SUPER-INTERMEDIARIES, CODE, HUMAN RIGHTS

IRA STEVEN NATHENSON*

Abstract

We live in an age of intermediated network communications. Although the internet includes many intermediaries, some stand heads and shoulders above the rest. This article examines some of the responsibilities of "Super-Intermediaries" such as YouTube, Twitter, and Facebook, intermediaries that have tremendous *power* over their users' human rights. After considering the controversy arising from the incendiary YouTube video *Innocence of Muslims*, the article suggests that Super-Intermediaries face a difficult and likely impossible mission of fully servicing the broad tapestry of human rights contained in the International Bill of Human Rights. The article further considers how intermediary content-control procedures focus too heavily on intellectual property, and are poorly suited to balancing the broader and often-conflicting set of values embodied in human rights law. Finally, the article examines a number of steps that Super-Intermediaries might take to resolve difficult content problems and ultimately suggests that intermediaries subscribe to a set of process-based guiding principles—a form of *Digital Due Process*—so that intermediaries can better foster human dignity.

---

* Associate Professor of Law, St. Thomas University School of Law, inathenson@stu.edu. I would like to thank the editors of the *Intercultural Human Rights Law Review*, particularly Amber Bounelis and Tina Marie Trunzo Lute, as well as symposium editor Lauren Smith. Additional thanks are due to Daniel Joyce and Molly Land for their comments at the symposium. This article also benefitted greatly from suggestions made by the participants of the 2013 Third Annual Internet Works-in-Progress conference, including Derek Bambauer, Marc Blitz, Anupam Chander, Chloe Georas, Andrew Gilden, Eric Goldman, Dan Hunter, Fred von Lohmann, Mark Lemley, Rebecca Tushnet, and Peter Yu. Finally, I would like to thank my St. Thomas Law colleagues Roy Balleste, John Makdisi, Roza Pati, Amy Ronner, and Siegfried Wiessner for their comments and suggestions, with extra thanks to Professors Pati and Wiessner for encouraging me to explore the synergies between cyberlaw and human rights, for inviting me to participate in the symposium, and for their tireless help and encouragement as I developed this article. Any errors or omissions are mine.

Table of Contents

Introduction

Remember, with great power comes great responsibility.

—Ben Parker's advice to Peter Parker in *Spider-Man*[1]

Don't be evil.

—Unofficial Google motto[2]

Everyone knows *Spider-Man*'s mantra of power and responsibility, a facile cliché that provides an easy shortcut for an otherwise serious moral imperative: those with exceptional power ought to shoulder special burdens on behalf of the less gifted.[3] A parallel admonition can be found in Google's oft-repeated[4] and oft-mocked[5]

---

[1] SPIDER-MAN (Sony 2002). The quote was first used by Spider-Man creator Stan Lee in Spider-Man's introduction in *Amazing Fantasy* #15 in August 1962, where an omniscient narrator describes the dilemma of Peter Parker's new powers: "With great power there must also come—great responsibility!" *See Amazing Fantasy #15: Man Before Hero*, ALEC READS COMICS (July 10, 2012), 8:44 PM http://alecreadscomics.wordpress.com/2012/07/10/amazing-fantasy-15-man-before-hero.

[2] Google Investor Relations, *Code of Conduct*, http://investor.google.com/corporate/code-of-conduct.html (last updated April 25, 2012). Documents filed attendant to Google's 2004 initial public offering state:

> Don't be evil. We believe strongly that in the long term, we will be better served-as shareholders and in all other ways-by a company that does good things for the world even if we forgo some short term gains. This is an important aspect of our culture and is broadly shared within the company.

Google, *2004 Founders' IPO Letter from Larry Page and Sergey Brin*, http://investor.google.com/corporate/2004/ipo-founders-letter.html (italics omitted); *see also* Google Inc., *Am. No. 4 to Form S-1 Reg. Stmt.* (July 26, 2004), http://www.sec.gov/Archives/edgar/data/1288776/000119312504124025/ds1a.htm.

[3] The obligatory database searches reveal unshocking results. Searching Westlaw for "great power" in the same sentence with "great responsibility" yielded 108 hits in the database for law journals (JLR), and 3,596 in the database for news sources (ALLNEWSPLUS).

[4] *See, e.g.*, *Ten things we know to be true*, GOOGLE.COM, http://www.google.com/about/company/philosophy/ (last visited Feb. 22, 2013) ("You can make money without doing evil."). Sources differ on the origin of "Don't be evil." One source identifies Gmail creator Paul Buchheit. *See Paul Buchheit on Gmail,*

vow that it do no evil.[6]

Perhaps these tired quotes about power and responsibility can be mined for new meaning.[7] This article explores the role of powerful internet intermediaries, i.e., entities that provide services that *intermediate* information between the creators or owners of such content, and those who wish to access or interact with such content. Examples include internet service providers providing internet access, as well as online content providers that host content such as

---

AdSense and More, GOOGLE BLOGOSCOPED (July 16, 2007), http://blogoscoped.com/archive/2007-07-16-n55.html. Alternatively, it may be Amit Patel, a Google engineer. *See* Asher Moses, *Don't Be Evil or don't lose value?*, SYDNEY MORNING HERALD (Apr. 15, 2008), http://www.smh.com.au/news/biztech/dont-be-evil/2008/04/15/1208025168177.html.

[5] In 2010, Steve Jobs declared "This don't be evil mantra: 'It's bullshit.'" John C. Abell, *Google's 'Don't Be Evil' Mantra Is 'Bullshit,' Adobe Is Lazy: Apple's Steve Jobs (Update 2)*, WIRED BUSINESS (Jan. 30, 2010, 11:16 PM), http://www.wired.com/business/2010/01/googles-dont-be-evil-mantra-is-bullshit-adobe-is-lazy-apples-steve-jobs/. Unsurprisingly, Jobs' complaints were rooted in his anger over Google's entry into the smartphone business. *Id.* A more damning condemnation comes from noted Google critic Siva Vaidhyanathan, who suggests "The 'Don't be evil' motto is itself evil, because it embodies pride, the belief that the company is capable of avoiding ordinary failings." SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 77 (2011); Jon M. Garon, *Searching Inside Google: Cases, Controversies and the Future of the World's Most Provocative Company*, 30 LOY. L.A. ENT. L. REV. 429, 430 (2010) (noting "[d]on't be evil" policy and criticisms of Google).

[6] *See* text accompanying note 2.

[7] The idea that exceptional power imposes exceptional obligations is by no means new. Voltaire said in the 18th century "Un grand pouvoir impose une lourde responsibilité," or "great power imposes a heavy responsibility." 48 ŒUVRES DE VOLTAIRE (Lefèvre, 1832); *see also President George Albert Smith & Spiderman & a French Guy*, MIDDLE-AGED MORMON MAN (June 19, 2012), http://middle-agedmormonman.blogspot.com/2012/06/president-george-albert-smith-spiderman.html (discussing Spider-Man and the Voltaire quote). The idea also dates to the Bible: "From everyone who has been given much, much will be demanded; and from the one who has been entrusted with much, much more will be asked." LUKE 12:48 (New Int'l version); *see also* Judith A. Aparri, *'With Great Power Comes Great Responsibility' and Other Lessons from Spider Man*, EVERYDAY CHRISTIAN (June 22, 2010), http://www.everydaychristian.com/blogs/post/with_great_power_comes_great_responsibility_spiderman/ (noting *Luke* 12:48).

photos, videos, and blogs. In particular, however, this article focuses on the nature and responsibilities of some of the most *powerful* intermediaries that provide heavily used search or content-hosting services, such as YouTube, Google, Facebook, and Twitter.[8] As Secretary of State Hillary Clinton noted in a 2010 speech on Internet freedom, "viral videos and blog posts are becoming the samizdat [or dissident activity] of our day."[9] Indeed, social networks are credited, rightly or wrongly, with playing a vital role in the Arab Spring.[10]

---

[8] *See, e.g.*, Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age*, 91 B.U. L. REV. 1435, 1439 (2011) (noting the "considerable control" internet intermediaries wield "over what we see and hear"). Although Google owns YouTube, this article treats them separately for analytic purposes.

[9] Secretary of State Hillary Rodham Clinton, *Remarks on Internet Freedom* (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm; *see also* Roy Balleste, *Persuasions and Exhortations: Acknowledging Internet Governance and Human Dignity for All*, 38 SYRACUSE J. INT'L L. & COM. 227, 246-47 (2011) (discussing Clinton's speech). "The underground dissident publications in Eastern Europe, known as samizdat, were important in cultivating dissident voices and circulating dissident speech behind the Iron Curtain." Anupam Chander, *Jasmine Revolutions*, 97 CORNELL L. REV. 1505, 1515 (2012).

[10] *See, e.g.*, RUSSELL L. WEAVER, FROM GUTENBERG TO THE INTERNET: FREE SPEECH, ADVANCING TECHNOLOGY, AND THE IMPLICATIONS FOR DEMOCRACY 76-84 (2013) (describing role of internet in Arab Spring); Nick Bilton, *Disruptions: Silencing the Voices of Militants on Twitter*, N.Y. TIMES BITS BLOG (Dec. 2, 2012) ("Twitter, perhaps more than any other social media outlet, has become one of the most powerful tools to promote democracy in the Middle East."). The *New York Times* describes a Facebook page dedicated to Khaled Mohamed Said, a man who was beaten to death by Egyptian police. *See* Jose Antonio Vargas, *Spring Awakening: How an Egyptian Revolution Began on Facebook*, N.Y. TIMES (Feb. 17, 2012), http://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html. The Facebook site for Mr. Khaled, in turn, states that "Khaled has become the symbol for many Egyptians who dream to see their country free of brutality, torture and ill treatment." FACEBOOK.COM, *Kullena Khaled Said' — 'We Are All Khaled Said*, https://www.facebook.com/elshaheeed.co.uk/info (last visited July 15, 2013).

