online identities and bypass government censorship of the Internet.[11]

Because the Digital Millennium Copyright Act (DMCA)[12] was not drafted with Tor in mind and because no anonymity network operator has yet faced secondary liability in a copyright infringement action, it is unclear whether Tor's volunteer operators will be exempt from liability under DMCA § 512(a), a provision giving safe harbor to transitory digital network communication providers.[13] And even though a global network like Tor could theoretically continue to function without any U.S.-based operators, the specter of infringement liability for these Tor operators is troubling because, at a minimum, it discourages the largest population of uncensored Internet users from volunteering as anonymity network operators.[14]

---

[9] Christopher Riley, *The Need for Software Innovation Policy*, 5 J. TELECOMM. & HIGH TECH. L. 589, 607 (2007) ("The legal status of Tor is far from clear.").

[10] Richard Abbott, *An Onion a Day Keeps the NSA Away*, J. INTERNET L., May 2010, at 22, 22.

[11] Tor is a volunteer-run network of computers that form a series of virtual tunnels through which Internet users can send and receive data anonymously. *Tor: Overview*, TOR PROJECT, http://www.torproject.org/about/overview.html.en (last visited July 2, 2012). This Comment uses the term "operator" to refer to an individual who installs Tor software on her computer for the benefit of others. The individual becomes one "stop" along the virtual Tor tunnel, encrypting data transmissions and handing them off to the next operator for further encryption—a process that anonymizes data and allows it to bypass any government-imposed censoring of the Internet. *See id.* (using the technical term "relay" instead of "operator"). By contrast, a "user" is an individual who installs Tor software for personal benefit: an Iranian blogger who seeks anonymity from prying government eyes; a Chinese college student who wants to get around the "Great Firewall of China"—a government censorship scheme that blocks access to websites like Facebook and Google; an American who is worried about identity theft. *See What Is a Tor Relay?* ELEC. FRONTIER FOUND., http://www.eff.org/torchallenge/what-is-tor (last visited July 2, 2012); *Inception*, TOR PROJECT, http://www.torproject.org/about/torusers.html.en (last visited July 2, 2011). The distinction between Tor operators and users is explored in further detail *infra* Part I.C.

[12] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C. (2006)).

[13] For further discussion of DMCA § 512(a), see *infra* Part III.

[14] The CIA reports that, as of 2008, the United States was second only to China in the number of Internet users. *The World Factbook—Country Comparison :: Internet Users*, CIA, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html (last visited July 2, 2012).

Recent litigation suggests that, in the near future, Tor operators may find themselves defendants in copyright infringement suits arising from illegal file-sharing activity. The year 2010 saw the opening salvos of massive copyright litigation involving the popular file-sharing protocol BitTorrent.[15] In a move reminiscent of the recording industry's unpopular onslaught against individual file sharers in the early 2000s, independent filmmakers began pursuing tens of thousands of BitTorrent users who allegedly shared copies of films like *The Hurt Locker*.[16] The filmmakers' strategy involved subpoenaing Internet service providers (ISPs) to identify users based on Internet Protocol (IP) addresses.[17] Although ISP delay tactics ultimately forced the filmmakers to voluntarily dismiss 90% of their defendants, more than 2300 unnamed defendants remain in the suit,[18] and the *Hurt Locker* litigation is but one of many mass copyright infringement actions against alleged BitTorrent users.[19] It seems inevitable that,

[15] BitTorrent is an Internet communication protocol that allows individuals to share large files quickly and easily. *What Is BitTorrent and Why Are Its Users Being Sued?*, THE TELEGRAPH (May 24, 2011, 2:21 PM), http://www.telegraph.co.uk/technology/8533353/What-is-BitTorrent-and-why-are-its-users-being-sued.html. Several BitTorrent-based file-sharing programs exist, including the popular "µTorrent" and "Vuze" (formerly called "Azureus"). *See Results for "File Sharing,"* CNET.COM, http://download.cnet.com/1770-2196_4-0.html?query=file+sharing&searchtype=downloads (last visited July 2, 2012). Two features distinguish BitTorrent from other file-sharing protocols: (1) BitTorrent breaks large files (like movies) into "chunks" for faster downloading and (2) it connects users directly to each other (rather than to a centralized server). *See What Is BitTorrent and Why Are Its Users Being Sued?*, *supra*. The absence of a centralized server is of legal import as copyright holders seeking legal redress for alleged infringement must bring separate suits against each individual file sharer—there is no Napster- or LimeWire-esque corporate middleman to sue. *See id.*

[16] *See* Voltage Pictures, LLC v. Does 1–5,000, 818 F. Supp. 2d 28, 45 (D.D.C. 2011) (denying a motion brought by putative defendants seeking to quash plaintiff's subpoenas issued to their ISPs, denying putative defendants' request for a protective order, and denying their motion to dismiss for improper joinder or want of personal jurisdiction); Eriq Gardner, *"Hurt Locker" Lawsuit Target [sic] Pirates*, REUTERS (May 11, 2010, 9:40 PM), http://www.reuters.com/article/2010/05/12/us-hurtlocker-idUSTRE64B0AU20100512 (explaining that the plaintiff in these lawsuits, U.S. Copyright Group, had previously filed approximately ten other suits alleging piracy of other films).

[17] *See Voltage Pictures*, 818 F. Supp. 2d at 30–31. An "IP address" is a unique number, assigned by an ISP, identifying an Internet-connected computer. Although IP addresses alone do not contain personally identifiable information, ISPs are able to link them to customer accounts to provide claimants with the necessary identification. *See Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RTS. CLEARINGHOUSE, http://www.privacyrights.org/fs/fs18-cyb.htm (last updated July 2, 2012). IP addresses can, however, convey meaningful information about a user's geographic location—a phenomenon called "geolocation." *See, e.g.*, Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALBANY L.J. SCI. & TECH. 61, 67–68 (2011) (describing how IP address data can reveal a user's location within a thirty-mile radius).

[18] *See* enigmax, *Record-Breaking BitTorrent Lawsuit Decimated*, TORRENTFREAK (Sept. 30, 2011), http://www.torrentfreak.com/90-of-defendants-dismissed-from-record-breaking-bittorrent-lawsuit-110930.

[19] *See, e.g.*, Patrick Collins, Inc. v. John Does 1–23, No. 11–cv–15231, 2012 WL 1019034, at *1 (E.D. Mich. Mar. 26, 2012) ("This case is one among many cases filed nationwide by copyright owners alleging that John Doe defendants downloaded their films without authorization using a peer-to-peer

eventually, some of the IP addresses subpoenaed in these BitTorrent lawsuits will identify innocent Tor operators who, because of the nature of this anonymity technology, will erroneously appear to be the sources of any infringing activity that passes through their virtual tunnels.

This Comment focuses on the threat of infringement litigation faced by Tor operators. Nevertheless, conclusions reached here should also extend to operators of other decentralized, volunteer-run online networks that primarily function as tools for bypassing censorship and anonymizing online activity. Tor is not unique, but it is the "most public and widespread anonymity network."[20] Indeed, a recent Harvard study analyzing bypass-tool usage in Iran, China, and other countries with substantial government censorship of the Internet found Tor to be one of the most popular tools as measured by unique monthly users.[21] And because Tor technology has broad implications across such diverse areas as law enforcement, online privacy, and net neutrality,[22] the legal status of its operator network is all the more worthy of examination.[23]

Using the Iranian uprising of 2009 as a case study, this Comment argues that Tor operators should be shielded from secondary infringement liability so that they can continue to facilitate speech in heavily censored nations. In doing so, Tor operators can improve U.S. access to world news and nurture the development of democratic habits abroad. Part I describes how Iranian citizen journalists and the global online community worked in tandem to smuggle news out of Iran amid a mainstream media blackout and despite the Iranian regime's best iron-fisted efforts to stifle what it viewed as dissent. These events did not go unnoticed in the United States, and Part

('P2P') file sharing network known as BitTorrent." (footnote omitted)); *see also* houstonlawy3r, *What to Do About These Smaller Doe Bittorrent Cases?*, FED. COMPUTER CRIMES (Aug. 26, 2011), https://torrentlawyer.wordpress.com/2011/08/26/small-doe-bittorrent-cases-in-home-state ("The bittorrent cases are speeding up, both in number of cases filed, and in the issues relating to the cases.").

[20] Abbott, *supra* note 10, at 26.

[21] *See* HAL ROBERTS ET AL., HARV. U. BERKMAN CTR. FOR INTERNET & SOC'Y, 2010 CIRCUMVENTION TOOL USAGE REPORT 9 (2010), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

[22] "Net neutrality" (short for "network neutrality") is a network design principle rooted in the assumption that public information networks are maximally useful when they are content-agnostic. *See Network Neutrality FAQ*, TIMWU.ORG, http://www.timwu.org/network_neutrality.html (last visited July 2, 2012). In other words, the social and economic utility of a network (like the Internet) increases as network accessibility increases, allowing all types of digital interactions to flow freely. *Id.* Professor Tim Wu draws a helpful analogy to electrical grids: the grid is an implicitly neutral network because it "does not care if you plug in a toaster, an iron, or a computer"; this neutrality has allowed the grid to "survive[] and support[] giant waves of innovation in the appliance market." *Id.* Proponents of Internet neutrality argue for similar open-access regulations while critics maintain that open access will "slow the pace of broadband deployment." Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141, 141 (2003).

[23] Abbott, *supra* note 10, at 22 ("[A]n understanding of Tor will affect every Internet discussion you will ever have. Learn to use Tor effectively and you will find yourself . . . chuckling as the naïve and uninitiated debate net neutrality, wiretapping, packet inspection, and other such anachronisms.").

I further explores key U.S. legislative and executive reactions to Iran's so-called "Twitter Revolution."[24] Finally, Part I discusses the role of anonymity network Tor during the Iranian uprising and explains how this technology is amenable to both infringing and noninfringing uses.

Part II paints a picture of Tor litigation as it is likely to emerge—in the context of illegal file sharing made untraceable by the union of Tor and BitTorrent. This Part describes potential theories of liability, concluding that (absent safe harbor immunity) a theory of contributory infringement is the likeliest to prevail against a Tor operator whose service allegedly facilitates copyright infringement.

Part III addresses statutory safe harbor under the DMCA, arguing that Tor operators, like many Internet service providers, should enjoy § 512(a) safe harbor protection from monetary liability in a copyright infringement action. Tor operators meet § 512's general conditions of eligibility and specifically qualify for immunity under § 512(a) as mere conduits of digital communication. Part III explains how this statutory defense, which failed file-sharing defendants like Napster, can prevail for Tor operators.

The statutory safe harbor shields defendants from monetary liability only and would leave Tor operators vulnerable to injunctive action following a finding of copyright infringement.[25] Anticipating the balancing of interests that would confront a court in deciding whether to grant such equitable relief, Part IV argues that the likely harm to a Tor operator's First Amendment interests militates against the use of injunctive remedies. By allowing speakers to disseminate news free from persecution, the operator exercises a protected right to receive information, and this speech-facilitating conduct is itself a form of speech warranting protection.

I. BACKGROUND

Internet freedom abroad is deeply entwined with U.S. foreign policy objectives ranging from human rights and freedom of expression to broader goals of democratization.[26] But the Internet and its "vast democratic forums"[27] remain quite vulnerable to censorship and perversion by

[24] Early mainstream media reports were quick to credit the micro-blogging service Twitter with fueling prodemocratic unrest in Iran. With hindsight, observers have come to view this characterization of Twitter's role as hyperbolic. *See, e.g.*, Morozov, *supra* note 7, at 10 (describing the U.S.-media-constructed narrative of events in Iran as "Iran's Twitter Revolution"); *infra* note 48 and accompanying text (discussing the debate, largely initiated by Malcolm Gladwell, over the role of social networking in Iran's 2009 uprising).

[25] *See infra* note 154 and accompanying text.

[26] *See Internet Freedom*, U.S. DEP'T ST., http://www.state.gov/e/eb/cip/netfreedom (last visited July 2, 2012) (reconfirming the State Department's commitment to "defense of a free, open, and interconnected Internet as a U.S. foreign policy priority").

[27] Reno v. ACLU, 521 U.S. 844, 868 (1997) (striking down a portion of the Communications Decency Act of 1996 on First Amendment overbreadth grounds).

oppressive governments. States like China,[28] Saudi Arabia,[29] and Iran[30] have long used the Internet to stifle dissent. And more recently in 2011, popular uprisings across the Arab world have set the region ablaze and brought the interplay of digital communication and democratization into sharp public focus.[31] In these places, blogging—arguably the apotheosis of free speech in the digital age—is often met with a gauntlet of online censorship, government surveillance, and licensing schemes[32] designed to silence dissent. Through the lens of Iran's 2009 uprising, this Part explores the problem of Internet censorship in Iran, key U.S. legislative and executive

[28] For example, in 2005, Chinese users of Microsoft's MSN Spaces blogging service learned that the company had bowed to their government's censorship scheme by blocking blog titles that used terms like "freedom" and "democracy." JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? 95 (2006). Goldsmith and Wu point to China as an example of "what a government that really wants to control Internet communications can accomplish." *Id.* at 89. For a discussion of Chinese censorship and circumvention efforts, see Jennifer Shyu, Comment, *Speak No Evil: Circumventing Chinese Censorship*, 45 SAN DIEGO L. REV. 211, 225–29, 240–43 (2008).

[29] The Saudi censorship machine is extensive but less aggressive than China's. GOLDSMITH & WU, *supra* note 28, at 74. The Saudi government-owned Internet infrastructure can filter and block all web traffic flowing into the Kingdom. *Id.* According to a 2004 OpenNet Initiative report, some of the most aggressively blocked websites were those providing "information about tools to circumvent the government's filtering, and sites that promote[d] religious dialogue between Muslims and Christians." *Id.*

[30] Iran is discussed *infra* Part I.A.

[31] For example, the Egyptian government took the radical step of shutting down all Internet service following mass anti-Mubarak protests in January 2011. *See* David Kravets, *Egypt's Last-Standing ISP Goes Dark*, WIRED (Jan. 31, 2011, 6:55 PM), http://www.wired.com/threatlevel/2011/01/egypt-isp-shuttered. When service was restored, the global online community mobilized to help Egyptian protesters safely reconnect to the outside world through Tor. *See, e.g.*, phobos, *Protecting Your Internet Traffic in Volatile Times*, TOR BLOG (Feb. 2, 2011), https://blog.torproject.org/blog/protecting-your-internet-traffic-volatile-times (encouraging readers to "join the Tor network to help others" remain anonymous and expressing concern over the possibility that Egyptian Internet traffic "is being recorded and possibly saved for future use"); Susannah Vila, *5 Things You Can Do to Support Egyptians from Anywhere*, MOVEMENTS.ORG (Jan. 28, 2011), http://www.movements.org/blog/entry/egypt-what-can-you-do (encouraging readers to help Egyptians browse the Internet anonymously by running a Tor relay). Recognizing the role of social networking in securing Mubarak's eventual ouster, one grateful Egyptian man went so far as to name his daughter "Facebook." *See* David Murphy, *Egyptian Man Names Daughter 'Facebook,'* PCMAG.COM (Feb. 20, 2011, 10:37 PM), http://www.pcmag.com/article2/0,2817,2380670,00.asp.

[32] For a discussion of the proposed Saudi licensing scheme, see Alexia Tsotsis, *Saudi Arabians Will Soon Need a License to Blog*, TECHCRUNCH (Sept. 23, 2010), http://www.techcrunch.com/2010/09/23/saudi-arabians-will-soon-need-a-license-to-blog ("[A]ll Saudi Arabian web publishers and online media, including blogs and forums, will need to be officially registered with the government."). Saudi bloggers already face ill-defined ex post criminal liability for posting content that violates social or religious "values." *See, e.g.*, *Blogger Fouad al Farhan Freed After More than Four Months in Prison*, REPORTERS SANS FRONTIÈRES (Apr. 28, 2008), http://en.rsf.org/IMG/article_PDF/saudi-arabia-blogger-fouad-al-farhan-freed-28-04-2008,26746.pdf ("[B]logger Fouad al Farhan . . . had been held in prison since 10 December 2007[] for posting an article on his blog discussing the 'advantages' and 'disadvantages' of being a Muslim."). For a comprehensive report on Internet censorship and surveillance in Saudi Arabia, see ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 561–570 (Ronald Diebert el al. eds., 2010).

reactions to this problem, and the salutary role played by the anonymity network Tor.

A. Iran: The Middle East's Largest Prison for Journalists and Netizens[33]

"Control has no meaning on the Internet . . . . It would crash like the Berlin Wall."

–Shaban Shahidi Moadab, Deputy Press Minister,
Iranian Ministry of Culture and Islamic Guidance[34]

Sadly for the Iranian civil rights movement, it is Mr. Shahidi Moadab's prophecy—not control over the Internet—that has "crashed." The Islamic Republic of Iran boasts one of the world's most comprehensive and sophisticated Internet censorship machines.[35] Theirs is an attempted panoptic use of the Internet, designed to induce self-censorship.[36]

Iran routes all web traffic through a government-run Internet backbone, allowing the regime to target and block content relating to human rights, women's rights, political reform, government criticism, religious minorities, criticism of Islam, sexuality, and a broad range of topics it considers immoral.[37] Iran's Press Law[38] further restricts speech through a licensing

---

[33] REPORTERS SANS FRONTIÈRES, WORLD DAY AGAINST CYBER CENSORSHIP 20 (2010), http://en.rsf.org/IMG/pdf/Internet_enemies.pdf ("With some sixty journalists and bloggers behind bars and another fifty forced to seek asylum elsewhere, the Islamic Republic of Iran has become the largest prison in the Middle East—and one of the world's largest prisons—for journalists and netizens."). Merriam-Webster defines "netizen" as "an active participant in the online community of the Internet." *Netizen*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/netizen (last visited July 2, 2011).

[34] Mr. Shahidi Moadab was quoted in Nazila Fathi, *Taboo Surfing: Click Here for Iran . . .*, N.Y. TIMES, Aug. 4, 2002, at C5 (internal quotation marks omitted). There, the author mistakenly identified the speaker as "Shaaban Sahidi." *See id.*

[35] DIEBERT ET AL., *supra* note 32, at 555.

[36] For a discussion of the Foucauldian reinterpretation of Bentham's Panopticon in the context of government surveillance and censorship in Iran and China, see Cameron J. Shahab & Reza Mousoli, *Cat and Mouse in Cyberspace: A Case Study of China vs Iran*, IRANIAN.COM (Sept. 10, 2010), http://www.iranian.com/main/2010/sep/cat-and-mouse-cyberspace. Michel Foucault, who visited Iran during the height of the 1978 anti-Shah protests, was highly critical of the Shah's secret police and their surveillance tactics. *See* JANET AFARY & KEVIN B. ANDERSON, FOUCAULT AND THE IRANIAN REVOLUTION 2 (2005); Shahab & Mousoli, *supra*.

[37] DIEBERT ET AL., *supra* note 32, at 553–55. The Iranian regime is also working on its very own, "clean" version of the Internet—"an insular nationwide intranet that is reportedly isolated from the regular Internet" and that "would be heavily regulated by the government." Ryan Paul, *Iran Moving Ahead with Plans for National Intranet*, ARS TECHNICA (Apr. 9, 2012, 10:10 PM), http://arstechnica.com/tech-policy/news/2012/04/iran-plans-to-unplug-the-internet-launch-its-own-clean-alternative.ars.

[38] QANUNI MATBU'AT [PRESS LAW] Tehran 1381 [2002], arts. 1, 6 (Iran) (defining "press" as including "[a]ll electronic publications" and explaining that "[t]he [p]ress is free, except for items which undermine Islam's bases and commandments, and public and private rights"), *translated in Iran Data Portal—Press Law*, PRINCETON UNIV., http://www.princeton.edu/irandataportal/legislation/press-law

scheme that puts bloggers and website operators under government regulatory authority.[39] Unlicensed speakers face criminal prosecution and punishment for speech-based crimes ranging from imprisonment to death.[40] Such harsh consequences create a very real need for anonymity technology to shield bloggers' IP addresses and hence their identities.[41]

Perhaps as a testament to its fractured leadership, the run-up to Iran's hotly disputed June 2009 presidential election saw a surge in online censorship targeting prominent political figures including former President Mohammad Khatami[42] and presidential candidate Mir Hossein Mousavi.[43] In the election aftermath, amid street demonstrations and widespread allegations of vote-rigging, the Iranian censors launched an undeclared war on social networking.[44] With the foreign press almost entirely banned from reporting on the election fallout,[45] the task of documenting this historic clash fell to Iran's citizen journalists.[46] Their contraband—uncensored

(last updated Aug. 3, 2011).

[39] DIEBERT ET AL., *supra* note 32, at 550; *see also* Article 19, *Memorandum on Media Regulation in the Islamic Republic of Iran* 8–9, UNHCR REFWORLD (May 2, 2006), http://www.unhcr.org/refworld/docid/475e4e270.html (discussing the Iranian licensing scheme and characterizing it as both a "matter of serious concern" and "a violation of the right to freedom of expression"). For a discussion of regulatory restrictions faced by Middle Eastern bloggers, see Mohamed Abdel Dayem, *Middle East Bloggers: The Street Leads Online*, COMMITTEE TO PROTECT JOURNALISTS (Oct. 14, 2009), http://www.cpj.org/reports/2009/10/middle-east-bloggers-the-street-leads-online.php.

[40] Punishable offenses include insulting Islam and criticizing state officials. DIEBERT ET AL., *supra* note 32, at 550; *see also* TA'AZIRAT [PENAL CODE] Tehran 1991, arts. 513–514, 609 (Iran), *available at* http://mehr.org/Islamic_Penal_Code_of_Iran.pdf (last visited July 2, 2010) (criminalizing speech that insults, *inter alia*, "the Islamic sanctities or any of the *imams*," the Prophet Muhammad, or "the leaders of the three branches of the government").

[41] Ethan Zuckerman, a researcher at Harvard University's Berkman Center for Internet and Society, has developed a guide for anonymous blogging that combines Tor, the blogging platform WordPress, and the use of free email accounts to produce a "very high level of anonymity." Ethan Zuckerman, *Anonymous Blogging with Wordpress & Tor*, GLOBAL VOICES ONLINE (Sept. 4, 2009, 6:03 PM), http://advocacy.globalvoicesonline.org/projects/guide.

[42] For example, Iran began blocking access to Khatami's website yarinews.org in February 2009. DIEBERT ET AL., *supra* note 32, at 553.

[43] *See id.* (explaining that "[m]any believe that supporters of President Mahmoud Ahmadinejad were behind the blocking orders" targeting Facebook, as opposition candidate "Mousavi[] had been using Facebook for political organizing").

[44] *See* REPORTERS SANS FRONTIÈRES, *supra* note 33, at 19 ("Iran's regime considers social networks to be instruments of the opposition. Facebook and Twitter, which relayed the calls for demonstrations, have been continuously blocked since June 2009. MySpace.com and Orkut.com have received the same treatment.").

[45] *Chaos Prevails as Protesters, Police Clash in Iranian Capital*, CNN.COM (June 21, 2009, 4:37AM), http://edition.cnn.com/2009/WORLD/meast/06/20/iran.election/index.html [hereinafter *Chaos Prevails*] ("The Ministry of Culture on Saturday banned international media from reporting on the demonstrations unless they receive permission from Iranian authorities. A freelance journalist said it was 'very dangerous' to take pictures.").

[46] A message on losing presidential candidate Mousavi's Facebook page, posted during the height of the June 2009 postelection protests, captured this sentiment: "Today you are the media . . . . It is your duty to report and keep the hope alive." *Id.* (internal quotation marks omitted).

accounts of peaceful street protests and a brutal government response—found its way to U.S. consumers thanks (in part) to cell phone technology, YouTube, and the volunteer efforts of world netizens who posted, retweeted, and shared news with the wired community.[47] And although the significance of social networking in aiding communication and activism *within* Iran is in dispute,[48] there can be little doubt that these tools played a crucial role in getting unfiltered news *out of* Iran.[49] Citizen journalism would be of little use without an effective news dissemination mechanism, and effective dissemination is precisely what the online community delivered. Netizens ensured that when the Iranian government killed peaceful protester Neda Agha-Soltan[50] in cold blood and in broad daylight, the YouTube-connected world was watching.[51]

To the Iranian government, these amateur videographers and other citizen journalists were dissidents, and their methods of news dissemination

---

[47] Former deputy national security adviser Mark Pfeifle went so far as to suggest that Twitter might deserve a Nobel Peace Prize for having "uniquely documented and personalized the story of hope, heroism, and horror in Iran." Mark Pfeifle, *A Nobel Peace Prize for Twitter?*, CHRISTIAN SCI. MONITOR, July 6, 2009, at 22, 22.

[48] Malcolm Gladwell is perhaps the most vocal critic of the idea that social networking can effect real social change. Regarding the role of Twitter in Iran's post-election uprising, he observed that "the people tweeting about the demonstrations were almost all in the West." Malcolm Gladwell, *Small Change: Why the Revolution Will Not Be Tweeted*, NEW YORKER, Oct. 4, 2010, at 42, 44. For Twitter co-founder Biz Stone's response to Gladwell, see Biz Stone, *Exclusive: Biz Stone on Twitter and Activism*, ATLANTIC (Oct. 19, 2010, 8:19 AM), http://www.theatlantic.com/technology/archive/2010/10/exclusive-biz-stone-on-twitter-and-activism/64772 ("Twitter users played their roles in . . . the political unrest in Iran but Mr. Gladwell is keen to downplay their efforts—and the fact that former national-security adviser Mark Pfeifle called for Twitter to be nominated for the Nobel Peace Prize seems only to have ruffled his feathers."). Stone argues that the "leaderless, self-organizing systems" that Gladwell dismissed as incapable of truly challenging the status quo are instead "the very embodiment of change" because they lower the bar to activism and allow individuals to act as one toward a common goal. *Id.*

[49] *See, e.g.*, Sara Ledwith, *Iran's Neda Shows Citizen Journalism Unleashed*, REUTERS (June 23, 2009, 2:36 PM), http://www.reuters.com/article/idUSTRE55M3AJ20090623 ("Since Reuters and other foreign media are subject to Iranian restrictions on their ability to report, film or take pictures in Tehran, they increasingly depend on people like the one on whose cameraphone Neda's death was recorded.").

[50] Neda, whose name in Persian means "voice," became the voice of Iran's freedom movement. *See Times Topics: Neda Agha-Soltan*, N.Y. TIMES (June 22, 2009), http://topics.nytimes.com/topics/reference/timestopics/people/s/neda_agha_soltan/index.html. The story of Neda's life, her video-recorded death, and her enduring legacy are well-told in the HBO documentary film *For Neda*. For a synopsis, see *HBO: For Neda: Synopsis*, HBO, http://www.hbo.com/documentaries/for-neda/index.html#/documentaries/for-neda/synopsis.html (last visited July 2, 2012).