But some caution against overstating the role of social media in the Arab Spring. A report issued by the Yale Center for the Study of Globalization, after reviewing a number of studies, concluded that although "[s]ocial media played a role," it "did not necessarily drive change." Ellen Lust, *Three Myths About the Arab Uprisings*, http://yaleglobal.yale.edu/content/three-myths-about-arab-uprisings (last visited Feb. 24, 2013); *see also* Guy Harris, *The Arab Spring:*

However, powerful internet intermediaries may also deprive us of our privacy,[11] misappropriate our creations,[12] and permit govern-

Revolution without Revolutionaries?, DEFENCE IQ, (Apr. 27, 2012), http://www.defenceiq.com/defence-technology/articles/social-media-and-the-arab-spring-revolution-withou/ (suggesting that "within the context of the 2011 revolutions, social media networks were essentially barometers, rather than catalysts"); Habibul Haque Khondker, *Role of the New Media in the Arab Spring*, GLOBALIZATIONS, at 678 (Oct. 2011), *available at* http://www.tandfonline.com/doi/pdf/10.1080/14747731.2011.621287 ("There is no question that social media played a significant role in the political movements in Tunisia and Egypt, but one should not overstate the role."); Anita Singh, *Ways With Words: role of Twitter and Facebook in Arab Spring uprising 'overstated', says Hisham Matar*, THE TELEGRAPH (July 11, 2011), http://www.telegraph.co.uk/culture/books/ways-with-words/8629294/Ways-With-Words-role-of-Twitter-and-Facebook-in-Arab-Spring-uprising-overstated-says-Hisham-Matar.html (noting the argument of author Hisham Matar that it "is an exaggeration" that the uprisings in Egypt and Tunisia "couldn't have happened without the internet"). For data on social media and the Arab world, see the *Arab Social Media Report* issued by the Dubai School of Government. *See* http://www.arabsocialmediareport.com/ (interactive site); *see also* Dubai School of Government, *Social Media in the Arab World: Influencing Societal and Cultural Change?* (July 2012), *available at* http://www.arabsocialmediareport.com/UserManagement/popupdownload.aspx.

[11] *See* Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1531 (asking whether people can demand reasonably balanced privacy rights "when the threats to privacy come not from government, but from private corporations, like Google and Facebook" and those "exposing too much personal information are not the government, but ourselves"); *see also* Rory Bahadur, *Electronic Discovery, Informational Privacy, Facebook and Utopian Civil Justice*, 79 MISS. L.J. 317, 366 (2009) ("In the not-too-distant future as we become comfortable accepting the reality that informational privacy is impossible and irrelevant in a spaceless, Facebook-driven world, the nature of the discovery process, and hence the adversarial system of justice, will be modified."); Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1316 (2009) (discussing "blurry-edged" social networks, which "people post content on a medium available to the whole world when that content is not intended for the whole world"); Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1380 (2012) ("From their inception, therefore, there have been concerns that [social networks] create privacy problems.").

[12] *See, e.g.*, Laurie Junkins, *Is Facebook Stealing Your Data?*, NAKEDLAW (Nov. 8, 2012), http://nakedlaw.avvo.com/consumer-protection/is-facebook-stealing-your-data.html; Victoria Lee, *Hoax warning on Facebook sparks fear: Social network forced to reassure users it doesn't 'own' copyright of photos*,

ments to more easily track people down.[13] At the same time, they are increasingly central to humanity's enjoyment of online access. Author Rebecca MacKinnon asks in her book *Consent of the Networked*,[14] "[h]ow do we make sure that people with power over our digital lives will not abuse that power?"[15] As she points out, neither governments *nor* corporations who "build, operate, and govern cyberspace" are being held sufficiently to task: "[t]hey are sovereigns operating without the consent of the networked."[16] Professor Frank Pasquale puts it even more directly: "Internet intermediaries govern online life."[17] Professor Siegfried Wiessner further warns us, "[p]ower is a jealously guarded thing."[18] Accordingly, this article

---

MIRROR NEWS (Nov. 27, 2012), http://www.mirror.co.uk/news/technology-science/facebook-copyright-policy-fears-go-1459499; Helen A.S. Popkin, *Facebook policy change results in hysteria — and a hoax*, NBC NEWS (Nov. 26, 2012), http://www.nbcnews.com/technology/technolog/facebook-policy-change-results-hysteria-hoax-1C7206892.

[13] *See, e.g.*, Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1557 (2010) (stating that "intermediated communications technologies empower the police," and that Facebook provides "a permanent archive" that waits "for the police to come along, where once [the information] would have disappeared"); *see also* Edward M. Marsico, Jr., *Social Networking Websites: Are MySpace and Facebook the Fingerprints of the Twenty-First Century?*, 19 WIDENER L.J. 967, 968 (2010) ("Police officers routinely use social networking sites to investigate crimes and those suspected of committing crimes."); Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 292 (2011) (noting that "even when the government lacks reasonable suspicion of criminal activity and the user opts for the strictest privacy controls, Facebook users still cannot expect federal law to stop their 'private' content and communications from being used against them").

[14] REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM (2012).

[15] *Id.* at xx.

[16] *Id.* at xxi.

[17] Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 105 (2010).

[18] Siegfried Wiessner, *Legitimacy and Accountability of NGOs: A Policy-Oriented Perspective*, *in* FROM GOVERNMENT TO GOVERNANCE? 2003 HAGUE JOINT CONFERENCE ON CONTEMPORARY ISSUES OF INTERNATIONAL LAW 95 (W.P. Heere ed., 2004), *reprinted in* W. MICHAEL REISMAN ET AL., INTERNATIONAL LAW IN CONTEMPORARY PERSPECTIVE 305 (2004).

scrutinizes some of the most powerful entities acting as central access points for internet content.

The central role played by powerful internet intermediaries—and the government-like power some exercise—is further underscored by a recent book, *The New Digital Age*,[19] jointly authored by Google chairperson Eric Schmidt and Washington insider Jared Cohen.[20] A search of the book's main text shows that the word "power" and variants thereof appear *142 times*, whereas the phrases "human right" or "human rights" appear only *four times*.[21] Whereas Schmidt and Cohen appear to be optimistic about the power of technology as a problem-solver,[22] others are more skeptical, such as author Evgeny Morozov, who chides what he calls the "Google Doctrine," an "enthusiastic belief in the liberating power of technology accompanied by the irresistible urge to enlist Silicon Valley start-ups in the global fight for freedom."[23] Similarly, Professor Siva Vaidhyanathan criticizes Google for engaging in the sin of hubris through "techno-fundamentalism," i.e., "the notion that you can always invent something to solve the problem that the last invention created."[24] Rebecca MacKinnon would agree, noting that putting too much faith in technology as a remedy against "repression can cause individuals to abdicate individual responsibility."[25]

Such concerns are becoming central to the study of cyberlaw. Professor Jacqueline Lipton notes that when "one intermediary holds a dominant position in" its niche, "the *power* of that intermediary may warrant significant scrutiny."[26] She therefore proposes that

---

[19] ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS (2013).

[20] *Id.*

[21] Search done using electronic edition of book, screenshots of searches on file with author.

[22] *See* SCHMIDT & COHEN, *supra* note 19, at 11.

[23] EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM xiii (2011).

[24] VAIDHYANATHAN, *supra* note 5, at 76.

[25] MACKINNON, *supra* note 14, at 236.

[26] Jacqueline D. Lipton, *Law of the Intermediated Information Exchange*, 64 FLA. L. REV. 1337, 1344 (2012) (emphasis added). Not surprisingly, Professor Lipton also makes passing reference to the line "With Great Power Comes Great

cyberspace law be rearticulated as "the law of the intermediated information exchange," placing primary focus on third-party intermediaries.[27] She further suggests that the future of cyberlaw "should revolve around detailed analysis of the legal *responsibilities* of Internet intermediaries in many contexts."[28] Professor Derek Bambauer similarly notes the need for new scholarship that provides "methodologies for grouping intermediaries."[29] This article attempts to address such concerns, limiting its discussion to powerful internet intermediaries that provide hosting or search services, and considering the nature of their power and attendant responsibilities.[30]

A study of the nature of intermediary power is a worthwhile effort. As MacKinnon points out, even though we depend on powerful internet intermediaries and we may understand "how power works in the physical world, . . . we do not yet have a clear under-

---

Responsibility" in a sub-heading in an unpublished manuscript she wrote and which I reviewed after selecting the same quote to open this article. *See* Jacqueline D. Lipton, *Cyberlaw 2.0*, at 10, *available at* http://works.bepress.com/jacqueline_lipton/12. Indeed, as the field of cyberlaw coalesces around the role of intermediaries, questions of power will likely emerge that transcend more parochial concerns such as intellectual property. *See also* Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393 (2013) [hereinafter Land, *Law of Internet*].

[27] Lipton, *supra* note 26, at 1338.

[28] *Id.* at 1367 (emphasis added).

[29] Derek E. Bambauer, *Middlemen*, 65 FLA. L. REV. FORUM 1, 3 (2013) [hereinafter Bambauer, *Middlemen*].

[30] A similarly narrow focus is taken in an article by Professors Citron and Norton, who limited their analysis to content hosts and search/application providers. *See* Citron & Norton, *supra* note 8, at 1439 n.21. Although much of what this article addresses may apply to conduit providers such as Verizon and AT&T, this article generally limits its analysis to intermediaries that interface more visibly and directly with internet users by providing top-layer services, such as content hosting, searching tools, and applications. This is not to say that backbone ISPs providing conduit and similar services are not powerful and do not bear especial responsibilities. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (stating that "nothing in society poses as grave a threat to privacy as the ISP, not even Google"); Pasquale, *supra* note 17, at 112 (citing Ohm, and noting the great threat to privacy posed by ISPs because they can collect data on everything users do online).

standing of how power works in the digital realm."[31] This article addresses such power. Although the internet includes numerous intermediaries, some providers stand far above the others.[32] For example, YouTube is paradigmatic of a new breed of internet intermediary, the *Super-Intermediary*, one that has especial degrees of user involvement, is subject to intensive legal scrutiny, and possesses a reputation as well-known as some of the most famous celebrities.[33]

As a powerful intermediary, YouTube faces constant recriminations and demands for takedown, but perhaps none more discussed than the 2012 controversy over the video *Innocence of Muslims*, a video that ultimately led—directly or not—to numerous acts of violence and death in the Middle East. YouTube ultimately blocked

---

[31] MACKINNON, *supra* note 14, at 13.

[32] "The trend toward globalized platforms like Facebook and Google creates a system for technology that is more likely to spread." SCHMIDT & COHEN, *supra* note 19, at 92.

[33] *See infra* Part I.B. Regarding the chosen terminology, it should be noted that Professor Robert Heverly uses the term in a different way, discussing *law* as a "Super Intermediary," arguing the law can have, for example, a "stopping effect" that prevents content from getting from producer to receiver, or a "forcing effect" that requires its modification. Robert A. Heverly, *Law as Intermediary*, 2006 MICH. ST. L. REV. 107, 120-21, 124 (2006). Thus, "Law is a Super Intermediary, one that can only be legally avoided on its own terms. Other intermediaries may be avoided without violating the law, but not the law as intermediary itself. There, only by meeting law's terms can its intermediary effects be avoided." *Id.* at 128.