[51] The grainy cell phone video of Neda's death is widely available online. *See, e.g.*, Xeni Jardin, *Iran: Neda (Warning: Graphic Video)*, BOINGBOING (June 21, 2009, 11:50 AM), http://www.boingboing.net/2009/06/21/iran-neda-warning-gr.html#previouspost. On the day of Neda's death, President Barack Obama warned the Iranian government that the world was, indeed, watching. *See* Press Release, Office of the Press Secretary, Statement of the President on Iran (June 20, 2009), *available at* http://www.whitehouse.gov/the_press_office/Statement-from-the-President-on-Iran ("The Iranian government must understand that the world is watching. We mourn each and every innocent life that is lost. We call on the Iranian government to stop all violent and unjust actions against its own people.").

were tools of subversion.[52] Blogger Jila Bani Yaghoob, winner of the 2010 "Reporters Without Borders Freedom of Expression" award, was arrested along with her husband and twenty other journalists during an election protest.[53] She was sentenced to one year in prison and was banned from working as a journalist for the next thirty years, and her husband received a five-year prison sentence.[54] Other activists soon learned that even their instant messaging activity—an ostensibly private mode of communication—could land them in jail.[55] As of March 30, 2012, the Threatened Voices project was actively tracking 316 Iranian bloggers who had been threatened or arrested by the Iranian government.[56]

The postelection wave of arrests[57] is perhaps not surprising in light of Iran's robust online surveillance apparatus,[58] which is aided by Western technology,[59] and Iran's well-documented animosity toward press freedom.[60] Nevertheless, these arrests helped shine a floodlight on the

[52] REPORTERS SANS FRONTIÈRES, *supra* note 33, at 19 (discussing Iranian Internet filtration, surveillance, blogger arrests, cyber-dissidence, and the government's desire to "block the transmission via the Internet of photos taken with a cell phone").

[53] *Cracking Down Remorselessly, Tehran Shows Its True Face*, REPORTERS SANS FRONTIÈRES (Oct. 28, 2010), http://en.rsf.org/iran-cracking-down-remorselessly-tehran-28-10-2010,38693.html.

[54] *Id.*

[55] *Internet Filtering in Iran*, OPENNET INITIATIVE 7 (June 16, 2009), http://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf ("Women's rights activists reported that they were shown transcripts of instant messaging sessions by authorities after their arrest, which, if true, would support the existence of an advanced surveillance program.").

[56] *Threatened Voices—Iran*, GLOBAL VOICES ONLINE, http://threatened.globalvoicesonline.org/bloggers/iran (last visited July 2, 2012). These statistics reveal a sharp increase in blogger arrests beginning in 2009. *Id.*; *see also Press Freedom Violations Recounted in Real Time (from July to December 2010)*, REPORTERS SANS FRONTIÈRES, http://en.rsf.org/iran-press-freedom-violations-recounted-09-09-2010,37863.html (last updated Feb. 11, 2011) (cataloging the legal entanglements of Iranian journalists and bloggers).

[57] *See, e.g.*, REPORTERS SANS FRONTIÈRES, *supra* note 33 (discussing the postelection arrests of blogger and human rights activist Shiva Nazar Ahrari as well as cyber-dissident Mojtaba Lotfi).

[58] *See Internet Filtering in Iran*, *supra* note 55, at 6 ("Iran is reportedly investing in improving its technical capacity to extensively monitor the behavior of its citizens on the Internet. The routing of Internet traffic through proxy servers offers the potential for monitoring and logging essentially all unencrypted Web traffic, including e-mail, instant messaging and browsing. The architecture of the Iranian Internet is particularly conducive to widespread surveillance as all traffic from the dozens of ISPs serving households is routed through the state-controlled telecommunications infrastructure . . . .").

[59] *See id.* at 6–7 ("In 2008, two European companies reportedly sold a sophisticated electronic surveillance system capable of monitoring Internet use that could be utilized for tracking and monitoring the online activities of human rights organizations and political dissidents. [The state-controlled Telecommunication Company of Iran] is said to have received the equipment from Nokia Siemens Networks, a joint venture between the Finnish cell phone maker and the German company Siemens.").

[60] Iran ranks a miserable 172 out of 175 on the Reporters Sans Frontières Press Freedom Index, owing to its "[a]utomatic prior censorship, state surveillance of journalists, mistreatment, journalists forced to flee the country, illegal arrests and imprisonment." *Press Freedom Index 2009*, REPORTERS SANS FRONTIÈRES, http://en.rsf.org/press-freedom-index-2009,1001.html (last visited July 2, 2012). Iran is at the "gates of the infernal trio" occupied by Turkmenistan, North Korea, and Eritrea—places "where the media are so suppressed they are non-existent." *Id.*

importance of unfiltered Internet access and online anonymity to U.S. democratization efforts abroad and U.S. access to world news; likewise, the arrests focused attention on the role to be played by volunteer-operated anonymity networks like Tor.[61]

B. The Official U.S. Reaction

Twitter's role in the Iranian story garnered so much media attention[62] that on June 16, 2009, the U.S. State Department asked the website to delay its scheduled maintenance in an effort to keep the service available to Iranian protesters.[63] The following month, the U.S. Senate added the Victims of Iranian Censorship (VOICE) Act to a defense spending bill authorizing up to $50 million in federal funding "to help Iranians evade their government's attempts to censor the Internet."[64] Enacted in October 2009, the VOICE Act explicitly authorizes spending to "develop additional proxy server capabilit[ies] and anti-censorship software" so that users in Iran may bypass Iranian government censorship of U.S.-funded Persian-language news websites.[65]

The VOICE Act also created the Iranian Electronic Education, Exchange, and Media Fund, a U.S. Treasury fund, to facilitate the development of technologies that will help the Iranian people "gain access to and share information; . . . exercise freedom of speech, freedom of expression, and freedom of assembly through the Internet and other electronic media; . . . and . . . counter efforts . . . to block, censor, and monitor the Internet."[66] Recent changes to U.S. export regulations continued

---

[61] *See, e.g.*, Cyrus Farivar, *How Geeks (and Non-Geeks) Can Help Iranians Online*, FRONTLINE (July 17, 2009, 2:36 PM), http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2009/07/how-geeks-and-non-geeks-can-help-iranians-online.html ("[T]here already is a growing legion of people worldwide who are helping Iranians improve access to the heavily-filtered and significantly slower [Iranian] Internet. Some have installed a piece of software called Tor on their home computers.").

[62] *See* Morozov, *supra* note 7, at 10 ("In the first days after the protests, it was hard to find a television network or a newspaper . . . that didn't run a feature or an editorial extolling the role of Twitter in fomenting and publicizing the Iranian protests.").

[63] *See* Daily Press Briefing, Ian Kelly, Spokesman, U.S. Department of State (June 16, 2009), *available at* http://www.state.gov/r/pa/prs/dpb/2009/jun/124991.htm; Sue Pleming, *U.S. State Department Speaks to Twitter over Iran*, REUTERS (June 16, 2009, 3:26 PM), http://www.reuters.com/article/idUSWBT01137420090616 ("The U.S. State Department said on Tuesday it had contacted the social networking service Twitter to urge it to delay a planned upgrade that would have cut daytime service to Iranians who are disputing their election."). More than one year after the election protests, the State Department continued to recognize the ability of social networking to foment social change. *See, e.g.*, Reza Aslan, *Tweeting to Iran*, DAILY BEAST (Feb. 20, 2011, 12:00 AM), http://www.thedailybeast.com/newsweek/2011/02/20/tweeting-to-iran.html (reporting that the State Department launched its own Persian-language Twitter feed).

[64] Eli Lake, *Senate OKs Funds to Help Thwart Iran Web Censors: Measure Aims to Circumvent "Cruel Regime,"* WASH. TIMES, July 26, 2009, at A1.

[65] Victims of Iranian Censorship Act, Pub. L. No. 111-84, §§ 1261–1266, 123 Stat. 2190, 2553–55 (2009) (codified at 22 U.S.C. §§ 6201, 6204 (2006)).

[66] *Id.* § 1263(c). In 2010, the House of Representatives considered, but ultimately did not pass, a

in a similar vein, "authorizing the exportation of certain Internet-based personal communications services and software," such as social networking and blogging services, to Iran.[67]

U.S. investment in Iranian democratization predates the 2009 election uprising. The State Department spent $31 million in 2007 and appropriated another $60 million in 2008, all with the goal of promoting free speech and democracy in Iran.[68] These funds enabled Voice of America Broadcasting to invest in a Tor-embedded, Persian-language version of the Firefox web browser.[69] Tor, in turn, allowed Iranian dissidents to access government-blocked websites, evade government detection, and generally "give Ahmadinejad's Web censors headaches."[70]

C. Tor: What Lawyers Should Know About Onion Routing

Tor primarily bills itself as a privacy and civil liberties tool (rather than a way of bypassing censorship[71]) and it discourages use of the Tor network for file-sharing purposes.[72] Tor uses "onion routing"—a technology originally developed by the U.S. Naval Research Laboratory to protect government communications.[73] Tor anonymizes[74] its users' Internet activity

---

related bill calling for the creation of an Internet Freedom Foundation. The foundation would have awarded grants to "develop deployable technologies to defeat Internet suppression and censorship" by foreign governments. Internet Freedom Act of 2010, H.R. 4784, 111th Cong. §§ 3, 5 (2010).

[67] Cuban Assets Control Regulations; Sudanese Sanctions Regulations; Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 10,998 (Mar. 10, 2010) (to be codified at 31 C.F.R. pt. 560); *see also* Mark Landler, *U.S. Hopes Exports of Internet Services Will Help Open Closed Societies*, N.Y. TIMES, Mar. 8, 2010, at A4 (discussing the Obama Administration's decision to allow the exporting of online services to Iran). For a discussion of the First Amendment implications of U.S.–Iran trade sanctions, see *infra* note 212 and accompanying text.

[68] Eli Lake, *Protestors Use Navy Technology to Avoid Censorship*, WASH. TIMES, June 26, 2010, at A1. Lake quoted former State Department Iran democracy program coordinator David Denehy, who said the program's goal was "to promote freedom of speech for Iranians to communicate with each other and the outside world." *Id.*

[69] *Id.* Tor is now available as a component of the Tor Browser Bundle for the Firefox browser. *See Tor Project: Torbutton*, TOR PROJECT, https://www.torproject.org/torbutton (last updated Dec. 17, 2011).

[70] Lake, *supra* note 68 (quoting Wired.com's national security blog editor, Noah Schachtman) (internal quotation mark omitted).

[71] *See* Roger Dingledine, *Ten Things To Look For in a Circumvention Tool*, TOR PROJECT 6 (Sept. 16, 2010), https://www.torproject.org/press/presskit/2010-09-16-circumvention-features.pdf (explaining that publicity, while beneficial, can attract the ire of censors who may choose to block a particular tool merely to create a repressive veneer and induce self-censorship).

[72] *See* Elec. Frontier Found., *Legal FAQ for Tor Relay Operators*, TOR PROJECT, http://www.torproject.org/eff/tor-legal-faq.html.en (last updated Aug. 24, 2011) [hereinafter EFF, *Legal FAQ*] (advising against the use of Tor for illegal purposes and explaining that "Tor has been developed to be a tool for free expression, privacy, and human rights"); *Tor FAQ*, TOR PROJECT, https://www.torproject.org/docs/faq.html.en (last visited July 2, 2012) (explaining that the Tor service is slow in part because many users "don't understand or care that Tor can't currently handle file-sharing traffic load").

[73] *Inception*, *supra* note 11; *see also Brief Selected History*, ONION ROUTING, http://www.onion-router.net/History.html (last visited July 2, 2012) (chronicling a brief selected history of onion routing,

by funneling web traffic through a series of encrypted virtual tunnels.[75] These tunnels are made possible by a distributed, volunteer-run network of Tor operators—individuals who run Tor software on their computers for the benefit of others.[76] New operators join, and thereby expand, the Tor network with the understanding that their efforts can help protect the anonymity of endangered citizen journalists and human rights activists in countries like Iran and China.[77]

As information travels from one Tor operator's tunnel to another, the software adds a new "layer" of encryption (hence the onion metaphor) such that no operator in the circuit can ever trace the transmission back more than one layer, protecting the Tor user who initiated it.[78] Tor operators called "relay nodes" pass information along the circuit and an "exit node" operator hands off the transmission to the user's intended destination.[79] That destination might be a website, an instant messaging server, or any other online service that users wish to access without revealing their true IP addresses.[80] From the destination's perspective, the transmission appears to come directly from the exit node; indeed the transmission bears the exit node operator's IP address.[81]

The Tor network's decentralized architecture and its reliance on volunteer operators are of potential legal import and therefore deserve further explanation. Centralized networks route all user activity through computers operated by a single entity.[82] Perhaps the most famous example

---

from its origins in 1995 as a project funded by the Office of Naval Research through 2004, when U.S. government ceased funding Tor). The name "Tor" derives from an acronym, T.O.R. signifying "The Onion Router." *See Tor Project: FAQ*, *supra* note 72.

[74] Achieving anonymity, in the Internet context, requires a two-pronged approach. First, the user must establish an anonymous Internet *connection* (one that does not reveal the user's unique IP address). This capability is the province of Tor and other anonymity services. Second, users must anonymize the *contents* of their communications. Users who interact with websites that offer transport layer security or "TLS" (indicated by the use of "https://" instead of "http://") enjoy this type of anonymity. *See, e.g.*, Abbott, *supra* note 10, at 24 (discussing TLS in the context of a Tor user who visits https://secure.wikileaks.org).

[75] *Tor: Overview*, *supra* note 11. For a brief video illustrating this process, see Conrad Warre, *How Tor Works*, MIT TECH. REV. (Apr. 21, 2009), http://www.technologyreview.com/video/?vid=315.

[76] *Tor: Overview*, *supra* note 11.

[77] *See Inception*, *supra* note 11; *What Is a Tor Relay?*, *supra* note 11 ("Working together, we can improve the network for everyone and protect the anonymity of Tor users all over the world.").

[78] *See* Abbott, *supra* note 10, at 23 (explaining how Tor builds multiple circuits thereby ensuring that "no one person is ever able to trace activity back to a particular user"); *Tor: Overview*, *supra* note 11.

[79] Abbott, *supra* note 10, at 23. While relay and exit node operators are listed publicly, a third type of operator (called a "bridge node") remains hidden from public view and reserves its services for users whose governments actively censor the Internet. *Id.*

[80] *Id.* at 22.

[81] *See id.* at 26. The fact that all Tor users take on the IP addresses of their exit node operators exposes the latter to liability for the former's wrongdoing. *See* discussion *infra* Part II.A.

[82] DINGLEDINE, *supra* note 71, at 3 ("A centralized tool puts all of its users' requests through one or

of a centralized file-sharing tool was Napster, whose servers maintained an index of MP3 song files available to download from its users.[83]

Tor is decentralized in the sense that the software itself routes all user activity through a series of volunteer operators, and no single entity monitors or controls the process.[84] In essence, the software does everything short of funding itself and updating its own code—functions currently performed by TorProject.org. Running in "client mode," Tor offers the user anonymity and access to censored websites. In "server mode," it adds the computer to a worldwide network of Tor operators who facilitate anonymous, unfiltered web access for Tor users.[85] This decentralized design allows the Tor service to endure in the absence of an overseeing entity.[86]

As with many Internet innovations, Tor technology is a double-edged sword.[87] The same anonymity technology that can save an Iranian dissident's life can make a direct infringer untraceable to the copyright holder.[88] And from Tor's perspective, a government-blocked website looks the same as Hulu.com's IP filtration scheme that permits access only to

---

a few servers that the tool operator controls.").

[83] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1012, 1027 (9th Cir. 2001) (affirming an injunction "against Napster's participation in copyright infringement" and determining that "Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index").

[84] DINGLEDINE, *supra* note 71, at 3 ("A decentralized design like Tor . . . sends the traffic through multiple different locations, so there is no single location or entity that gets to watch what websites each user is accessing.").

[85] Eric J. Stieglitz, Note, *Anonymity on the Internet: How Does It Work, Who Needs It, and What Are Its Policy Implications?*, 24 CARDOZO ARTS & ENT. L.J. 1395, 1402–03 (2007) (discussing Tor in the context of tools that allow Internet users, including Chinese dissidents, to bypass censorship).

[86] *See* Abbott, *supra* note 10, at 26 ("Tor is not Napster. There is no central authority to shut down and no key technology to outlaw."); *see also* DINGLEDINE, *supra* note 71, at 2 (comparing Tor to Psiphon, Java Anon Proxy, Freegate, and Ultrareach—censorship-bypass tools that do not have volunteer-operated networks). A similarly decentralized architecture has made Gnutella, another file-sharing network, notoriously difficult to shut down. Less than one month after the court-ordered injunction of the LimeWire service (a popular Gnutella client), LimeWire Pirate Edition emerged, courtesy of an unknown development team. *See* Arista Records LLC v. Lime Wire LLC, No. 06 Civ. 05936 (KMW), 2010 U.S. Dist. LEXIS 115675, at *6 (S.D.N.Y. Oct. 26, 2010) (granting a permanent injunction against Lime Wire LLC); Chloe Albanesius, *Report: LimeWire 'Resurrected' by Secret Dev Team*, PCMAG.COM (Nov. 9, 2010, 5:50 PM), http://www.pcmag.com/article2/0,2817,2372412,00.asp ("LimeWire Pirate Edition should work better than the last functioning version of LimeWire (5.5.10), and it should keep working for longer. There's no adware or spyware: the piratical monkeys are doing this for the benefit of the community." (quoting an anonymous source) (internal quotation marks omitted)).

[87] Speaking in the context of liberation technology, Professor Diamond observes that, "[i]n the end, technology is merely a tool, open to both noble and nefarious purposes" but notes that innovative citizens in places like Iran can use these tools to bring down authoritarianism. Diamond, *supra* note 4, at 71, 80.

[88] Lawrence Lessig makes a similar (if more dramatic) point, noting that, "technologies that enable Aung San Suu Kyi to continue to push for democracy in Burma will enable Al Qaeda to continue to wage its terrorist war against the United States." LAWRENCE LESSIG, CODE: VERSION 2.0, at 225 (2006).

U.S. web users[89]—both are roadblocks easily bypassed by routing traffic through operators in other locations.

On one hand, some see Tor as a "beacon of democracy."[90] In June 2009, as U.S. media found themselves sifting through Twitter feeds for news on the Iranian situation,[91] the Electronic Frontier Foundation (EFF) (a U.S.-based nonprofit organization dedicated to defending civil rights in the "digital world") urged "[t]hose looking to help fight censorship" in Iran to become Tor operators.[92] Newly minted activists and technophiles around the world shared EFF's sentiment,[93] and Tor usage within Iran increased 950% during that month.[94] Currently, over 42,000 Iranians use Tor on any given day.[95]

---

[89] *See Help: International (Outside USA)*, HULU, http://www.hulu.com/support/article/171122 (last visited July 2, 2012) ("Our intention is to make Hulu's growing content lineup available worldwide as quickly as possible. This requires working with the content owners to clear the rights for each show or film in each specific region. . . . We don't have a definite timeline, but we'll continue to work to make it happen."). Hulu's filtration scheme demonstrates one way in which websites utilize geolocation—the derivation of geographic information from a user's IP address. For a discussion of geolocation, see King, *supra* note 17.

[90] Abbott, *supra* note 10.

[91] Golnaz Esfandiari, *The Twitter Devolution*, FOREIGN POL'Y (June 7, 2010), http://www.foreignpolicy.com/articles/2010/06/07/the_twitter_revolution_that_wasnt ("Western journalists who couldn't reach—or didn't bother reaching?—people on the ground in Iran simply scrolled through the English-language tweets posted with tag #iranelection."). Esfandiari argues that media reports of Twitter usage within Iran were greatly exaggerated—a position that is not incompatible with this Comment's discussion of social networking as a vehicle for getting unbiased news reports *out of* Iran.

[92] Richard Esguerra, *Help Protesters in Iran: Run a Tor Bridge or a Tor Relay*, ELECTRONIC FRONTIER FOUND. (June 29, 2009), http://www.eff.org/deeplinks/2009/06/help-protesters-iran-run-tor-relays-bridges. EFF continues to promote Tor as a way to aid Iranian activists. *See The EFF Tor Challenge*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/torchallenge (last visited July 2, 2012) ("Activists worldwide use Tor to protect their anonymity online and to circumvent Internet censorship. But they all rely on a limited number of user-provided 'relays' to protect themselves and communicate with others. Internet users worldwide need your help to make the Tor network stronger and faster, so take the Tor Challenge today!"); *What Is a Tor Relay?*, *supra* note 11 (describing Tor and quoting an anonymous Iranian human rights activist as saying that "we use Tor to access our website and to publish to our blog, which is blocked inside of our country").

[93] *See, e.g.*, DanX, *How to Setup a Tor Relay or Tor Bridge*, WHY WE PROTEST (June 18, 2009), https://whyweprotest.net/community/threads/how-to-setup-a-tor-relay-or-tor-bridge.69952 (describing Tor as "something of great value to our friends in Iran"); Cory Doctorow, *Run a TOR Node, Help Iranians and Others Keep Their Privacy*, BOINGBOING (June 29, 2009, 10:34 PM), http://www.boingboing.net/2009/06/29/run-a-tor-node-help.html ("Whatever you think of Mousavi, I suspect that we all agree that Iranian citizens should be allowed to communicate without being spied upon by their governments (if only Americans enjoyed this right!).").

[94] *See* karsten, *Measuring Tor and Iran (Part Two)*, TOR BLOG (July 1, 2009), http://blog.torproject.org/blog/measuring-tor-and-iran-part-two.

[95] *See Tor Metrics Portal: Users*, TOR PROJECT, https://metrics.torproject.org/users.html?graph=direct-users&country=ir#direct-users (last visited July 2, 2012) (showing a mean of 42,062 daily users connecting from Iran).

Others view Tor differently—as a "den of thieves and pedophiles"[96]—because it can frustrate law enforcement efforts that rely on IP tracking. Tor is particularly frustrating in that it does not, at present, give law enforcement "backdoor" access to encrypted data.[97] And because of its decentralized design and multilayered encryption, Tor operators are incapable of identifying the sources of transmissions that travel through their virtual tunnels.[98] An Internet user could theoretically use Tor to remain anonymous while engaging in all manner of illegal online activity—from defamation to child pornography trafficking[99] to material support of terrorism.[100] Even under court order, a Tor operator would have "no incriminating information to turn over."[101]

Although a complete discussion of Tor in the context of wiretap law is beyond the scope of this Comment, it is worth noting that Tor operators, and providers of similar anonymity technologies, may soon find themselves the targets of new legislation requiring backdoor access to encrypted data. FBI and NSA officials have urged Congress to propose legislation that would require all communication-enabling services to be technically capable of complying with wiretap orders.[102] Encryption services would likely be required to be capable of unscrambling their data and intercepting peer-to-peer communications if asked to do so by a court.[103] Such legislation would undermine Tor's many positive uses because, once a backdoor is

---

[96] Abbott, *supra* note 10, at 22.

[97] *Tor Project: FAQ*, *supra* note 72 ("There is absolutely no backdoor in Tor. Nobody has asked us to put one in, and we know some smart lawyers who say that it's unlikely that anybody will try to make us add one in our jurisdiction (U.S.). If they do ask us, we will fight them, and (the lawyers say) probably win.").

[98] This statement presumes that the Tor operator is using Tor software as intended. Like most software, Tor can be hacked. *See, e.g.*, *infra* note 99 and accompanying text (discussing hacks directed at catching child pornography traffickers).

[99] German police have intercepted child pornography trafficked over Tor. *See* Ryan Singel, *German Cops Raid Home of Wikileaks and Tor Volunteer—Update*, WIRED (Mar. 25, 2009, 12:04 PM), http://www.wired.com/threatlevel/2009/03/wikileaks-domai (reporting a raid on the home of Wikileaks supporter and Tor operator, Theodor Reppe, as part of a child pornography investigation). In the United States, concerns over Tor-encrypted child-pornography trafficking led security researcher and renowned hacker HD Moore to develop a controversial program that can identify child pornographers on the Tor network. *See* Robert Lemos, *Tor Hack Proposed to Catch Criminals*, SECURITYFOCUS (Mar. 8, 2007), http://www.securityfocus.com/news/11447. A representative of the Tor Project pointed out that Moore's program, called "Torment . . . could also be used by authoritarian regimes to track down democracy activists or by the United States' enemies to track down the military intelligence officers that use the network." *Id.*

[100] The extent of illegal activity over any effective anonymity network is perhaps by its very nature impossible to ascertain. That said, there is some evidence of child-pornography trafficking and file sharing over the Tor network. *See* Singel, *supra* note 99.

[101] Abbott, *supra* note 10.

[102] Charlie Savage, *U.S. Is Working to Ease Wiretaps on the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1.

[103] *Id.*

opened for law enforcement, it is likely only a matter of time before hackers and hostile governments find their way in.[104]

Whatever the outcome of this proposed legislation, those who view Tor as a "den of thieves" may soon find support for their position in the context of copyright infringement litigation. The next Part explores the likely shape of this litigation: Volunteer Tor operators may find themselves wrongly fingered as infringers, blamed for file-sharing activity that passed through their virtual tunnels.

II. LOOKING AHEAD: TOR LITIGATION

The use of Tor to conceal copyright infringement is, as of this writing, an unlitigated area. Nevertheless, Tor operators in the United States are almost certain to soon find themselves defendants in copyright infringement actions. This Part explores the likely path of Tor litigation as a logical consequence of pending actions involving the popular file-sharing protocol BitTorrent, as well as the theories of liability likely to be employed against Tor operators.

A. Anonymity and Illegal File Sharing: Tor Meets BitTorrent

More than a decade ago, former Grateful Dead lyricist and famed cyber-libertarian[105] John Perry Barlow prophesied that "[t]he future will win; there will be no property in cyberspace."[106] Today, those who see Tor as a den of copyright thieves might consider it a point for Barlow. File sharing continues to be a major source of copyright litigation,[107] and individuals are using Tor to hide file-sharing activities.[108] This marriage of

---

[104] Greek hackers exploited a similar legally mandated backdoor in 2005, prompting Columbia University computer science professor Steven M. Bellovin to characterize the FBI–NSA proposal as "a disaster waiting to happen." *Id.* (quoting Bellovin) (internal quotation mark omitted). The Tor Project points out an additional problem with backdoors: "[T]he policy mechanisms needed to ensure correct handling of this responsibility are enormous and unsolved." *Abuse FAQ*, TOR PROJECT, http://www.torproject.org/docs/faq-abuse.html.en (last visited July 2, 2012).

[105] "Cyberlibertarianism" is an ideology that "emphasizes individual rights, especially online rights, as the most important political good." Alexandra Samuel, *Hacktivism and the Future of Democratic Discourse*, *in* DEMOCRACY ONLINE 123, 131 (Peter M. Shane ed., 2004).

[106] John Perry Barlow, *The Next Economy of Ideas: Will Copyright Survive the Napster Bomb? Nope, but Creativity Will*, WIRED, OCT. 2000, at 240, 241.