Other legal scholars have also made reference to "super-intermediaries" in a variety of non-internet contexts. *See* Jonathan M. Barnett, *Intellectual Property as a Law of Organization*, 84 S. CALIF. L. REV. 785, 824 (2011) (referring to "the monolithic superintermediary that occupies a single node of the supply chain"); Tamar Frankel, *Cross-Border Securitization: Without Law, but not Lawless*, 8 DUKE J. COMP. & INT'L L. 255, 259 (1998) (noting how unbundling of banking services formerly provided by one banking "super-intermediary" allows multiple actors to become involved); Saul T. Omarova, *The Quiet Metamorphosis: How Derivatives Changed the "Business of Banking"*, 63 U. MIAMI L. REV. 1041, 1047 (2009) (describing the "largest U.S. commercial banks to emerge, in the last twenty plus years, as a new breed of financial super-intermediary"). This is unsurprising, as early scholarship on intermediaries arose in the context of the banking industry. Heverly, *supra*, at 108 n.1; *cf. also* Samuel Issacharoff & Daniel R. Ortiz, *Governing Through Intermediaries*, 85 VA. L. REV. 1627, 1631 (1999) (noting that some political actors are powerful "superagents" that "introduce a whole new set of possible agency costs").

the video in a number of countries, though not in the United States, despite the "suggestion" of the Obama administration that the video ought to be taken down.[34] To be clear, the *Innocence of Muslims* video is both offensive and absurd. As discussed below,[35] the video intentionally mocks the prophet Muhammad, and led to tragic real-world results. One focus of this article, then, is whether human rights law might provide guidance to Super-Intermediaries such as YouTube when faced with a social, cultural, or political "hot potato" like *Innocence of Muslims*.

Importantly, this article bypasses the question of whether corporations are actually bound by international human rights law.[36] Rather than asking whether human rights law can be enforced against intermediaries, the article asks whether human rights law can provide meaningful guidance to corporate intermediaries so that they can act

---

[34] *See infra* Part II.D.

[35] *See infra* Part II.

[36] As Professor Ralph Steinhardt notes, "[i]n international human rights law, the bedrock principle of state responsibility traditionally places a comprehensive obligation on governments to protect human rights and either imposes no obligations on non-state actors like corporations or imposes obligations only in extraordinary circumstances defined by international agreement." Ralph G. Steinhardt, *Soft Law, Hard Markets: Competitive Self-Interest and the Emergence of Human Rights Responsibilities for Multinational Corporations*, 33 BROOK. J. INT'L L. 933, 933 (2008); *see also* Jonathan Bellish, *Towards a More Realistic Vision of Corporate Social Responsibility Through the Lens of the Lex Mercatoria*, 40 DENV. J. INT'L L. & POL'Y 548, 563 (2012) (citing Steinhardt, *supra*). *But see* Land, *Law of Internet*, *supra* note 26, at 445 (arguing that human rights provision regarding freedom of expression applies directly to non-state actors such as internet intermediaries).

Professor Anupam Chander notes that "[w]hile many have denounced Google, Microsoft, and Yahoo for betraying their obligations to the people of China and other repressive regimes through complicity with state repression, no one has yet explained why these companies might owe obligations to distant peoples." Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 6 (2011); *see also* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD 208 (2013) (noting that "human rights, cultural norms, privacy and security are all at risk" in today's networked world). Another author evokes a variant of the "great power" quotation, noting that the arguments in favor of applying human rights to corporations include "the notion that 'power must be balanced by responsibilities.'" JENNIFER A. ZERK, MULTINATIONALS AND CORPORATE SOCIAL RESPONSIBILITY: LIMITATIONS AND OPPORTUNITIES IN INTERNATIONAL LAW 77 (2006).

in a socially responsible manner.[37] As the article will suggest, there

[37] Such concerns have been a part of the dialogue concerning Internet governance for some time. For example, Professor Milton Mueller points to NGOs focused on civil liberties and human rights as one of the major issue networks that converged in WSIS. *See* MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 88-89 (2010) (giving examples of NGOs that "apply human rights principles specifically to communication-information technology," such as the European Digital Rights Initiative, Article 19, EPIC, and others).

Along similar lines, corporate social responsibility (CSR) regarding human rights values is extremely important. In 2003, the U.N. Human Rights Subcommission noted "that even though States have the primary responsibility [for] human rights, transnational corporations and other business enterprises, as organs of society, are also responsible for promoting and securing the human rights set forth in the Universal Declaration of Human Rights." Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights, U.N. Doc. E/CN.4/Sub.2/2003/12/Rev.2 (2003), *available at* http://www1.umn.edu/humanrts/links/norms-Aug2003.html; *see also* James P. Kelly, III, *Multinational Businesses and the Matrix of Human Rights Governance Networks*, 12 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 71, 72 (2011) (noting documents regarding corporations). Also relevant is the United Nations Global Compact's *Ten Principles of Corporate Social Responsibility*, which has been characterized as the "most comprehensive and legally significant instrument detailing the contents" of corporate social responsibility. Bellish, *supra* note 36, at 560; *see also* United Nationals Global Compact, *The Ten Principles*, http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/ (last visited Apr. 17, 2013). The Global Compact arose from a drive by the Secretary-General to persuade "world business leaders to *embrace and enact* a Global Compact" to ensure that companies: 1) neither commit nor become complicit in human rights abuses; and 2) support appropriate public policies. ANDREW CLAPHAM, HUMAN RIGHTS OBLIGATIONS OF NON-STATE ACTORS 218 (2006) (emphasis in original).

Much has been written on CSR and human rights. "The concept of CSR refers to a corporation's responsibility to protect the fundamental rights of its employees and consumers as specified in the Universal Declaration of Human Rights, which was adopted by the United Nations General Assembly in 1948." Marie Nissanka, *Book Review: A. Voiculescu and H. Yanacopulos, Eds., The Business Of Human Rights: An Evolving Agenda For Corporate Social Responsibility (Zed Books, 2011)*, 6 INTERDISC. J. HUM. RTS. L. 167, 167 (2012); *see also* Larry Catá Backer, *Transparency Between Norm, Technique and Property in International Law and Governance: The Example of Corporate Disclosure Regimes and Environmental Impacts*, 22 MINN. J. INT'L L. 1, 22 (2013) (stating that "corporate responsibility to respect human rights is based on the social norm obligations of corporations which is defined substantively by the International Bill of Human Rights" and a number of International Labor Organization core conventions).

can be little doubt that most major western intermediaries value acting in such a manner.[38] This is not to say, however, that they cannot do better.

Additionally, the article avoids making express normative claims about *which* human rights ought to trump others.[39] Indeed, the *Innocence of Muslims* video provides a paradigmatic example of a "hard" case, a seemingly intractable clash between the values of freedom of expression and concerns in Islamic countries regarding defamation of religion. Put differently, *Innocence of Muslims* may present a form of speech that may generally be considered to be offensive, but not universally offensive.[40] In the United States, such speech would likely be protected under the First Amendment. In other parts of the world, such speech might similarly be considered offensive but still tolerated under the law because of other values such as freedom of expression. But in some parts of the world, concerns over defamation of religion might trump freedom of expression, rendering such speech intolerable.

Accordingly, how one balances a set of values can vary tremendously depending on one's region, religion, and culture. This is not to say that other examples might not be worth addressing, such as varying treatments of speech concerning homosexuality, hate speech, or anti-Semitism. However, the *Innocence of Muslims* video is exceptional as a watershed event in the history of the Internet, where

---

[38] *See* Chander, *supra* note 36, at 7 ("Even without a theory of obligation, new media enterprises have sought to improve their human rights practices, especially in China."); *see also* Peter Muchlinski, *Corporate Social Responsibility and International Law: The Case of Human Rights and Multinational Enterprises*, *in* THE NEW CORPORATE ACCOUNTABILITY: CORPORATE SOCIAL RESPONSIBILITY AND THE LAW 436 (Doreen McBarnet et al. eds. 2007) ("The observance of fundamental human rights can be said to lie at the heart of ethical business practice.").

[39] *See* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 384-86 (2009) [hereinafter Bambauer, *Cybersieves*] (noting unhelpfulness of using U.S. speech standards); *see generally* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863 (2012) [hereinafter, Bambauer, *Orwell*].

[40] Thanks to Professor John Makdisi for pointing out the distinction between speech that is universally understood to be offensive *and* impermissible, and scenarios where there are variations in the levels of social offensiveness and legal impermissibility. In using the word "offensive," the article speaks in general terms rather than in terms of First Amendment jurisprudence.

a video posted to a private intermediary caused an international outcry, including numerous instances of violence. It shined a light onto the ever-increasing power of internet intermediaries, and how their conduct may rival that of nation-states in terms of their ability to shape international affairs. As a "perfect storm," the video practically screams out for an examination of the emerging power of such entities.

Accordingly, the article will treat *Innocence of Muslims* as a test case. Further, rather than choosing which substantive rights or values might trump others, the article will instead attempt to make descriptive claims about problems with the *procedures* used by powerful intermediaries, as well as normative claims about process-based principles that might better foster human rights values. In so doing, the article will craft a framework for identifying Super-Intermediaries, address *Innocence of Muslims* as a paradigmatic example of the challenges such intermediaries face, review human rights law as a potential solution, and finally, consider a variety of approaches that might be taken by powerful internet intermediaries when they grapple with the seemingly intractable problems of incendiary speech.[41]

Part I introduces the author's conception of Super-Intermediaries. It provides a framework that looks to relevant stakeholders, namely, the relationship between users and intermediaries, the types of legal actors that shape an intermediary's conduct, and the strength of an intermediary's reputation. Part I also explores the theoretical underpinnings of the stakeholder framework, and the benefits of identifying Super-Intermediaries.

Part II then turns to a particularly vexing test case for Super-Intermediaries, namely, the *Innocence of Muslims* video. After discussing the history and nature of the video, the article scrutinizes

---

[41] Thus, the article's approach is consistent with the "New Haven School of Jurisprudence" approach, which uses inter-disciplinary analysis to: 1) review the social problem at hand; 2) consider conflicting interests; 3) analyze past legal treatments; 4) predict future treatments; and 5) to assess past treatments, consider alternatives, and recommend solutions aimed at a "public order of human dignity." Siegfried Wiessner, *The New Haven School of Jurisprudence: A Universal Toolkit for Understanding and Shaping the Law*, 18 ASIA PAC. L. REV. 45, 48 (2010).