[107] As of January 2011, nearly 100,000 BitTorrent users in the United States had been sued for copyright infringement since the start of 2010. Ernesto, *100,000 P2P Users Sued in US Mass Lawsuits*, TORRENTFREAK (Jan. 30, 2011), http://www.torrentfreak.com/100000-p2p-users-sued-in-us-mass-lawsuits-110130. By August 2011, that number had doubled. Ernesto, *200,000 BitTorrent Users Sued in the United States*, TORRENTFREAK (Aug. 8, 2011), http://www.torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808.

[108] A recent study analyzing BitTorrent usage over the Tor network concluded that "more than half of the traffic carried over Tor is BitTorrent." Abdelberi Chaabane et al., *Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network*, NETWORK & SYS. SECURITY, Sept. 1–3, 2010, at 167, 170, *available at* http://planete.inrialpes.fr/papers/TorTraffic-NSS10.pdf. The Tor Project

anonymity technology and file sharing is perhaps no more surprising than a burglar's decision to wear gloves instead of leaving fingerprints.[109] And the honeymoon is not likely to be over anytime soon, as increased federal funding[110] of Tor-like technology will encourage new anonymity and censorship-bypass providers to enter the marketplace.[111]

District courts in Washington, D.C. are already seeing the likely precursors of Tor litigation. In "the most sweeping antipiracy litigation since 2003," thousands of users of the popular file-sharing protocol BitTorrent were accused of sharing unauthorized copies of independent films including Academy Award-winner *The Hurt Locker*.[112] U.S. Copyright Group (USCG), the plaintiff in what has come to be known as "*Hurt Locker* litigation," filed a number of John Doe infringement suits seeking subpoenas forcing the alleged infringers' ISPs to reveal each user's identity using lists of IP addresses furnished by the plaintiffs.[113] If any of the true infringers had the presence of mind to mask their IP addresses using Tor, the subpoenaed ISPs will reveal the identities of the Tor exit node operators whose IP addresses appear, on the surface, to be those of the direct infringers.[114] Thus, Tor operators may soon find themselves in court facing damages of up to $150,000 per illegally copied movie.[115]

This type of litigation puts ISPs in the unenviable position of potentially having to produce and reveal customer information, but these are hardly the only costs incurred by ISPs as a consequence of file sharing. ISPs have a business interest in minimizing illegal file-sharing activity

---

acknowledges widespread file sharing via Tor—an activity that it considers to be abuse. *See* mikeperry, *Tips for Running an Exit Node with Minimal Harassment*, TOR BLOG (June 30, 2010), https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment ("Excessive bittorrent abuse over Tor unfortunately means you will likely receive a deluge of DMCA abuse complaints."). For a discussion of DMCA abuse complaints directed at Tor operators, see *infra* notes 137–38 and accompanying text.

[109] Eric Stieglitz arguably predicted the Tor–BitTorrent union back in 2007 when he wrote, "[M]usic traders could easily move away from open peer-to-peer software and to anonymous networks where their true identity would remain masked from legal process." Stieglitz, *supra* note 85, at 1413.

[110] *See, e.g.*, *supra* notes 64–66 and accompanying text (discussing the VOICE Act).

[111] The Tor Project's Executive Director Andrew Lewman has said that the "growing amount of money available for Web circumvention and activism" will encourage the already observable trend of "companies retooling themselves to become circumvention providers." Lake, *supra* note 64 (quoting Lewman).

[112] Greg Sandoval, *Accused 'Hurt Locker' Pirates Turn to Law School*, CNET NEWS (Nov. 1, 2010, 5:39 AM), http://news.cnet.com/8301-31001_3-20021307-261.html.

[113] *See* Voltage Pictures, LLC v. Does 1–5,000, 818 F. Supp. 2d 28, 31, 45 (D.D.C. 2011).

[114] For further discussion of this hypothetical scenario see *infra* note 186 and accompanying text.

[115] These are the damages alleged by USCG in the *Hurt Locker* litigation. *See USCG v. The People*, ELEC. FRONTIER FOUND., http://www.eff.org/uscg (last visited July 2, 2012) ("Once the user's identity is known, USCG's strategy appears to be to threaten a judgment of up to $150,000 per downloaded movie—the maximum penalty allowable by law in copyright suits and a very unlikely judgment in cases arising from a single noncommercial infringement—in order to pressure the alleged infringers to settle quickly for $1,500 to $2,500 per person.").

since these transmissions—typically large music and video files—place significant strains on bandwidth. One solution is bandwidth throttling, a technique in which ISPs selectively block what they suspect to be file-sharing traffic.[116] ISPs can identify file-sharing traffic through a controversial technique called "deep-packet inspection" (DPI).[117] For example, in 2007, the public learned that one ISP, Comcast, had been using DPI to identify and selectively block BitTorrent traffic—a practice that initially raised the ire of the FCC.[118] The bad news for ISPs is that Tor frustrates DPI[119] and therefore hinders proactive attempts to thwart copyright thievery.

Tor-facilitated infringement also poses special problems for plaintiffs. Unable to trace the direct infringer whose IP remains buried beneath layers of Tor encryption and without the prophylaxis of DPI-facilitated ISP bandwidth throttling, it stands to reason that copyright holders will soon turn to the only identifiable targets: the Tor operators whose IP addresses—and hence identities—are, for the most part, publicly available. Exit node operators face the greatest risk of liability because all Tor users take on the IP address of their exit node operator.[120] In other words, "[w]hen someone does something improper via Tor, the exit node operator often gets blamed."[121]

---

[116] *See, e.g.*, David Kravets, *Comcast Ordered to Allow Free Flow of File Sharing Traffic*, WIRED (Aug. 1, 2008, 9:03 AM), http://www.wired.com/threatlevel/2008/08/fcc-declares-co. ISPs often rely on this method of managing the flow of Internet data, also known as "traffic shaping." *See* Peter Svensson, *Comcast Blocks Some Internet Traffic*, WASH. POST (Oct. 19, 2007, 6:32 PM), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/19/AR2007101900842.html; *see also* Kravets, *supra* (reporting that Comcast's practice of throttling was widespread).

[117] *See* Kravets, *supra* note 116.

[118] *In re* Formal Complaint of Free Press & Pub. Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, 23 FCC Rcd. 13028, 13029–31 (Aug. 1, 2008). The FCC ordered Comcast to stop the practice, which it analogized to opening "customers' mail because [Comcast] wants to deliver mail not based on the address or type of stamp on the envelope but on the type of letter contained therein." *Id.* at 13051. Two years later, an appeals court vacated the FCC's decision. *See* Comcast Corp. v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010).

[119] As discussed *supra* note 74, Tor encrypts the Internet *connection*, and users are encouraged to take the additional step of encrypting the actual *contents* of their transmissions. These double-encrypted Tor transmissions appear least vulnerable to DPI. *See* Chaabane et al., *supra* note 108, at 169 (using DPI to analyze Tor network usage and noting that more than 25% of traffic volume remained unrecognizable, probably due to encryption); NEDANET, http://nedanet.org (last visited July 2, 2012) ("The [Iranian] regime appears to be using deep packet inspection on all traffic in and out of Iran. Do not use unencrypted communications for anything sensitive unless you want to be jailed, tortured, and killed!").

[120] *See* Stjepan Groš et al., *Protecting TOR Exit Nodes from Abuse*, MIPRO, May 24–28, 2010, at 1246, 1246 ("[T]he Tor network is abused by the attackers but also people use it for all sorts of illegal activities, of which child pornography is probably the most severe. This especially hurts the people who run, so called, *exit nodes* because it seems like this malicious traffic is coming from them, and not from those that originated the traffic.").

[121] Abbott, *supra* note 10, at 26.

Even without the problem of untraceability, suing throngs of direct infringers is a Herculean task.[122] Thus, in the BitTorrent context, plaintiffs have historically pursued the websites that make it possible for individuals to find (and share) BitTorrent files.[123] One could argue that Tor operators are analogous to these BitTorrent clearinghouses in that they too facilitate illegal file sharing.

B. Theories of Liability

A plaintiff alleging copyright infringement against a Tor operator would likely proceed under a theory of contributory infringement because the alternate theories of vicarious liability[124] and inducement[125] are less likely to succeed. Vicarious liability is ill-suited because it would require showing that the defendant had "an obvious and direct financial interest in the exploitation of copyrighted materials."[126] Tor operators gain no financial benefit from their actions. If anything, they incur costs in the form of reduced bandwidth and computer processing resources.[127]

Inducement theory is also ill-suited as a theory of liability because it would require the plaintiff to show that the Tor operator intended to induce infringement by communicating messages "designed to stimulate others to

---

[122] Indeed plaintiffs in the *Hurt Locker* litigation were forced to voluntarily dismiss tens of thousands of unnamed defendants from the suit because ISPs were releasing user information so slowly that plaintiffs could not meet the court's filing deadlines. *See supra* note 18 and accompanying text.

[123] Courts have taken notice of this inherent difficulty when granting injunctive relief to copyright holders in actions against BitTorrent indexing websites. *See, e.g.*, Columbia Pictures Indus., Inc. v. Fung, No. CV 06-5578 SVW (JCx), 2010 Dist. LEXIS 91169, at *8 (C.D. Cal. May 20, 2010) ("[G]iven the multiplicity of infringements of Plaintiffs' works caused by a single user downloading a single dot-torrent file from Defendants' sites . . . it would be untenable for Plaintiffs to track and proceed against each infringing end-user." (citation omitted)).

[124] A defendant can be held vicariously liable for copyright infringement activity by a third party if the defendant: (1) "possess[es] the right and ability to supervise the infringing conduct" and (2) "ha[s] an obvious and direct financial interest in the exploitation of copyrighted materials." 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A][2] (2011) (footnote omitted) (internal quotation marks omitted).

[125] Under a theory of inducement, a defendant can be held liable for the direct infringement activity of a third party if the defendant's "active steps to encourage infringement lead[] to actual infringement taking place." *Id.* § 12.04[A][4][a] (footnote omitted) (internal quotation marks omitted).

[126] Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

[127] *See Tor FAQ*, *supra* note 72 ("Tor relays do use a lot of ram. It is not unusual for a fast exit relay to use 500–1000 MB of memory."). Tor exit node operators probably incur the greatest time cost, as successful operation of an exit node requires something on the order of an advanced computer science degree and a fairly intricate understanding of copyright law. A brief glance at the elaborate response templates developed by the Tor community to aid exit node operators in dealing with ISP complaints should make this point abundantly clear. *See, e.g.*, Elec. Frontier Found., *Response Template for Tor Relay Operator to ISP*, TOR PROJECT, https://www.torproject.org/eff/tor-dmca-response.html (last updated May 31, 2011) [hereinafter EFF, *Response Template*]; *Tor Abuse Templates*, TOR PROJECT, https://trac.torproject.org/projects/tor/wiki/doc/TorAbuseTemplates (last visited July 2, 2012).

commit violations."[128] Because this theory, a creature of the Supreme Court's 2005 decision in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,[129] has not been heavily tested, it remains unclear whether it could be used effectively in the Tor context.[130] Nevertheless, inducement theory is not likely to succeed against a Tor operator because of one critical distinction from the defendant file-sharing services in *Grokster*: While Grokster, Ltd. somewhat blatantly advertised its illegal purpose,[131] Tor operators (and the Tor Project) typically hold themselves out as a privacy and civil liberties tool and they actively discourage illegal file sharing over the network.[132] Although the Grokster service was structurally analogous to Tor in that both networks are decentralized,[133] the *Grokster*-borne inducement theory seems ill-suited in the Tor context.

Instead, plaintiffs will probably proceed under the more promising theory of contributory infringement. To prevail under this theory, a plaintiff would need to prove that the Tor operator: (1) had knowledge of infringement and (2) materially contributed to it.[134] The file-sharing service Napster was famously enjoined under this theory of liability.[135]

Applied to a Tor operator, the first element of contributory infringement—knowledge of infringement—is easily satisfied if the operator received notice of alleged infringement, e.g., in the form of a complaint from the copyright holder[136] or (as more commonly happens) from the operator's ISP. When an ISP receives a complaint from a copyright holder alleging infringement by one of the ISP's customers, the ISP may forward the notice to the alleged infringer as part of a statutorily

---

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

[129] *Id.*

[130] Riley, *supra* note 9, at 607.

[131] *Grokster*, 545 U.S. at 936–38.

[132] *See supra* notes 71–72 and accompanying text. Notably, discouraging file sharing is different from policing file sharing—a practice that itself carries risk of liability for the Tor operator. I discuss this risk *infra* notes 181–82 and accompanying text.

[133] *Grokster*, 545 U.S. at 928.

[134] *See* Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (defining a contributory infringer as "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another" (footnote omitted)); *see also* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1171 (9th Cir. 2007) (adopting *Gershwin* as the test for contributory liability).

[135] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001). The Ninth Circuit also held that Napster was likely to be found liable under a theory of vicarious liability because Napster profited directly from infringement and had both the right and ability to police infringing activity as a consequence of its centralized server system. *Id.* at 1022–24. Napster also tried (unsuccessfully) to invoke the same statutory safe harbor that this Comment argues should protect Tor operators. *See id.* at 1025. For a discussion of why Tor operators can succeed where Napster failed, see *infra* Part III.C.

[136] Napster was found to have actual knowledge of illegal file sharing partly because plaintiff Recording Industry Association of America had placed it on notice of thousands of infringing files. *Napster*, 239 F.3d at 1020 n.5.

prescribed process commonly known as "notice and takedown." By implementing the notice and takedown regime established in § 512(c) of the Digital Millennium Copyright Act (DMCA), the ISP lays a foundation for its own immunity as a transitory digital communication provider under § 512(a).[137]

Tor exit node operators are particularly likely to receive these § 512(c) notices, because theirs are the only IP addresses that a destination website will ever see.[138] Indeed, the risk associated with exit node operation may explain why the majority of Tor node operators disallow exit connections entirely.[139] Exit node operators who find themselves the recipients of § 512(c) notices might choose to respond to the ISP and contest the allegations.[140] In the context of a contributory infringement action, such a response might paradoxically increase the operator's risk of liability by proving the knowledge element.