YouTube's selective censoring of the video, including the technology—i.e., the *code*[42]—that YouTube apparently used to selectively block the video in some parts of the globe.

Part III then turns to human rights law, particularly the Universal Declaration of Human Rights (UDHR),[43] the International Covenant on Civil and Political Rights (ICCPR),[44] and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[45] After noting portions of these documents that may provide analogous guidance regarding self-regulation of online speech by intermediaries such as YouTube, the article asks whether these documents provide a useful foundation for Super-Intermediary decision-making in difficult cases of disputed content. Also, Part III further explores a notable example of private self-ordering, the Global Network Initiative, an organization consisting of major internet

---

[42] To be certain, "code" is an amorphous term, possibly referring to underlying internet architecture such as core protocols and the domain name system, along with the hardware used to route internet communications. It could also refer to higher-level protocols, such as the HTTP protocol that makes possible the World Wide Web. It could further refer to the websites and applications that sit on top of such protocols, such as Facebook and Twitter. All such types of "code" are relevant to this article, and a suitable definition of "code" might be the one provided by Professor Lawrence Lessig: "The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave." Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 509 (1999). Accordingly, "code" governs the expression that people may make or access in different parts of the world. For example, software filtering can block certain kinds of speech automatically, such as pornography or copyright infringement. Alternatively, a user's "Internet Protocol" address might be identified to permit an intermediary to provide different experiences for users from different parts of the world, thus blocking expression in one area that is accessible in another. *See generally infra* Part IV.B (addressing how code can be used to geographically tailor a user's experience).

[43] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc A/810 at 71 (1948), *available at* http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=eng [hereinafter UDHR].

[44] International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171, *available at* http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx [hereinafter ICCPR].

[45] International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3, *available at* http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx [hereinafter ICESCR].

companies as well as academics, and which proposes using a subset of human rights principles regarding freedom of expression and privacy to guide member conduct.[46]

Part IV then focuses on the *codes* and *processes* that Super-Intermediaries use to control disputed information. Unfortunately, it appears that much development of intermediary law, along with such code, has been fueled not by concerns over speech, but instead by fear of intellectual property piracy. Accordingly, many of the procedures used by Super-Intermediaries appear to be poorly suited to disputes such as those raised by *Innocence of Muslims*.

Part V addresses these concerns from a broader perspective. It considers a number of possible solutions, such as doing nothing different, creating stakeholder communities, creating dispute-resolution bodies, and using code such as automated filters. Finding each of these solutions to be problematic, the article ultimately concludes that the problem might be better addressed by processes that put a more demanding burden on Super-Intermediaries. In other words, it is time for *Digital Due Process*. Through such principles, Super-Intermediaries may better foster human dignity.

I. Super-Intermediaries

The development of Super-Intermediaries—in essence, the most powerful of the internet intermediaries—is not surprising, considering the consolidation that naturally takes place in many industries. At the beginning of the internet era, online services for individual users were provided by a myriad of entities, such as universities, local providers, and others, and such services continue to be provided by such entities today. Although there were notable early attempts at providing platform services, such as CompuServe, Prodigy, and especially AOL, dedicated "one-stop" platforms were later superseded by the lure of websites. This led to incredible expansion in the amount of information online. As Professor Yochai

[46] GLOBAL NETWORK INITIATIVE, http://globalnetworkinitiative.org (last visited July 14, 2013).

Benkler notes, internet users solved the "information overload" problem by eventually "congregating in a small number of sites."[47] Over time, the interactivity allowed by online intermediaries has expanded significantly, leading to today's so-called "Web 2.0" and social networks.[48]

Part I first examines definitions for "Web 2.0" and "social media/networks." Concluding that such definitions are *functional* and not helpful in analysis, Part I then proposes a descriptive *stakeholder* framework for identifying Super-Intermediaries, along with a number of features that might be prevalent in powerful intermediaries. Finally, Part I explains the theoretical underpinnings of the framework, and makes a number of observations regarding the nature and importance of identifying Super-Intermediaries.

A. More than "Web 2.0" or Social Media

Although the definition of "Web 2.0" is subject to debate, a fair definition might be a more "user-friendly" version of the Web, which "can encourage more active user interaction, involvement and participation in generating content and in creating a less generic interface."[49] This may "involve: (1) the development of internet-

---

[47] YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 241 (2006); *see also* Ira S. Nathenson, *Internet Infoglut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 HARV. J. L. & TECH. 43, 51-54 (1998) (explaining "infoglut").

[48] Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY (Sept. 3, 2005), http://oreilly.com/web2/archive/what-is-web-20.html.

[49] Warren B. Chik, *Paying it Forward: The Case For a Specific Statutory Limitation on Exclusive Rights for User-Generated Content Under Copyright Law*, 11 J. MARSHALL REV. INTELL. PROP. L. 240, 244 (2011); *see also* O'Reilly, *supra* note 48. Some credit Tim O'Reilly with coining the term "Web 2.0." Gillian K. Hadfield, *Legal Infrastructure and the New Economy*, 8 I/S: J. L. & POL'Y FOR INFO. SOC'Y 1, 15 n.26 (2011). In turn, O'Reilly's definition for Web 2.0 says to "[b]uild applications that harness network effects to get better the more people use them," or to "harness[] collective intelligence." O'Reilly Radar, *Web 2.0 Compact Definition: Trying Again*, http://web.archive.org/web/20090123232944/http://radar.oreilly.com/archives/2006/12/web-20-compact.html (last visited Feb.

based applications that are more user-centric in design; (2) increasing engagement in user collaboration; and the encouragement of both original and derivative [user-generated content]."[50] According to one author:

> The main feature of Web 2.0 is this focus on the de-centralization of power, individual engagement, developing a 'digital society,' and 'grassroots culture building' in the internet environment. Web 2.0 describes a change in the nature and a shift in the social dynamics of the WWW rather than any technical changes in the internet infrastructure itself. Web 2.0, thus, encompasses the practices of social networking, blogging, video sharing, music mash-ups, and other user-centric activities involving the user as a creator. The application platforms supporting such activities require a greater role to be played by internet intermediaries, through the development of facilitative forms of web-based services technology and functions.[51]

Attempts to define "social media" or "social networks" lead to similarly broad definitions. A government site says that "[t]hrough social media, people or groups can create, organize, edit, comment on, combine, and share content," listing examples such as blogs, social networks, microblogs, wikis, video, podcasts, and more.[52] Professor Spencer Weber Waller notes that "[t]here are many definitions for social networking or social networking sites."[53]

23, 2013).

[50] Chik, *supra* note 49, at 244.

[51] *Id.* at 245 (footnotes omitted).

[52] HowTo.gov, *Types of Social Media*, http://www.howto.gov/social-media/social-media-types (updated Nov. 26, 2012).

[53] Spencer Weber Waller, *Antitrust and Social Networking*, 90 N.C. L. REV. 1771, 1776 (2012). As a commonly cited example, Professor Waller points to boyd [sic] and Ellison's definition: social networks are "[W]eb-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the

Another source suggests that "the definition is not so clear-cut," and "social networking sites tend to have an 'I'll know it when I see it' flavor."[54]

B. What are Super-Intermediaries?

The distinctions between Web 2.0 and social media provided above are not very clear. From a regulatory standpoint, they are not particularly helpful, either. Both definitions take a *functional* approach, describing certain intermediaries by how they work and how people use them. Put differently, such intermediaries are primarily defined as *things*, with primary focus on an intermediary's architecture and technology, and without sufficient consideration of the roles the intermediaries play for a broader set of relevant stakeholders in society. Thus, descriptions focused on "Web 2.0" or "social media" may fail to paint a picture sufficiently complete for those who would seek to impose obligations—whether social, moral, or legal—on internet intermediaries. Moreover, the definition of Web 2.0 is anomalous for today's world where much speech is funneled through a few intermediaries. If Web 2.0 was an age of "the decentralization of power,"[55] then *power* is becoming recentralized in Super-Intermediaries.

It might be more helpful to instead look at intermediaries from the perspective of key third-party *stakeholders*, and to consider how differing stakeholders interact with and react to prominent intermediaries. Such stakeholders may be an intermediary's users, governmental actors, claimants against the intermediary or its users, and the general public. As suggested below, certain Super-Intermediaries may be qualitatively different from normal Web 2.0

---

system." *Id.* (quoting danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html).

[54] Catherine Tucker & Alexander Marthews, *Social Networks, Advertising, and Antitrust*, 19 GEO. MASON L. REV. 1211, 1213 (2012) (citing Waller, *supra* note 53).

[55] Chik, *supra* note 49, at 245.

or social networking platforms, although the differences may sometimes be in degree rather than in function.[56] Thus, the key difference between an ordinary intermediary and a Super-Intermediary may be in the intermediary's power.[57]

Nine stakeholder features—many or all of which may exist to a high degree in a powerful Super-Intermediary—are:

- Interactivity
- Networking
- Personalization
- Governmental legal scrutiny
- Private legal scrutiny
- Internal legal scrutiny
- Political activity
- Ubiquity
- Hero/villain ambiguity

As shown by Table 1 below, these nine features can be further categorized as follows via the umbrella categories of: 1) users, namely, the user experience; 2) legal actors, namely, the sources and types of legal scrutiny; and 3) reputation, namely, how others perceive the intermediary.

---

[56] As noted, other scholars have used variations of the term Super-Intermediary, typically in the banking context. *See supra* note 33. Professor Heverly suggests that *law* as "Super Intermediary" "can only be legally avoided on its own terms. Other intermediaries may be avoided without violating the law, but not the law as intermediary itself." Heverly, *supra* note 33, at 128. Here, a "Super-Intermediary" need not be one that *cannot* be avoided: it suffices that Super-Intermediaries such as Google, YouTube, Facebook, and Twitter are the key "players" in town if a user wants to effectively engage in the type of services offered.

[57] *See* Robert W. Gehl, *What's on Your Mind?: Social Media Monopolies and Noopower*, 18 FIRST MONDAY 3 (Mar. 4, 2013), *available at* firstmonday.org/ojs/index.php/fm/article/view/4618/3421 (arguing that "social media's linkages with marketing and state power imbricates these sites as special layers in the protocological stack of contemporary informational capitalism").

Table 1: Three Categories of Super-Intermediary Features

Users	**Legal Actors**	**Reputation**
Interactivity	Governmental	Political activity
Networking	Private	Ubiquity
Personalization	Internal	Hero/villain ambiguity

The three subsections below will describe each feature and provide illustrative examples.[58] The article will then seek to justify for the reader the theoretical basis for the framework, the features chosen, and why it is useful to identify Super-Intermediaries.[59]

1. User Relationship

Considering that an intermediary *intermediates* between users and others, the nature and quality of the relationship between the two is a critical factor in concluding whether a provider is a Super-Intermediary. This subsection looks to interactivity, networking, and personalization.

a. Interactivity

First, Super-Intermediaries provide a high degree of *interactivity*,[60] whether through websites or applications. Thus, the services provided by internet intermediaries are now much more varied than simply providing internet connectivity.[61] Many of today's interme-

[58] *See infra* Parts I.B.1 to I.B.3.

[59] *See infra* Part I.C.

[60] *Cf.* Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) (holding that personal jurisdiction may be obtained more easily over commercially interactive websites).

[61] This development was arguably anticipated back in the early days of internet regulation. For example, the definition of "service provider" in the Copyright Act's notice and takedown statute includes both a traditional definition regarding "transmission, routing, or providing" online communications, and a much broader definition, "a provider of online services or network access." 17

diaries *are* the focus of networked user interaction. People use Facebook to connect to their network of friends, to view information such as friends' updates, and to post information such as status updates. Thus, while people still use their local telephone or cable company as intermediaries to *access* the internet, they use that access to then *use* the services of intermediaries such as Facebook, YouTube, and Twitter.[62] Interestingly, although Super-Intermediaries often have a particularly high degree of interactivity, they need not be directly commercial to obtain "super" status. Even though YouTube, Facebook, and Twitter have various mechanisms through which they monetize their services, they do not charge users directly. Indeed, as discussed later, "free" may be one of the keys to attaining Super-Intermediary status.[63]

b. Networking

Second, a Super-Intermediary tends to foster *networking*.

U.S.C. § 512(k)(1) (2010). Courts have had little trouble concluding that a variety of online services qualify as "service providers" under the second definition. *See* Ira S. Nathenson, *Looking for Fair Use in the DMCA's Safety Dance*, 3 AKRON I.P.J. 121, 135-36 n.73 (2010) (collecting cases) [hereinafter Nathenson, *Safety Dance*]. Although the definition under the Communication Decency Act (CDA) of "interactive computer service" seems to focus more on basic access-providing, courts have similarly had no difficulty applying the CDA's immunity provision to protect a wide swath of service providers from liability for defamation and other claims. *See* 47 U.S.C. § 230(f)(2) (2000) (defining "interactive computer service" as "any information service . . . that provides or enables computer access by multiple users to a computer server . . ."); *see also* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) (noting that "courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of 'interactive computer service,'" and therefore immunizing online dating service); Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 801 (N.D. Cal. 2011) (holding that Facebook is an interactive computer service); Gentry v. eBay, Inc., 99 Cal. App. 4th 816, 831 n.7 (2002) (holding that eBay is an interactive computer service).

[62] Once when Google's services suffered a short outage, worldwide internet traffic dropped by 40%. *See* Neil McAllister, *Google Goes Dark for 2 Minutes, Kills 40% of World's Net Traffic*, THE REGISTER (Aug. 17, 2013), http://www.theregister.co.uk/2013/08/17/google_outage/.

[63] *See infra* text accompanying notes 159-63.

This feature overlaps somewhat with interactivity but is still different. Interactivity does not require networking: indeed, many people use the internet to interact with websites and blogs without ever forming social contacts or networks with other users of a site. In contrast, networking requires users to form personal or professional networks.[64] Networkability is the hallmark of Facebook, its *raison d'être*. Thus, a Facebook user can create a network of friends, even though each person friended has a different network. Although some Facebook users leave their profiles completely open to the public, most users appear to limit full access to approved "friends." Twitter is also networkable, but to a lesser degree than Facebook. A Twitter user can "follow" another user's postings, known as "tweets."[65] Indeed, Twitter users often strive for a large number of followers.[66] However, unlike Facebook, many Twitter users leave their feeds of tweets fully public, permitting others to view the tweets without having to follow anyone.[67] YouTube is perhaps closer to Twitter than Facebook in terms of networkability. YouTube permits the creation of channels to which others can subscribe. Some such channels are popular and may eventually reach the strength of television networks.[68] However, like Twitter, many users make their

---

[64] Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479 (1998).

[65] Thus, unless a Twitter user makes her or his tweets private, others may subscribe. My public Twitter feed is available at http://twitter.com/nathenson. A Twitter user may also create public lists of other Twitter users, to which others can subscribe. For instance, I have created a number of public lists available at http://twitter.com/nathenson/lists.

[66] *See, e.g.*, Katie Heaney & Louis Peitzman, *How To Actually Get More Twitter Followers*, BUZZFEED (Mar. 5, 2013), http://www.buzzfeed.com/katieheaney/how-to-actually-get-more-twitter-followers. A high follower count is so valued that a market has emerged to create fake Twitter followers. *See* Nicole Perlroth, *Fake Twitter Followers Become Multimillion-Dollar Business*, N.Y. TIMES BITS BLOG (Apr. 5, 2013), http://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/.

[67] Indeed, Twitter may be used passively by a person who merely reads the feed of another. Or Twitter may be used interactively by someone who retweets or replies to a posting. Or it may also be used to build a network of followers and followees. And of course, many people use Twitter in a variety of these ways.

[68] Perhaps that "tipping point" has already arrived. In October 2012, eight

videos publicly available, reducing the impetus for others to follow another user.

c. Personalization

Third, a Super-Intermediary tends to provide significant opportunities for *personalization* of its services. Thus, Facebook users have significant control over what information goes on their profiles, and get to select which postings they "like." Twitter users not only post 140-character "tweets," but also can follow others, be followed, and create and appear in user-generated lists. Similarly, via a user's account ID or via cookies stored on the user's device,[69] intermediaries such as YouTube, Amazon, Facebook and eBay can customize their recommendations based on the history or preferences of the user. Such individualization has its benefits and drawbacks, of course, such as the case of "personalized" search engine results.[70]

---

million people watched live-streaming on YouTube of Felix Baumgartner's record jump from the edges of outer space. Dorothy Pomerantz, *Felix Baumgartner and the YouTube Tipping Point*, FORBES (Oct. 15, 2012), http://www.forbes.com/sites/dorothypomerantz/2012/10/15/felix-baumgartner-and-the-youtube-tipping-point/.

[69] Cookies "are small, often encrypted text files, located in browser directories [that] are used by web developers to help users navigate their websites efficiently and perform certain functions," such as storing a user's preferences or storing information about a user's activities. ALL ABOUT COOKIES, http://www.allaboutcookies.org/ (last visited July 15, 2013).

[70] *See* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1186-88 (2008) (noting that personalized search can both avoid and foster search engine manipulation); Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 YALE J. L. & TECH. 188, 198 (2006) (arguing that "[p]ersonalized ranking algorithms represent the next major advance in search relevancy"); Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151, 1215 (2006) (noting potential consumer benefits of individualized search, but suggesting that "Coasean-filter-like technology" be used to "store the consumer's dataset on the device itself rather than in central third-party-operated repositories"); Greg Lastowka, *Google's Law*, 73 BROOK. L. REV. 1327, 1365-66 & n.187 (2008) (noting difficulties of current search technology for terms that have divergent meanings, and noting that personalized search may "eventually increase the contextual cues Google can bring to search queries"); Pasquale, *supra* note 17, at

It should be noted that the first three features—interactivity, networking, and personalization—seem at first glance to overlap with descriptions of "social networks" and "Web 2.0." To some extent that may be so. However, the importance of these features in the present context is not how the features *work*, but how each contributes to the relative perception of the provider as a Super-Intermediary. Indeed, by themselves, these features do not guarantee Super-Intermediary status, as can be demonstrated by considering the numerous social networks that have never risen to Super-Intermediary status, such as Friendster and as of this writing, probably LinkedIn.[71] MySpace may at one point have been a Super-Intermediary, but its demise as a popular platform reduces its contemporary power. Instagram (which is owned by Facebook) might be considered an up-and coming Super-Intermediary, as might Twitter-owned Vine.[72] But a Super-Intermediary needs more than functional interactivity: it needs to attract legal scrutiny,[73] and it needs to have a sufficiently notorious reputation.[74]

2. Legal Scrutiny

Intensive legal scrutiny is an additional indicator of Super-Intermediary status.[75] This is a likely result of the great power of the

---

116-17 (noting concerns such as inaccurate searches due to an overly trained profile).

[71] *See* Sorav Jain, *40 Most Popular Social Networking Sites of the World*, SOCIAL MEDIA TODAY (Oct. 6, 2012), http://socialmediatoday.com/node/195917 (listing sites).

[72] Oliver Duggan, *Facebook's Instagram Beats Twitter's Vine in the War of the Micro-Film Apps*, THE INDEPENDENT (June 28, 2013), http://www.independent.co.uk/life-style/gadgets-and-tech/facebooks-instagram-beats-twitters-vine-in-the-war-of-the-microfilm-apps-8679057.html.

[73] *See infra* Part I.B.2.

[74] *See infra* Part I.B.3.

[75] Notably, Professor Robert Heverly makes the intriguing descriptive claim that *law* itself can be a Super-Intermediary. *See* Heverly, *supra* note 33, at 127-29. Heverly rejects the conventional wisdom that an intermediary must have volition. *Id.* at 110-11. This is an interesting claim, and one that may be consistent with the framework laid out here. Indeed, arguments may be made that *law* itself is some-

intermediary, combined with the concerns of lawmakers and the public to constrain the provider. Considering that Super-Intermediaries wield exceptional power over people's online presence and over information, such providers have come under greater scrutiny due to concerns such as intellectual property, privacy, anti-trust, and other matters of public concern. This subsection looks to governmental, private, and internal legal scrutiny.

a. Government

The first type of legal scrutiny comes from the *government*. Here, the constraints may come in a variety of forms, particularly legislative proposals and executive action. Interestingly, early in the Internet era, some of Congress' actions were aimed at fostering the development of service providers. Thus, Title II of the Digital Millennium Copyright Act of 1998 (DMCA) was created to *foster* the development of internet services, doing so by creating qualified safe harbors from copyright liability.[76] Similarly, portions of the Communications Decency Act of 1996 (CDA) were passed for similar reasons, out of concerns over defamation liability.[77] More recently,

---

thing that is interactive (people engage in the law-making process and legal system), individualized (through individual cases), and networkable (through the structure of the court system, for example). Equally so, law could be said to be subject to legal actors: the government (through the law-making, law-execution, and law-interpretation roles of the three branches), private actors (through those who seek to enforce, establish, modify, or establish law), and internally (through devices such as separation of powers, judicial review, and appellate review). Finally, there is little doubt that law has a strong reputation, considering the power of violence that law wields, the ubiquity of the law (as evidenced by the many television shows about the law), and the law's ever-unclear status as hero or villain.