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

EFF, a prominent nonprofit organization dedicated to defending civil liberties "in the digital world,"[141] argues that Tor operators who enable others to use the Internet anonymously are performing lawful activities and should not be liable for activity occurring in their tunnels.[142] Since 2005, EFF has actively sought test case volunteers in the hopes of setting "a clear legal precedent establishing that merely running a relay does not create

---

[137] *See* 17 U.S.C. § 512(a), (c) (2006).

[138] *See supra* notes 120–21 and accompanying text. Tor Project acknowledges this risk and warns exit node operators of it. *See Abuse FAQ*, *supra* note 104 ("If you run a Tor relay that allows exit connections . . . it's probably safe to say that you will eventually hear from somebody. Abuse complaints may come in a variety of forms.").

[139] *See* mikeperry, *supra* note 108 ("[E]xit nodes are typically on the scarce side. Exits usually occupy 30–33% of network by capacity, but are currently at a whopping 38.5% . . . .").

[140] *See, e.g.*, EFF, *Response Template*, *supra* note 127 (informing Tor operators that "anyone providing routing services may face copyright complaints" but that the DMCA "safe harbors should provide protections" to operators and their ISPs).

[141] *About EFF*, ELEC. FRONTIER FOUND., http://www.eff.org/about (last visited July 2, 2012). EFF has been involved as plaintiff, defense counsel, or amicus curiae in a number of landmark disputes over digital rights, including *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), and *Reno v. ACLU*, 521 U.S. 844 (1997). *See Legal Victories*, ELEC. FRONTIER FOUND., http://www.eff.org/victories (last visited July 2, 2011).

[142] EFF, *Legal FAQ*, *supra* note 72 ("[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. . . . 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.").

copyright liability for either operators or their bandwidths providers."[143] EFF's position will gain support if Tor operators are found to qualify for immunity under § 512(a), the safe harbor provision for service providers that merely act as conduits for digital communication[144]—an argument presented in the next Part.

III. TOR OPERATORS AND THE DMCA § 512(A) SAFE HARBOR

Tor operators live in a fog of uncertainty surrounding secondary infringement liability because their services have both infringing and noninfringing uses. This specter of liability is, by itself, harmful because it discourages new operators from joining the network, particularly as exit nodes.[145] And in a decentralized, volunteer-run network like Tor, a dearth of operators is an existential threat to the overall service. For example, one major problem for Tor users is network latency (i.e., slow download and upload speeds)—a problem attributable to network size.[146] While Tor's user base continues to grow, the growth of its operator network (currently estimated at over 2800 active nodes[147]) has lagged behind, in part due to legal uncertainty.[148] There is a dearth of exit node operators[149]—an

---

[143] *Id.*; *see also* Roger Dingledine, *EFF Is Looking for Tor DMCA Test Case Volunteers*, SEUL.ORG (Oct. 26, 2005), http://archives.seul.org/or/talk/Oct-2005/msg00208.html (describing the ideal test case client).

[144] *See* 17 U.S.C. § 512(a) (2006).

[145] *See* Tsuen-Wan "Johnny" Ngan et al., *Building Incentives into Tor*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 238, 241 (Radu Sion ed., 2010) ("[L]egal uncertainty may drive users away from running [Tor] as an exit relay.").

[146] *See* DINGLEDINE, *supra* note 71, at 5 ("[As compared to centralized-trust designs,] distributed-trust designs . . . have a harder time tracking their users, and if they rely on volunteers to provide capacity, then getting more volunteers is a more complex process than just paying for more bandwidth."); *see also* Cyrus Nemati, *SXSW: Of Tech, Nerds, and New Media*, CENTER FOR DEMOCRACY & TECH. (Mar. 15, 2010), http://www.cdt.org/blogs/cyrus-nemati/sxsw-tech-nerds-and-new-media ("Tor is a fantastic anonymity network that is also fantastically slow, but the more people who use it, the faster it gets. This enables Internet users in free countries to do a little bit to help create an anonymous network for oppressed peoples.").

[147] *See Tor Network Status—Network Detail*, TORSTATUS, http://torstatus.blutmagie.de/network_detail.php (last visited July 2, 2012) (showing a total of 2832 nodes in the "Aggregate Summary—Number of Routers Matching Specified Criteria"). The Tor Project reports similar statistics. *See Tor Metrics Portal: Network*, TOR PROJECT, https://metrics.torproject.org/network.html (last visited July 2, 2012). These are rough estimates because, of the three classes of nodes comprising the Tor operator network, only two (relay nodes and exit nodes) are listed publicly. Abbott, *supra* note 10, at 23; *see also TorDNSExitList*, TOR PROJECT, https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorDNSExitList (last visited July 2, 2012) (explaining how to determine if a particular IP address belongs to a Tor exit node). Publicly listed nodes are susceptible to blocking by governments or websites that seek to deter Tor usage. For this reason, the IP addresses of Tor "bridge" providers (the third type of node) are never made public. Abbott, *supra* note 10, at 22–23.

[148] Ngan et al., *supra* note 145.

[149] *See Tor FAQ*, *supra* note 72 ("If you have lots of bandwidth, you should definitely run a normal relay . . . . If you're willing to be an exit, you should definitely run a normal relay, since we need more exits.").

unsurprising fact, given that they face the greatest risk of liability.

This specter of liability also chills speech. Fearing liability, ISPs and institutional service providers (including universities) increasingly censor their users—including Tor operators.[150] And operators who receive DMCA § 512(c) notices from their ISPs may, quite understandably, choose to cease the activity rather than risk losing Internet connectivity.[151]

This Part argues that Tor operators, like ISPs, should be entitled to statutory safe harbor under DMCA § 512(a) as conduits for transitory network communications.[152] Section 512 of the DMCA, also called the Online Copyright Infringement Liability Limitation Act (OCILLA), creates four separate safe harbor provisions.[153] Parties falling within a safe harbor provision are exempt from monetary liability, but they may still face injunctive orders.[154]

A. Tor Operators Are Eligible for § 512 Safe Harbor Protection

Section 512(a) limits monetary liability for digital network communication service providers that merely act as conduits for information.[155] "Service provider" is a term of art, defined within the statute to indicate "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[156] Tor fits this definition rather neatly—it passes a user's Internet traffic through a circuit of Tor

---

[150] Researchers at the University of Colorado, Boulder, experienced this effect firsthand. To better understand Tor's uses and misuses, they launched an exit node and collected usage data in the form of traffic logs. The researchers received numerous § 512(c) notices and were asked by university administration to discontinue the node. *See* McCoy et al., *supra* note 8, at 63–66, 71.

[151] The Tor Project recommends that exit node operators communicate proactively with their ISPs so that they "don't end up being shut down due to easily preventable abuse complaints." mikeperry, *supra* note 108. However, as one exit node operator's comment illustrates, this is easier said than done: "I just had to shut down my exit node due to DMCA complaints for bittorrent traffic. My exit node received 7 DMCA complaints within two months. . . . The provider was very understanding, but were [sic] getting pressure from their upstream provider." Anonymous, *Tips for Running an Exit Node with Minimal Harassment*, TOR BLOG (Sept. 17, 2010), https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment.

[152] 17 U.S.C. § 512(a) (2006).

[153] *See* Online Copyright Infringement Liability Limitation Act, Pub. L. 105-304, 112 Stat. 2860 (codified at § 512). *See generally* NIMMER & NIMMER, *supra* note 124, § 12B.01[C][1–2] (providing an overview of DMCA limitations on liability); *id.* § 12B.02 (discussing the first safe harbor provision, for transitory digital network communications).

[154] *See id.* § 12B.01[C][2] ("The distinctive feature of [OCILLA] is that it creates something that falls slightly short of being a complete exemption. Instead, it creates various 'limitations on liability,' which are tantamount to exemptions in all material respects but one: a party who qualifies may still be subject to injunction." (footnotes omitted)).

[155] § 512(a).

[156] *Id.* § 512(k)(1)(A).

operators before routing it to the destination. As the Tor Project website explains, "Tor does not modify, or even know, what you are sending into it. It merely relays your traffic."[157]

To qualify for any of the four safe harbors in § 512, service providers must meet two threshold conditions for eligibility. They must (1) maintain a termination policy for repeat infringers[158] and (2) comply with "standard technical measures."[159]

First, under § 512(i)(1)(A), service providers must adopt, reasonably implement, and inform their subscribers or account holders of their termination policies addressing repeat infringers.[160] Tor arguably meets this condition through the use of "exit policies" that govern the specific types of connections (known as "ports") that are permitted or denied by each operator.[161] For example, Tor's default exit policy attempts to prevent spamming and file sharing by blocking the ports typically associated with those activities.[162]

Admittedly, exit policies do not constitute strict adherence to § 512(i)(1)(A). Tor is not a subscription service, and its users—be they repeat infringers or law-abiding citizens—are quite intentionally unidentifiable. However, in the context of an anonymity network, an operator who adopts a reasonable exit policy designed to prevent file-sharing traffic is complying with this provision to the fullest extent possible and should be deemed eligible for safe harbor protection.

The second condition for safe harbor eligibility, § 512(i)(1)(B), requires service providers to "accommodate[] and . . . not interfere with standard technical measures."[163] Although the term "standard technical measures" is subsequently defined as "technical measures that are used by copyright owners to identify or protect copyrighted works,"[164] it remains an

---

[157] *Tor FAQ*, *supra* note 72. This statement assumes that the Tor operator is using the software as intended. It is technically possible for operators to modify Tor's software in such a way as to allow inspection of outgoing data. Tor operators are cautioned not to do this. *See* EFF, *Legal FAQ*, *supra* note 72 ("Do not examine the contents of anyone's communications without first talking to a lawyer."). Tor users can protect themselves against malicious exit nodes by using encryption—"https" instead of "http." *See Surveillance Self-Defense*, ELEC. FRONTIER FOUND., https://ssd.eff.org/tech/tor (last visited July 2, 2012).

[158] § 512(i)(1)(A).

[159] *Id.* § 512(i)(1)(B).

[160] *Id.* § 512(i)(1)(A).

[161] *See Tor FAQ*, *supra* note 72 (explaining that exit policies were implemented to minimize abuse).

[162] *Id.*; *see also* Abbott, *supra* note 10, at 26 ("Nearly every exit node disallows email traffic to prevent spam and blocks file-sharing traffic to prevent DMCA issues. . . . This ability to block access . . . gives exit node operators protection and thereby increases the number of willing operators."). *But see* McCoy et al., *supra* note 150, at 67 (observing that port-based blocking strategies are easily circumvented).

[163] § 512(i)(1)(B).

[164] *Id.* § 512(i)(2).

elusive concept in practice.[165]

Countersurveillance specialist Richard Abbott suggests that Tor operators may run afoul of the § 512(i)(1)(B) noninterference requirement because they enable Tor users to reach websites in spite of IP filtering—a method that allows websites to display content only to users within a given geographic location, while blocking the rest.[166] IP filtering, also called "geo-blocking," allows websites to deliver copyrighted content in compliance with licensing agreements that restrict distribution rights to specific locations.[167] Tor defeats IP filtering because it can, for example, enable U.S.-based users to access BBC broadcast materials intended for U.K. audiences by routing traffic through an exit node whose IP address is located in the United Kingdom.[168] However, an interpretation of "standard technical measures" that encompasses IP filtering would be unworkably broad. As Abbott points out, it would sweep in other widely used (and legal) technologies, including virtual private networks (VPNs).[169]

---

[165] *See* NIMMER & NIMMER, *supra* note 124, at § 12B.02[B][3][a] ("Even as of many years after enactment of [OCILLA], it is unclear whether there is any such thing as 'standard technical measures.'").

[166] Abbott, *supra* note 10, at 25–26.

[167] *See* Michael Geist, *Geo-Blocking Sites a Business Rather Than Legal Issue*, MICHAEL GEIST (July 8, 2010), http://www.michaelgeist.ca/content/view/5179/135 ("[T]he geo-blocking approach is . . . an attempt to preserve an older business model, namely content licencing on a country-by-country or market-by-market approach . . . ."). Dr. Geist observed that geo-blocking is a worldwide phenomenon, affecting U.S. users (who, at that time, could not reach the U.K.-based music service Spotify) and Canadian users (who cannot reach the popular U.S.-based music service Pandora). *Id.* Spotify launched a service for the United States in July 2011. *See, e.g.*, Don Reisinger, *Spotify (Finally) Launches in the U.S.*, CNET NEWS (July 14, 2011, 5:10 AM), http://news.cnet.com/8301-13506_3-20079400-17/spotify-finally-launches-in-the-u.s.

[168] I borrow this example from Abbott, *supra* note 10, at 25 ("Tor allows anyone to access the BBC's Web site via a UK exit node via a UK IP address.").

Tor's IP filter-busting capabilities could, incidentally, also spell liability for Tor operators and distributors of Tor technology, *even in the absence of actual infringement*. Although this frightening prospect is beyond the scope of this Comment, a brief explanation is warranted. The operator's liability might arise under DMCA § 1201(a)(1)(A), a provision that outlaws circumvention of copyright access protection measures. IP address filtering is arguably a "technological measure that effectively controls access" to a protected work and is circumvented by the Tor operator who masks the actual user's IP address—conduct prohibited under § 1201(a)(1)(A). *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, § 103, 112 Stat. 2860, 2863 (1998) (codified as 17 U.S.C. § 1201 (2006)). A related provision, § 1201(a)(2), creates liability for manufacturers and traffickers of technology that circumvents such access-protection measures. *Universal City Studios, Inc. v. Reimerdes* teaches that "the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it." 111 F. Supp. 2d 294, 325 (S.D.N.Y. 2000), *aff'd sub nom.* Universal Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001). Any distributor of Tor software is arguably vulnerable to liability under this line of reasoning. At present, that distributor is U.S.-based nonprofit organization The Tor Project.