[76] Online Copyright Infringement Liability Limitation Act, Pub. L. No. 105-304, Title II, § 202(a), 112 Stat. 2877 (1998) (codified as amended at 17 U.S.C. § 512 (2010)).

[77] Communications Decency Act of 1996, Pub. L. No 104-104, Title I, § 509, 110 Stat. 137-38 (1996) (codified as amended at 47 U.S.C. § 230). This act has since been often interpreted to provide immunity to interactive computer services from defamation and other liability. *See, e.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

however, lawmakers have proposed several bills aimed at constraining service providers, particularly the infamous SOPA/PIPA bills of 2012, which aimed to more directly regulate internet service providers, domain name registrars, financial institutions and advertising providers.[78] Large service providers may also be the target of investigations by administrative agencies.[79] A more stunning example of raw governmental action against a Super-Intermediary might be China's cyberattacks against Google and other American companies.[80]

b. Private

The second type, unsurprisingly, is *private* legal scrutiny. Super-Intermediaries have been sued often in matters ranging from small to large. Table 2, below, provides examples of lawsuits asserted against a representative set of service providers. The table lists the number of times each term is listed as a defendant in federal district court filings.[81] The searches were limited to matters concern-

[78] *See infra* text accompanying notes 390-92; *see also, e.g.*, Annemarie Bridy, *Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA*, 30 CARDOZO ARTS &ENT. L.J. 153 (2010); Michael A. Carrier, *SOPA, PIPA, ACTA, TPP: An Alphabet Soup of Innovation-Stifling Copyright Legislation and Agreements*, 11 NW. J. TECH. & INTELL. PROP. 21 (2013); Jared Newman, *SOPA and PIPA: Just the Facts*, PC WORLD (Jan. 17, 2012), http://www.pcworld.com/article/248298/sopa_and_pipa_just_the_facts.html.

[79] *See* Geoffrey Manne, *FTC Ends Google Antitrust Investigation. Critics and Competitors: Move On*, FORBES (Jan. 1, 2013), http://www.forbes.com/sites/beltway/2013/01/03/ftcs-google-antitrust-investigation-was-silly-critics-and-competitors-move-on/ (regarding FTC investigation); *see also* Juergen Baetz, *Google Takes Another Step Toward EU Antitrust Case Settlement*, SILICON VALLEY MERCURY NEWS (Apr. 15, 2013), http://www.economist.com/news/business/21576386-settlement-between-search-firm-and-european-union-takes-shape-try-it-and-see (regarding European Union investigation).

[80] SCHMIDT & COHEN, *supra* note 19, at 108-09 (stating that Google's investigation provided "sufficient evidence" that "the Chinese government or its agents were behind the attack").

[81] The searches were made using Bloomberg Law's docket search, which permits searching by defendant. The searches were limited to federal district court

ing either the power of a provider (antitrust) or concerning the provider's status as an intermediary, namely, defamation/libel/assault and intellectual property (specifically, copyright and trademark).[82] The listing also includes control counter-examples, such as Walmart and Apple. Although both have online presences, Walmart is primarily a retailer. For its part, Apple falls somewhat in a no-mans-land. On the one hand, it is a major provider of hardware such as iPhones, iPads, and Macintosh computers. On the other hand, it provides online services such as the iTunes store, which sells applications. The listing also includes major providers from the Web 1.0 era, such as Geocities, Hotmail, and AOL.

---

dockets over the past five years ending April 18, 2013. This avoided the potential for duplication, since cases removed from state courts might be duplicated. Since the vast majority of cases involving internet intermediaries will likely be filed in or removed to federal district court, a database of such cases would appear to provide the most fruitful place to search. *See* 28 U.S.C. § 1331 (federal-question jurisdiction); *id.* § 1332 (diversity jurisdiction); *id.* § 1338 (patent, copyright, and federal trademark jurisdiction); *id.* § 1441 (removal jurisdiction).

[82] The relevant codes on the civil cover sheet are 320 (Assault, Libel & Slander), 410 (Antitrust), 820 (Copyrights), and 840 (Trademark). Code 830 for Patent was omitted as such claims are less likely tied to an intermediary's status as an intermediary. Even then, these numbers may not accurately reflect lawsuits. First, a search term may show up in the defendant field even if the intermediary is not a defendant. Examples include suits filed against holders of Hotmail email accounts. Thus, the numbers provided in Table 2 may overstate the number of times a particular intermediary has been actually sued. Regardless, the numbers provided may still be useful as an indicator of the number of times an intermediary was sued, either directly or because of the conduct of its users. Second, the searches did not include cases where an intermediary was listed as a plaintiff. Relevant omitted examples might include declaratory judgment actions filed by an intermediary, or Anti-SLAPP suits filed by an intermediary.

It should also be noted that because the statistics are derived from the checkboxes on the federal Civil Cover sheet, the data is limited to those categories. Thus, it is not possible to do a search for other types of arguably relevant claims such as trade secrets or right of publicity. However, it is likely that the vast majority of claims arising from the defendants' status as intermediaries are most likely to be claims for copyright and trademark violations, and to a lesser extent, for defamation. The reason for the likelihood of fewer defamation claims is the Communications Decency Act, which generally immunizes most service providers from defamation claims. *See* 47 U.S.C. § 230(f) (2000); Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

Table 2: Search Terms in Defendant Field of Federal Civil Cover Sheet for Assault (Including Defamation), Antitrust, Copyright, and Trademark

Search term	**Total:**
Walmart OR Wal-mart OR "Wal Mart" OR Walmart.com	178
"Apple Inc." OR "Apple, Inc." OR Apple.com	87
Amazon or Amazon.com	85
Verizon OR "Verizon Wireless" OR Verizon.com OR VerizonWireless.com	85
Google OR Google.com	83
Microsoft OR Microsoft.com	36
eBay or eBay.com	21
AOL or "America Online" or "America On-Line"	18
Facebook OR Facebook.com	17
Yahoo OR Yahoo.com	15
YouTube OR YouTube.com	10
Ripoffreport OR Ripoffreport.com OR "rip off report" or "rip-off report" OR Xcentric	6
Twitter OR Twitter.com	5
"Huffington Post" OR HuffingtonPost.com OR TheHuffingtonPost.com OR "Arianna Huffington"	5
Wordpress OR Wordpress.com OR Automattic OR Automattic.com	5
Wikipedia OR Wikipedia.com OR Wikimedia OR Wikimedia.com	3
Craigslist OR Craigslist.com	2
Hostgator OR Hostgator.com	2
Hotmail OR Hotmail.com	2
Napster OR Napster.com	1
"Drudge Report" OR DrudgeReport.com OR TheDrudgeReport.com OR "Matt Drudge" OR "Matthew Drudge"	1
Tumblr OR Tumblr.com	1
Flickr OR Flickr.com	0
Geocities OR Geocities.com	0

Most of the claims noted above—defamation, copyright, and trademark—are claims likely to be asserted against such providers due to their status as internet intermediaries, i.e., entities that exist to

transport *information*.[83] Although antitrust does not necessarily involve speech, it is nevertheless included because antitrust is more likely to be asserted against an actor when it gains power and market share, i.e., power in the market.[84]

The numbers from federal district court filings are inconclusive. Major intermediaries of yesteryear, such as Napster, Hotmail, and Geocities, barely register on the listing. These are further indicia of their declining and in some cases, increasingly irrelevant status as powerful intermediaries. Among entities that act primarily as intermediaries, the top numbers are for Amazon (85), Verizon (85), Google (83), eBay (21), AOL (18), Facebook (17), Yahoo (15), and YouTube (10). Several technology companies had numbers consistent with these figures or higher, such as Apple (87) and Microsoft (36).[85] But these numbers are all dwarfed by Walmart, which garnered 178 hits for the relevant classes of claims for the same five-year period. Compared to Walmart, none of the intermediaries seem particularly super.

However, district court filings show only the tip of the iceberg, because most claims against intermediaries are likely asserted *privately* by way of private extrajudicial procedures.[86] Thus, one of

---

[83] Assault cannot be culled from the search without examining each complaint individually. However, that should not affect the results significantly. First, the search showed few hits for the relevant cover sheet code, number 320. Second, it is highly unlikely that common-law claims for assault or battery will be asserted often against service providers, which provide their services remotely, precluding a physical touching.

[84] *See, e.g.*, Bracha & Pasquale, supra note 70, at 1180 ("It is unclear whether search engines fall under the strict definition of a natural monopoly, but they exhibit very similar characteristics." (footnote omitted)); Frank Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV. 115, 130 (2006) ("To the extent that search is a natural monopoly or oligopoly, government must try to assure that search engines are responsible for their results.").

[85] To be sure, both Apple and Microsoft sometimes act in an intermediary capacity, such as Apple through its cloud-storage capacity and iTunes store, and Microsoft through its Bing search engine.

[86] Ira S. Nathenson, *Civil Procedures For a World of Shared and User-Generated Content*, 48 U. LOUISVILLE L. REV. 911, 916 (2010) [hereinafter Nathenson, *Civil Procedures*] (discussing prevalence of "private extra-litigation procedures" in intellectual property rights enforcement).

the major tools used to enforce rights against internet intermediaries is the notice and takedown system, spurred on by the Digital Millennium Copyright Act of 1998 (DMCA).[87] Under this system, service providers will expeditiously remove claimed infringement upon proper notice, and in turn, receive a statutory safe harbor from monetary liability.[88] Copyright owners make extensive use of the notice-and-takedown system, sending numerous takedowns every year.[89] Direct evidence of this can be found by examining the archives of the *Chilling Effects* database, which collects takedowns and other demands sent to service providers.[90] As of February 2013, the database contained nearly 143 thousand DMCA takedown notices.[91]

Additionally, many service providers have extended the takedown procedures beyond copyright, honoring "quasi-DMCA" takedown notices for other claims such as trademark, trade dress, patent, trade secret, and more.[92] Though the DMCA does not extend its safe harbor beyond copyright, emerging case law gives a potent signal that a good-faith quasi-DMCA takedown system may serve a similar safety-valve function. For example, in *Tiffany (NJ) Inc. v. eBay, Inc.*,[93] the Second Circuit affirmed dismissal of Tiffany's contributory trademark infringement claim. The defendant, eBay,

---

[87] 17 U.S.C. § 512(c) (2010).

[88] *See id.*; *see also* Nathenson, *Safety Dance*, *supra* note 61 (explaining function of notice-and-takedown regime).

[89] Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMP. & HIGH TECH. L.J. 621 (2006).

[90] *See* Chilling Effects Clearinghouse, http://chillingeffects.org.

[91] *See* Chilling Effects Clearinghouse, *Cease and Desist Notices: DMCA Safe Harbor*, http://www.chillingeffects.org/dmca512c/notice.cgi (last visited Feb. 26, 2013). Because most of the notices in the database are forwarded there by Google and Twitter, this number—as shockingly large as it is—likely scratches only the surface of the total number of takedowns sent to service providers. *See* Jon Brodkin, *Twitter Uncloaks a Year's Worth of DMCA Takedown Notices, 4,410 in All*, ARS TECHNICA (Jan. 27, 2012), http://arstechnica.com/tech-policy/2012/01/twitter-uncloaks-a-years-worth-of-dmca-takedown-notices-4410-in-all/ (noting that Twitter and Google forward takedown notices to *Chilling Effects*, but Facebook does not).

[92] *See* Nathenson, *Safety Dance*, *supra* note 61, at 136-37.

[93] 600 F.3d 93 (2d Cir. 2009).

had taken incredible steps to institute a variety of programs to battle counterfeit goods, including a notice and takedown system.[94] Under these circumstances, the appellate court agreed with the district court that even though eBay had generalized knowledge that some auction listings were for counterfeit Tiffany merchandise, eBay would not be liable without "specific knowledge of individual instances of infringement."[95]

c. Internal

Finally, as noted, there is a third type of legal scrutiny, one that is especially indicative of Super-Intermediary status, namely, when an intermediary engages in intensive *internal* legal scrutiny that leads it to adopt procedures to limit legal exposure or to mollify important stakeholders, such as users and rights-holders. One example would be the quasi-DMCA policies noted above.[96] Notably, eBay instituted a number of processes, such as a takedown system. It also established a "Verified Rights Owner (VeRO) Program" to help rights owners.[97] The VeRO Program allows sellers to create "About Me" pages on eBay to inform customers of useful information in identifying genuine goods.[98] Ebay also engages in other internal self-regulation, such as an algorithmic "fraud engine" that uses filters to ferret out listings where counterfeiting may exist.[99] Such features helped the Second Circuit significantly in its conclusion that eBay was not a contributory trademark infringer.[100]

The eBay fraud engine is a special example of internal legal self-scrutiny, namely, the use by intermediaries of *code* to self-

---

[94] *See id.* at 98-101.

[95] *Id.* at 106-09.

[96] *See supra* text accompanying notes 92-94.

[97] eBay, *How eBay Protects Intellectual Property (VeRO)*, http://pages.ebay.com/help/policies/programs-vero-ov.html.

[98] eBay, *VeRO: Participant About Me Pages*, http://pages.ebay.com/help/community/vero-aboutme.html.

[99] *Tiffany (NJ)*, 600 F.3d at 98-99.

[100] *See id.* at 98-100.

regulate. YouTube does something very similar with its "Content Identification" program, which permits copyright owners to upload video or audio files to serve as digital "fingerprints."[101] YouTube then uses those fingerprints to identify potentially infringing user uploads, permitting the copyright claimant to either block the video, track it, or add advertising.[102] Surprisingly, most Content ID participants choose to monetize videos.[103] This is perhaps a major indicator of a Super-Intermediary: the power to control content that is not backed up by law, but *is* law. It is law because it is code that functions as a regulator, just as law does.[104] This theme will be explored further in Part IV.B, which addresses codes and control.

3. Reputation

The final set of features that suggest Super-Intermediary power is related to reputation. This subsection looks to political activity, ubiquity, and hero/villain status.

a. Political Activity

The first is the extent of *political activity*. Political activity can be measured in numerous ways. One example is the use of media to advance a political agenda. When the SOPA and PIPA bills were pending before Congress, service providers ran a "blackout" that did a much better job of persuading Congress than did the content providers who lobbied for an expansion of intellectual property

---

[101] YouTube, *Content ID*, http://www.youtube.com/t/contentid (last visited July 14, 2013).

[102] *See id.* For more on the Content ID program, including discussion of problems of fair use, see Nathenson, *Civil Procedures*, *supra* note 86, at 936-44.

[103] *See* Brian Stelter, *Some Media Companies Choose to Profit From Pirated YouTube Clips*, N.Y. TIMES (Aug. 16, 2008), at C1, http://www.nytimes.com/2008/08/16/technology/16tube.html (noting that ninety percent of materials identified by Content ID are monetized rather than blocked).

[104] LAWRENCE LESSIG, CODE 2.0 121 (2006).

enforcement rights.[105]

Another example is campaign contributions. For example, in 2011-2012, Microsoft contributed over $4 million and Google $3.2 million,[106] while Facebook donated over $630,000.[107] Google and Microsoft were also active in lobbying, respectively spending more than $16 million (Google)[108] and $8 million (Microsoft).[109] Additional examples include forming political action committees (PACs) and lobbying groups. In 2013, Twitter formed a PAC to address issues such as free speech, governmental surveillance, and intellectual property reform.[110] Similarly, Facebook founder Mark Zuckerberg formed lobbying group FWD.us, joined by Microsoft founder Bill Gates, Yahoo CEO Marissa Mayer, and Google Chair Eric Schmidt.[111]

If this is not sufficient proof of the burgeoning power of Super-Intermediaries, one might look to the increasing intertwining of such intermediaries with traditional actors in high governmental positions. Many politicians today make extensive use of Twitter and

---

[105] *See* Ned Potter, *Wikipedia Blackout: Websites Wikipedia, Reddit, Others Go Dark Wednesday to Protest SOPA*, PIPA, ABC NEWS (Jan. 27, 2012), http://abcnews.go.com/Technology/wikipedia-blackout-websites-wikipedia-reddit-dark-wednesday-protest/story?id=15373251.

[106] OpenSecrets.org, *Computers/Internet*, http://www.opensecrets.org/industries/indus.php?ind=B12 (last visited Apr. 18, 2013) (contributions and lobbying). The top contributor was Oracle Corp. with over $4.3 million. *Id.*

[107] *Id.*

[108] *Id.* One source reports that Google's lobbying budget is the eighth largest in the country. *See* Matt Brian, *Google's Lobbying Budget is Eighth Largest in US, Surpassing Even Lockheed Martin*, THE VERGE (June 4, 2013), http://www.theverge.com/2013/6/4/4394234/google-eight-biggest-record-lobbying-washington.

[109] OpenSecrets.org, *Computers/Internet*, *supra* note 106.

[110] *See* Cecilia Kang, *Twitter Joins Washington's Influence Economy, Forms PAC*, WASH. POST (Aug. 9, 2013), http://www.washingtonpost.com/business/technology/twitter-joins-washingtons-influence-economy-forms-pac/2013/08/09/8af1a97a-0124-11e3-96a8-d3b921c0924a_story.html.

[111] *See* Tom Warren, *Mark Zuckerberg adds Bill Gates and Steve Ballmer to his FWD.us lobbying group*, THE VERGE (Apr. 26, 2013), http://www.theverge.com/2013/4/26/4269228/bill-gates-steve-ballmer-join-mark-zuckerbergs-fwd-us-group.

Facebook.[112] Rebecca MacKinnon reports that in 2010 and 2011, Facebook "beefed up its Washington-based policy team," both to lobby against unwanted regulations, as well as to assist politicians interested in using Facebook as a campaign tool.[113] She also notes that Google hires executives with experience in government and diplomacy for jobs "described internally as 'foreign minister' and 'ambassador.'"[114] Indeed, considering the increasing mixing of Super-Intermediaries and governmental interests, it should shock no one that the book *The New Digital Age* was written jointly by the chair of Google and a former State Department adviser.[115]

Finally and of particular concern, recent revelations have shed light on Super-Intermediaries' possible role in governmental surveillance. For instance, recent allegations claim that the National Security Agency (NSA) reimbursed Silicon Valley millions of dollars for participating in its Prism surveillance program.[116] Although

---

[112] *See, e.g.*, Barack Obama (BarackObama) on Twitter, https://twitter.com/BarackObama; The White House (whitehouse) on Twitter, https://twitter.com/whitehouse; Mitt Romney (MittRomney) on Twitter, https://twitter.com/mittromney; Barack Obama, https://www.facebook.com/barackobama; The White House, https://www.facebook.com/WhiteHouse; Mitt Romney, https://www.facebook.com/mittromney. Indeed, President Obama's mastery of social media has often been pointed to as a key element in his campaign strategies. *See, e.g.*, WEAVER, *supra* note 10, at 97-99 (noting Obama campaign's use of the internet); Jennifer Aaker & Victoria Chang, *Obama and the Power of Social Media and Technology*, EUR. BUS. REV. (2009), http://www.europeanbusinessreview.com/?p=1627; Dylan Byers, *President Obama, Media Puppet-Master*, POLITICO.COM (Feb. 18, 2013), http://www.politico.com/blogs/media/2013/02/president-obama-media-puppetmaster-157259.html; Gehl, *supra* note 57 ("The most obvious contemporary intersection of marketing, social media, and state power is in the complex and powerful microtargeting of voters, especially visible in recent U.S. Presidential elections.").

[113] MACKINNON, *supra* note 14, at 7.

[114] *Id.* She further describes the activities of French President Nicolas Sarkozy at the 2010 conference of the e-G8, a conference in France of "Internet CEOs, government representatives, and assorted Internet celebrities," held in advance of the G8 meeting. *Id.* at 197.

[115] *See* SCHMIDT & COHEN, *supra* note 19; *see also infra* text accompanying notes 134-51.