[169] Abbott, *supra* note 10, at 25. Using VPN technology, an employer can give its remote employees secure, encrypted access to data residing on the employer's private network. *See, e.g.*, *Cisco VPN Client*, CISCO, http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html (last visited July 2, 2012). VPN technology is spreading beyond the corporate world as a way for users of unsecured

Tor operators are, therefore, "service providers" who meet § 512's two general requirements. This threshold eligibility opens up four statutory safe harbors, of which only § 512(a) (the safe harbor for "Transitory Digital Network Communications," also called the conduit safe harbor) is likely to be invoked by a Tor operator.[170] It is to the operator's eligibility under this subsection that I now turn.

B. Tor Operators Should Enjoy § 512(a) Conduit Safe Harbor

Under DMCA § 512(a), a service provider is not liable for

> infringement of copyright [that occurs] by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections

provided that five statutory requirements are met.[171] Tor meets the five requirements as follows.

First, under § 512(a)(1), the transmission must be "initiated by or at the direction of a person other than the service provider."[172] This is true of Tor operators in that they merely relay Internet traffic initiated by a Tor user.[173] Second, under § 512(a)(2), "the transmission, routing, provision of connections, or storage" must be "carried out through an automatic technical process without selection of the material by the service provider."[174] That is precisely what Tor software does: it automatically selects a random circuit of Tor operators through which it routes the Tor user's activity.[175] Operators do not select the routed material—the software does it for them.

One could argue that the operator's ability to set an exit policy[176]

---

public Wi-Fi connections to protect themselves from a form of identity theft know as "session hijacking." *See, e.g.*, Jolie O'Dell, *HOW TO: Protect Yourself from Firesheep with a VPN*, MASHABLE TECH (Oct. 28, 2010), http://www.mashable.com/2010/10/28/firesheep-vpns (discussing VPN as a way to protect private information from hackers using the malicious session hijacking program Firesheep).

[170] 17 U.S.C. § 512 (2006) also provides limited liability, under specified circumstances, to service providers that (1) store data only temporarily (the "System Caching" safe harbor under § 512(b)), (2) store user-generated data (the safe harbor for "Information Residing on Systems or Networks at Direction of Users" under § 512(c)), or (3) act as search engines (the safe harbor for "Information Location Tools" under § 512(d)). Tor operators perform none of these functions.

[171] *Id.* § 512(a).

[172] *Id.* § 512(a)(1).

[173] *See supra* note 157 and accompanying text.

[174] § 512(a)(2).

[175] *See Tor: Overview*, *supra* note 11 ("Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays . . . . To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network.").

[176] For a discussion of Tor operator exit policies, see *supra* notes 161–62 and accompanying text.

constitutes a selection of routed material, thereby disqualifying Tor operators from the conduit safe harbor for failure to meet § 512(a)(2). This is partly true. By turning off a specific port, an operator can ensure that the type of material typically transmitted through the blocked port will not be routed through that operator's tunnel. However, rather than selecting (or more accurately, blocking) specific material, the exit node operator is making a wholesale decision to block *all* material—infringing or otherwise—that may be transmitted over a given port. This level of control is therefore much too attenuated to constitute a "selection" of material for § 512(a)(2) purposes.

Under the third statutory requirement, service providers must "not select the recipients of the material except as an automatic response to the request of another person."[177] This is true as to the ultimate recipient of material transmitted through a circuit of Tor operators because the destination is predetermined by the Tor user who initiated the request. Operators who route traffic along the circuit are not properly characterized as "recipients";[178] hence, it is irrelevant that the precise pathway (that is, the sequence of operators randomly selected by Tor software to form the circuit) is not actually selected by the user.

Tor operators also meet the fourth statutory requirement:

> [N]o 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 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.[179]

Operators do not store the transmitted data—they merely hand it off from one node to another until reaching the exit node, which then passes the data to the user's destination.[180] Although it is technically possible for a malicious exit node operator to capture and store information at this final handoff,[181] doing so would require modifying the Tor software itself.[182] Such an individual is not so much a Tor operator as a garden-variety hacker.

---

[177] § 512(a)(3).

[178] *See supra* note 157 and accompanying text.

[179] § 512(a)(4).

[180] The same process occurs in reverse when the destination responds to a Tor user's request: data travels back through a random circuit of Tor operators before arriving at the user. *See Tor: Overview*, *supra* note 11.

[181] *See* McCoy et al., *supra* note 8, at 67–68 (explaining that an eavesdropping exit node can, in some situations, capture identifying information such as usernames and passwords).

[182] *See* EFF, *Legal FAQ*, *supra* note 72 ("You may be technically capable of modifying the Tor source code or installing additional software to monitor or log plaintext that exits your relay. However, Tor relay operators in the United States can possibly create civil and even criminal liability for themselves under state or federal wiretap laws if they monitor, log, or disclose Tor users' communications . . . .").

Tor operators meet the final requirement, transmission of material "through the system or network without modification of its content,"[183] as a consequence of the same automatic process discussed in connection with § 512(a)(3). Operators do not inspect content much less modify it. They merely route information along a randomly assigned circuit.

C. Conduit Safe Harbor in the File-Sharing Context: Why Tor Operators Can Prevail Where Napster Failed[184]

I anticipate that Tor litigation will arise in an illegal file-sharing context, most likely in connection with the popular BitTorrent file-sharing protocol. For example, the *Hurt Locker* litigation[185] might lead to the identification of defendants' IP addresses belonging to Tor exit node operators.[186] In the absence of direct evidence, plaintiffs would likely be unable to prove direct infringement by a Tor operator because the operator's passivity weighs heavily against finding the volitional element required for direct infringement.[187] There is, however, a case to be made for contributory infringement liability.[188]

Defendant file-sharing services have not fared well in secondary infringement actions,[189] and it stands to reason that Tor operator–defendants

---

[183] § 512(a)(5).

[184] This Part uses Napster, rather than Grokster, as a comparator for reasons discussed *supra* text accompanying notes 130–33.

[185] *See supra* notes 113–15 and accompanying text.

[186] Rights holders who seek to identify direct infringers through the statutory subpoena process described in DMCA § 512(h) do, admittedly, face an uphill battle. This is because § 512(h) has been interpreted not to apply to online service providers that act merely as conduits for allegedly infringing information. *See, e.g.*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1237 (D.C. Cir. 2003) ("[T]he text of § 512(h) and the overall structure of § 512 clearly establish . . . that § 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others."), *cert. denied*, 543 U.S. 924 (2004); *see also In re* Charter Commc'ns, Inc. Subpoena Enforcement Matter, 393 F.3d 771, 777 (8th Cir. 2005) (agreeing with *Verizon*'s reasoning).

[187] *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1369–70 (N.D. Cal. 1995) ("Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.").

[188] An interesting question arises as to whether plaintiffs would seek to subpoena the Tor operator in an attempt to reveal the direct infringer's identity. By its nature, Tor ensures that operators will have "no incriminating information to turn over." Abbott, *supra* note 10 (noting further that operators cannot "effectively police the activity of users"). Although the last link in the chain—the exit node—can potentially eavesdrop on the information that passes between it and the destination, it has no way of identifying the original user who initiated the communication. *Id.* at 23–24; *see also supra* note 157 (discussing exit node abuse).

[189] *See, e.g.*, A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 927 (N.D. Cal. 2000) (granting plaintiff's motion for preliminary injunction), *aff'd in part*, *rev'd in part*, 239 F.3d 1004 (9th Cir. 2001); A&M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136, at *10 (N.D. Cal. May 12, 2000) (denying defendant Napster's motion for summary judgment and finding that

would face many of the same arguments against safe harbor that helped plaintiffs defeat the likes of Napster. But Tor is not a file-sharing service, and decentralized, volunteer-run anonymity networks like Tor can satisfy conduit safe harbor requirements where file-sharing services have failed.

Admittedly, the Tor network does resemble a file-sharing network,[190] and the emergence of Tor–BitTorrent hybrid programs such as Vuze[191] blurs the distinction even further. File-sharing pioneer Napster tried the § 512(a) defense and failed so miserably that its de facto successor, Grokster, did not even bother invoking a conduit safe harbor defense when it stood accused of contributory infringement.[192] Napster's play for conduit safe harbor failed because it did not "transmit, route, or provide connections for allegedly infringing material *through* its system."[193] Noting the intentions of Congress to limit § 512(a) to situations "in which a service provider plays the role of a 'conduit' for the communications of others,"[194] the district court found that Napster's role in conveying "address information to establish a connection between the requesting and host[ing] users" did not constitute a connection provided "through" its system.[195] Rather than traveling through the Napster system, the connection was found to occur "through the Internet."[196]

Tor is easily distinguishable from Napster. Whereas Napster's infringing transmissions never traveled through Napster servers—passing instead from host to recipient "through the Internet"[197]—an infringing transmission would travel directly through a Tor operator's computer. The fact that traffic emerges at the destination bearing the exit node's IP address is proof that it has traveled "through" that operator. Thus, Tor operator–defendants should qualify for safe harbor under § 512(a).

Unfortunately, even if Tor operator–defendants qualify for safe harbor protection from monetary remedies under § 512(a) for the reasons described

---

Napster "does not meet the requirements of subsection 512(a)").

[190] *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 44.

[191] The popular BitTorrent client Vuze (formerly called Azureus) has built-in Tor support. Vuze does, however, discourage using Tor to anonymize file-sharing traffic. *See Anonymous File Sharing Using Azureus with Tor and I2P*, VUZEWIKI, http://wiki.vuze.com/w/Anonymous_file_sharing_using_Azureus_with_Tor_and_I2P (last updated Mar. 3, 2010, 7:35 PM) ("Please DO NOT use Tor for routing peer-to-peer data traffic, it can not handle the bandwidth. They have indicated that they will make efforts to ban such usage if it continues, which will likely affect both legitimate and unwanted use!" (emphasis omitted)). These statements, however self-serving when delivered by Vuze, are echoed by Tor. *See, e.g.*, sources cited *supra* note 72.

[192] *See supra* notes 129–33 and accompanying text (discussing litigation against Grokster).

[193] *A & M Records*, 2000 WL 573136, at *10 (emphasis added).

[194] *Id.* at *8 (quoting H.R. REP. NO. 105-551, pt. 2 (1998)).

[195] *Id.*

[196] *Id.* Although neither party had attempted to define "routing" for the purposes of § 512(a), the court found that routing also did not occur through Napster's system. *Id.*

[197] *Id.* at *7–8.

in this Part, they may yet face injunctive action under § 512(j)(1)(B). Courts considering such injunctive relief must weigh a number of statutorily delineated factors including the burden placed upon a service provider, the magnitude of likely harm to the rights holder, technical feasibility and effectiveness of injunctive relief, and the availability of less burdensome solutions.[198] Part IV argues that injunctive action against a Tor operator impinges on the operator's First Amendment speech interest—a serious burden that militates against the granting of injunctive relief.

IV. BALANCING HARMS: TOR AND FIRST AMENDMENT INTERESTS

"[I]n cyberspace, the First Amendment is a local ordinance."

–John Perry Barlow[199]

The Tor operator is an individual who enables others to bypass censorship and speak anonymously, and any limitation on the operator's ability to perform these functions raises First Amendment issues. By allowing speakers—Tor users—to convey information anonymously and without fear of reprisal, Tor operators are furthering a First Amendment right to receive information.[200] Further, the act of facilitating someone else's speech arguably constitutes "speech" for First Amendment purposes, and is worthy of protection in and of itself.[201] Courts in equity should weigh the burden upon these twin interests when considering injunctive relief against a Tor operator.[202]

A. Tor and the Right to Receive Information

The First Amendment undoubtedly protects an individual's right to receive information.[203] This right operates in tandem with the press freedom

---

[198] 17 U.S.C. § 512(j)(2)(A)–(D) (2006).

[199] LESSIG, *supra* note 88, at 383 n.4 (quoting John Perry Barlow).

[200] *See infra* notes 203–04 and accompanying text.

[201] For example, in the context of campaign finance, restrictions on speech-facilitating monetary contributions implicate the First Amendment. *See, e.g.*, Buckley v. Valeo, 424 U.S. 1, 19 (1976) (per curiam) ("A restriction on the amount of money a person or group can spend on political communication during a campaign necessarily reduces the quantity of expression by restricting the number of issues discussed, the depth of their exploration, and the size of the audience reached.").

[202] As discussed *supra* Part III, § 512(a) shields transitory digital network providers from monetary liability only—it leaves open the possibility of injunctive or equitable relief. In the file-sharing context, plaintiffs have often sought injunctive relief to stop alleged infringement. *See, e.g.*, Arista Records LLC v. Lime Wire LLC, No. 06 Civ. 05936 (KMW), 2010 U.S. Dist. LEXIS 115675, at *6 (S.D.N.Y. Oct. 26, 2010) (permanently enjoining the LimeWire file-sharing service).

[203] Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas. 'This freedom [of speech and press] . . . necessarily protects the right to receive . . . .'" (alteration and omissions in original) (quoting Martin v. City of Struthers, 319 U.S. 141, 143 (1943))).

as a necessary consequence of the right to distribute information.[204]

Today's press, the primary distributor of information, is a much-democratized version of its former self thanks to the phenomenon of citizen journalism.[205] Beyond our borders, oppressive regimes can no longer rely on state-run media to deliver a preapproved monologue, as citizen journalists have turned media into dialogue.[206] We Americans, in turn, are no longer required to judge the adequacy of our elected representatives' foreign policy decisions based solely on reports obtained through mainstream media. Admittedly, the democratization of journalism has its flaws: amateur journalists can be unreliable sources of information[207] and professional journalists might feel the need to abandon or abridge their journalistic standards to compete with the amateurs in terms of sheer speed of news dissemination.[208] Nevertheless, as a phenomenon that can lend individuals access to otherwise-unobtainable news, citizen journalism is a good thing. That an informed citizenry is essential to the proper functioning of our own democracy is "at once a cornerstone of serious legal and moral philosophy, a high school civics verity, and a cliché."[209]

Like the Iranian example of 2009, subsequent democratic movements in Tunisia, Egypt, Libya, and much of the Arab world—a phenomenon termed the "Arab Spring"[210]—illustrate that people's ability to receive

---

[204] *See Martin*, 319 U.S. at 143 ("The right of freedom of speech and press has broad scope. The authors of the First Amendment knew that novel and unconventional ideas might disturb the complacent, but they chose to encourage a freedom which they believed essential if vigorous enlightenment was ever to triumph over slothful ignorance. This freedom embraces the right to distribute literature . . . and necessarily protects the right to receive it." (footnote omitted)).

[205] *See* A. Michael Froomkin, *Technologies for Democracy*, *in* DEMOCRACY ONLINE, *supra* note 105, at 3, 9 ("Blogs represent one of the latest examples of the Internet's democratization of publishing.").

[206] *See, e.g.*, Kendra Heideman & Haleh Esfandiari, *You Are the Media: How Iranians "Democratized" the Media*, WOODROW WILSON INT'L CTR. FOR SCHOLARS, http://www.wilsoncenter.org/event/you-are-the-media-how-iranians-democratized-the-media (last visited July 2, 2012) ("[T]he rise of citizen journalism in Iran after the 2009 election symbolized a reversal of information dissemination, an effective 'democratization' of media. . . . [J]ournalist Roozbeh Mirebrahimi . . . commented that this transformation crushed the traditional 'monologue' and instead created a new 'dialogue' in Iran.").

[207] *See* ANDREW KEEN, THE CULT OF THE AMATEUR: HOW TODAY'S INTERNET IS KILLING OUR CULTURE 5 (2007) ("It's the blind leading the blind—infinite monkeys providing infinite information for infinite readers, perpetuating the cycle of misinformation and ignorance.").

[208] *See* Larry E. Ribstein, *From Bricks to Pajamas: The Law and Economics of Amateur Journalism*, 48 WM. & MARY L. REV. 185, 209 (2006) ("When 'pajama bloggers' who need not answer to an editor can rush stories onto millions of computer screens, professionals might abandon their standards in order to compete.").

[209] Froomkin, *supra* note 205, at 3.

[210] *See* Con Coughlin, *From Arab Spring to Boiling-Hot Summer: Iran Is Ruthlessly Exploiting the Pro-Democracy Movement for Its Own Ends*, TELEGRAPH (May 10, 2011, 8:05 PM), http://www.telegraph.co.uk/comment/columnists/concoughlin/8505793/From-Arab-Spring-to-boiling-hot-summer.html (explaining that the term "Arab Spring" was "meant to encapsulate the youthful exuberance of the pro-democracy movements that had sprung up throughout the Middle East" in early

accurate, timely information about world events is well-served by the courageous work of citizen journalists abroad.[211] Tor technology promotes the exercise of the right to receive information.[212] This technology offers a nontraceability[213] that is essential to protect speakers who live under political repression—so essential that Lawrence Lessig has advocated for recognition of a protected legal right to "privacy-enhancing technologies."[214] Protecting online privacy is a laudable goal unto itself,[215] and a speaker's right to the same anonymity enjoyed by Publius of the *Federalist Papers* is hardly in dispute.[216] However, the Tor operator's role takes on constitutional dimensions when we recognize that protecting speaker anonymity promotes a First Amendment right to receive information.

B. Speech-Facilitation as Protected Speech

People volunteer to become Tor operators because they believe in protecting civil liberties on the Internet. They donate things of measurable pecuniary value: bandwidth, computer resources, and time. They do these things to send a political statement about freedom in a digital age. Their conduct, like the burning of a flag or a draft card, speaks volumes and should be protected as speech.

During the same year that saw the invention of the World Wide Web,[217]

2011).

[211] Even old-guard media establishments like the *New York Times* have incorporated citizen journalism into their reporting on the Middle Eastern protest movements. *See, e.g.*, *Arab World Uprisings: A Country-by-Country Look*, N.Y. TIMES (last updated Dec. 10, 2011), http://www.nytimes.com/interactive/world/middleeast/middle-east-hub.html?ref=middleeast (combining uncensored and often untranslated Twitter postings with *Times* correspondent reports on Libya, Yemen, Syria, and Egypt).

[212] Writing on the issue of U.S. trade sanctions against Iran, Nadia Luhr argues that the sanctions regime prior to March 2010 operated as a prior restraint on speech because it caused Americans to be deprived of Iran-related news. Nadia L. Luhr, Note, *Iran, Social Media, and U.S. Trade Sanctions: The First Amendment Implications of U.S. Foreign Policy*, 8 FIRST AMEND. L. REV. 500, 520 (2010); *id.* at 501 ("Prohibiting American Web 2.0 companies from providing access to users in sanctioned countries restricted Americans' ability to receive communications from these users, and such a prohibition constituted unconstitutional prior restraint.").

[213] Internet anonymity—or, more specifically, nontraceability—is the ability "to send a message without the content of that message being traced to the sender." LESSIG, *supra* note 88, at 224–25.

[214] *Id.* Lessig defines "privacy-enhancing technologies" as those "technologies designed to give the user more technical control over data associated with him or her." *Id.* at 223.

[215] It is also a goal shared by the Obama administration. *See* Julia Angwin, *Watchdog Planned for Online Privacy*, WALL ST. J., Nov. 12, 2010, at A1 ("The Obama Administration is preparing a stepped-up approach to policing Internet privacy that calls for new laws and the creation of a new position to oversee the effort . . . .").

[216] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.").

[217] The year was 1989, and the inventor's name was Tim Berners-Lee (not Al Gore). *See Tim*

the U.S. Supreme Court famously determined that defendant Gregory Lee Johnson's conduct—burning the American flag—was a form of political expression protected by the First Amendment.[218] *Johnson* teaches that "conduct possesses sufficient communicative elements to bring the First Amendment into play" when it evinces an "intent to convey a particularized message" and when that message is likely to be understood by its audience.[219]

By the *Johnson* definition, a Tor operator's conduct contains enough elements of speech to implicate the First Amendment. Tor's purpose is articulated ad nauseam on numerous web pages hosted by the Tor Project, the Electronic Frontier Foundation (EFF), and even the U.S. Naval Research Laboratory.[220] Tor exit node operators are also advised to post web pages called "exit notices" so that curious ISPs can easily understand their *raisons d'être*.[221] The message is intentional, particularized, and conveyed in the customary manner of the Internet—a web page.

Critics will be quick to point out that a weighing of First Amendment interests is unnecessary because "copyright law contains built-in First Amendment accommodations."[222] However, as the Supreme Court observed in *Eldred v. Ashcroft*, copyright laws are not "categorically immune" from First Amendment challenges.[223] It stands to reason that relief granted in vindication of a copyright violation is similarly not immune from countervailing First Amendment considerations. A court considering injunctive relief against a Tor operator is free to, and in fact *must*, balance interests and harms in furtherance of equity.

We should apply laws to cyberspace in speech-protective ways because in doing so we allow a democratizing medium to flourish elsewhere in the

---

Berners-Lee, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/People/Berners-Lee/Overview.html (last visited July 2, 2012).

[218] Texas v. Johnson, 491 U.S. 397, 406 (1989).

[219] *Id.* at 404 (quoting Spence v. Washington, 418 U.S. 405, 410–11 (1974)).

[220] *See, e.g.*, Esguerra, *supra* note 92 (EFF); *Executive Summary*, ONION ROUTING, http://www.onion-router.net/Summary.html (last visited July 2, 2012) (U.S. Naval Research Laboratory).

[221] *See* mikeperry, *supra* note 108 ("Once you have a good reverse DNS name, you should put some content there that explains what Tor is for those who see the name and try to visit it via http."). For a sample Exit Notice, see *This Is a Tor Exit Router*, TOR PROJECT, http://gitweb.torproject.org/tor.git?a=blob_plain;hb=HEAD;f=contrib/tor-exit-notice.html (last visited July 2, 2012) ("This router is part of the Tor Anonymity Network, which is dedicated to providing privacy to people who need it most: average computer users.").

[222] Eldred v. Ashcroft, 537 U.S. 186, 193, 219–21 (2003) (holding that the Copyright Term Extension Act, Pub. L. No. 105-298, § 102(b), (d), 112 Stat. 2827–28 (1998) (codified as amended at 17 U.S.C. §§ 302, 304 (2006)), which increases the duration of copyright protection of new and existing works from fifty years to seventy years following the author's death, did not violate the First Amendment).

[223] *Id.* at 221 ("We recognize that the D.C. Circuit spoke too broadly when it declared copyrights 'categorically immune from challenges under the First Amendment.'" (quoting Elrod v. Reno, 239 F.3d 372, 375 (D.C. Cir. 2001))).

world.[224] As Jack Balkin has observed, the Internet is home to discussions, debates, and collective activities whose value transcends national borders.[225] And where people desire democracy but have little familiarity with its customs, the Internet becomes a pedagogical tool conveying democratic culture—"a culture in which ordinary people can participate, both collectively and individually, in the creation and elaboration of cultural meanings that constitute them as individuals."[226]

Balkin argues that we should protect this digital democratic culture because of its innate value to mankind, and regardless of its impact on American politics or foreign policy.[227] But one need not go quite that far to protect a Tor operator's speech—that speech immediately invokes a political discussion of American civil liberties on the Internet and carries implications for U.S. foreign policy. The proof is in the blogosphere. Despite the best efforts of an unpopular and often lawless Iranian government, democratic culture is emerging in the digital Iran. The Iranian blogosphere, an online community inhabited by over 60,000 routinely updated weblogs, is "full of advocates, on all sides. . . . featur[ing] thousands of politically attentive individuals, commenting on every imaginable issue, with a breadth of perspectives."[228] Iranian citizen journalism is arguably on its way to *replacing* state-run media as a primary source of news.[229]

By enabling an Iranian blogger to speak without fear of imprisonment and providing an Iranian reader with the opportunity to become an educated global citizen unconstrained by censorship, we promote free expression, tolerance, and a sense of shared responsibility—cultural elements that are as

---

[224] This is rooted in the ideas of Jack Balkin, who writes, "The Internet teaches us that the free speech principle is about, and has always been about, the promotion and development of a democratic culture." Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 34 (2004).

[225] Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 438 (2009) ("[W]hat people do on the Internet transcends the nation state; they participate in discussions, debate, and collective activity that does not respect national borders.").

[226] *Id.* (citing Balkin, *supra* note 224, at 3–6, 33–50).

[227] *Id.* at 438–39 ("These are valuable human activities in their own right; they should not be protected only because and to the degree that they might contribute to debate about American politics, or even American foreign policy." (citing Balkin, *supra* note 224, at 32)).

[228] John Kelly & Bruce Etling, *Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere* 10–11 (Berkman Ctr. for Internet & Soc'y, Berkman Ctr. Research Publ'n No. 2008-01, 2008), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf. I am unable to determine the extent to which these bloggers make use of anonymity technology.

[229] *See* Doug Bernard, *Blogs as Journalism in Iran*, VOICE OF AM. (Apr. 12, 2010, 8:00 PM), http://www.voanews.com/english/news/science-technology/Blogs-as-Journalism-in-Iran-90741249.html (noting that, in Iran, "news stories often first appear on blogs, where writers are freer to cover events outside the sanction of government censors"). Indeed, Iranian political cartoonist Nikahang Kowsar says that what the U.S. considers citizen journalism is "just journalism" in Iran. *Id.*

vital to a democracy as the right to vote.[230] Balkin argues that democracy in its broadest sense goes beyond an individual's relationship to the state and extends instead to culture as a whole.[231] If we are truly committed to nurturing democracy in places like Iran, we must recognize the role played by online speakers in allowing individuals to mold a new culture from clay of the old.

CONCLUSION

Tor operators, by their very existence, trigger a political dialogue about the importance of online civil liberties, and their services facilitate the development of democratic culture in places like Iran. They demonstrate that Tor has undeniable noninfringing uses that merit protection, and its volunteer operators should thus enjoy full First Amendment protection. At a minimum, they should benefit from § 512(a) safe harbor as conduits of digital communication.

Without a doubt, anonymity comes at a price and anonymity technology may frustrate the efforts of creative artists who struggle to enforce their copyrights. But set on a scale, our interests in cherishing the right to receive information, protecting politically expressive conduct online, and nurturing nascent democratic cultures by allowing the Internet to flow freely in places like Iran outweighs the risk that Tor-like anonymity networks will facilitate infringement.

[230] Kelly & Etling, *supra* note 228, at 21, 22 ("Democracy requires voting booths, yes, but it also needs a culture of robust free expression with a tolerance for disagreement and dissent, undergirded by a general acceptance of certain moral fundamentals, including principles of fairness and equality, and a sense of shared citizenship and responsibility.").

[231] Balkin, *supra* note 224, at 39 ("Power to the people—democracy—in its broadest, thickest sense, must include our relationship not simply to the state but to culture as a whole, to the processes of meaning-making that constitute us as individuals. Those processes of meaning-making include both the ability to distribute those meanings and the ability to receive them.").