[116] *See* Ewen MacAskill, *NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies*, THE GUARDIAN (Aug. 22, 2013), http://www.the

analysis of NSA surveillance is beyond the scope of this article, one cannot help but conclude that the specter of a possible "corporate-government surveillance partnership" provides yet another example of the power of Super-Intermediaries.[117]

b. Ubiquity

The second reputational feature is the degree to which the intermediary is a *ubiquitous* component of national and even international activity. Short of intermediaries running down the red carpet wearing Prada or a tuxedo, there can be little doubt these days that Super-Intermediaries such as Google, YouTube, Facebook, and Twitter are celebrities. Television commercials and shows such as *Big Bang Theory*, *The Simpsons*, *South Park*, and *Modern Family* include in-plot references to such providers.[118] In addition, the film *The Social Network*,[119] a film about the creation of Facebook, was a

guardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

[117] *See* Bruce Schneier, *Public-Private Surveillance Partnership*, BLOOMBERG VIEW (July 31, 2013), http://www.bloomberg.com/news/2013-07-31/the-public-private-surveillance-partnership.html. The *New York Times* reports that when Facebook's Chief Security Officer left the company in 2010, he took a position at the NSA, "underscor[ing] the increasingly deep connections between Silicon Valley" and the NSA. James Risen & Nick Wingfield, *Web's Reach Binds N.S.A. and Silicon Valley Leaders*, N.Y. TIMES (June 19, 2013), http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html.

[118] For instance, Twitter was mentioned in 50% of commercials during the 2013 Super Bowl. Matt McGee, *Game Over: Twitter Mentioned In 50% Of Super Bowl Commercials, Facebook Only 8%, Google+ Shut Out*, MARKETING LAND (Feb 3, 2013), http://marketingland.com/game-over-twitter-mentioned-in-50-of-super-bowl-commercials-facebook-only-8-google-shut-out-32420. Another site lists a number of television shows referring to Facebook. *See* Gau Mug, *Facebook References in Popular TV Culture*, GEEKS & NERDS ONLINE, http://www.techgau.org/2012/01/facebook-references-in-popular-tv.html. Yet another site notes a number of songs containing Twitter references, including Miley Cyrus' rap "Good-Bye Twitter." Joe Lynch, *Music's 7 Best Twitter References*, FUSE (Mar. 21, 2013), http://www.fuse.tv/2013/03/music-7-best-twitter-references.

[119] THE SOCIAL NETWORK (Columbia Pictures 2010).

major hit.[120] Further, whereas the internet itself is a source of news and information, today's Super-Intermediaries are themselves news-makers. YouTube is regularly a topic of discussion in the media, and Facebook and Twitter were proclaimed to be major factors in the unfolding of the Arab Spring.[121] Social media providers were credited for playing a major role in disseminating information in the wake of the April 2013 bombing of the Boston Marathon.[122] Indeed, unlike a bland dial-up internet provider, today's Super-Intermediaries are ubiquitous, akin to celebrities that play a major part in how we define ourselves. Professor Siva Vaidhyanathan describes "Googlization," meaning that "Google has permeated our culture."[123] Google "is a ubiquitous brand: *Google* is used as a noun and a verb everywhere from adolescent conversations to scripts for *Sex and the City*."[124]

Although such providers might be international in scope, they need not be. A Super-Intermediary might have a regular reach only in one country but pervasively so; however, to the extent a Super-Intermediary permits user networks to reach out internationally, the more easily it is characterized using the label. Indeed, it might be suggested that the degree of international market presence should be a separate factor. However, international presence is not set into a separate category or subcategory, because an intermediary of any

---

[120] One of the stars of *The Social Network* was Andrew Garfield, who played Eduardo Saverin, a college friend and early business partner of Facebook founder Mark Zuckerberg. Garfield later went on to star in the title role of the 2012 film *The Amazing Spider-Man*, which brings us back to the quote about Spider-Man that starts this article. *See supra* text accompanying note 1; *see also* THE AMAZING SPIDER-MAN (Columbia Pictures 2012).

[121] *See* David Wolman, *Facebook, Twitter Help the Arab Spring Blossom*, WIRED (Apr. 16, 2013), http://www.wired.com/magazine/2013/04/arabspring.

[122] For example, "[a]uthorities and first responders used Twitter to relay real-time updates." Cadie Thompson *Social Media Played Critical Role in Boston Marathon Response*, CNBC (Apr. 16, 2013), http://www.cnbc.com/id/100645753. Also, surveillance video of suspects was posted to the FBI website, with video hosted by YouTube. FBI, *Surveillance Video Related to Boston Bombings*, http://www.fbi.gov/news/updates-on-investigation-into-multiple-explosions-in-boston/surveillance-video-related-to-boston-bombings (last visited Apr. 18, 2013).

[123] VAIDHYANATHAN, *supra* note 5, at 2.

[124] *Id.*

major size risks impacting human rights, either directly or by complicity with a state. Thus, international status should not be a highly determinative factor. Instead, what seems more relevant is the degree to which the intermediary becomes a major actor in culture, whether nationally or even in the international arena.

c. Hero/Villain

The third and final factor relevant to Super-Intermediary status is whether the public tends to lionize or demonize the provider; in other words, whether the public tends to cast the provider as either *hero or villain*. Indeed, the quotes beginning this article compare Spider-Man and Google, one a fictional superhero and the other perhaps the most powerful of today's Super-Intermediaries.[125] There is no doubt that Google views itself as an aspiring champion of the good through its unofficial vow "Don't be evil."[126] However, Professor Siva Vaidhyanathan points out that "Google never promised to be comfortable and benign: it just promised not to be evil, whatever that means."[127]

Regardless of the normative bent of Google's "no evil" vow, Google also has an official but lesser-known mission statement, one that may speak more accurately about Google's goals: "Google's mission is to organize the world's information and make it universally accessible and useful."[128] Regarding Twitter, one source commented in 2011 that although it then lacked a business model, Twitter nevertheless had a mission statement: "To instantly connect people everywhere to what's most important to them."[129] Face-

[125] *See supra* text accompanying notes 1-2.

[126] *See supra* text accompanying note 2.

[127] VAIDHYANATHAN, *supra* note 5, at 75; *see also* MACKINNON, *supra* note 14, at xx (stating that the question is how to "maximize the good" and "minimize the evil" of digital technology).

[128] Google, *Company*, http://www.google.com/about/company/.

[129] Mark Evans, *Twitter's New Mission Statement*, TWITTERATI (Jan. 11, 2011), http://www.twitterrati.com/2011/01/11/twitters-new-mission-statement/; *see also* Twitter's *New CEO Finally Nails Down the Company's Long-Term Vision*, MASHABLE (Jan. 10, 2011), http://mashable.com/2011/01/10/twitters-new-ceo-

book's mission is to "make the world more open and connected."[130] To be sure, numerous organizations, large and small, important and irrelevant, have mission statements.

One benchmark of a Super-Intermediary's power can be found when even a damaged reputation does not materially reduce its user base, either because the users are too devoted to shift, or too locked-in to seek out alternatives.[131] For example, major intermediaries have been regularly castigated by their users for matters such as privacy violations, changes to terms and conditions, and changes to features. Yet such changes have had little demonstrable impact on the use of such services, and their power base has only increased. Indeed, it may be that for Super-Intermediaries, fame and infamy are the same thing, so long as people continue to use the services they love to hate.[132]

---

finally-nails-down-the-companys-long-term-vision/ (Twitter CEO echoing mission statement).

[130] Facebook, *About*, https://www.facebook.com/facebook?v=info (last visited July 17, 2013). Facebook's IPO filing included a letter from CEO Mark Zuckerberg that included the mission statement noted above, as well as additional goals, such as "chang[ing] how people relate to their governments and social institutions," to "bring a more honest and transparent dialogue around government that could lead to more direct empowerment of people, more accountability for officials and better solutions to some of the biggest problems of our time." Terrence O'Brien, *Zuckerberg outlines idealistic Facebook mission in IPO filing*, ENGADGET (Feb. 1, 2012), http://www.engadget.com/2012/02/01/zuckerberg-outlines-idealistic-facebook- mission-in-ipo-filing/.

[131] In *The New Digital Age*, Schmidt and Cohen suggest that citizens will have more options as "the proliferation of companies continues." SCHMIDT & COHEN, supra note 19, at 65. They therefore naively place responsibilities on users to read intermediary policies before sharing information. *Id.* But two features of today's information infrastructure lead to *lock-in*, making it difficult for users to seek viable options, even when users bother to read terms and conditions. First, the era of Super-Intermediaries is one of consolidation. Instead of many websites, we see a small set of major players that dominate their fields. Professor Yochai Benkler notes that "power law distribution" means that people solve the problem of information overload by "congregating in a small number of sites." BENKLER, *supra* note 47, at 241. Second (and related), incumbent companies may be well-positioned to reap the rewards of their extant power because "new nodes prefer to attach to already well-attached nodes," meaning "the rich get richer." *Id.* at 244; *see also* Pasquale, *supra* note 17, at 153 (noting "switching costs").

[132] "Whatever is done from love always occurs beyond good and evil."

C. Why Super-Intermediaries?

Each of the nine features discussed above suggests a component of intermediary power. The totality of these features may indicate that an intermediary has significant *actual power*, thus meriting the label Super-Intermediary.[133] Today, major internet intermediaries recognize the power they wield, which is amply illustrated by the recent book *The New Digital Age*, by Google chair Eric Schmidt and Washington insider Jared Cohen.[134] The authors consider the internet both "a source for tremendous good and potentially dreadful evil."[135] They therefore extol the value of *code*: as the authors note, "[w]e spent a great deal of time . . . predicting trends and theorizing possible tech-oriented solutions."[136]

Reading the book, however, one senses a strong preoccupation with power. First, the authors represent a significant intermingling of old and new forms of power. Cohen is the essence of an east-coast Washington political insider, having served as an adviser for two Secretaries of State.[137] Schmidt is the pinnacle of a Dot-Com chieftain, the executive chair and former CEO of the world's premier search company, based in the west coast.[138] This intermingling of what Professor Lawrence Lessig calls "East Coast Code" and "West Coast Code"[139]—i.e., governmental power and algorithmic power—

FRIEDRICH NIETZSCHE, BEYOND GOOD AND EVIL 90 (Walter Kaufman tr. 1966) (aphorism 153).

[133] Professor Milton Mueller charges that "we should not allow the commons to be privatized." Milton Mueller et al., *The Internet and Global Governance: Principles and Norms for a New Regime*, 13 GLOBAL GOVERNANCE 237, 249 (2007) (emphasis removed).

[134] SCHMIDT & COHEN, *supra* note 19.

[135] *Id.* at 3.

[136] *Id.* at 11.

[137] Cohen is "a former adviser to Condoleezza Rice and Hillary Clinton." Julian Assange, *The Banality of 'Don't Be Evil'*, N.Y. TIMES (Jun. 2, 2013), http://www.nytimes.com/2013/06/02/opinion/sunday/the-banality-of-googles-dont-be-evil.html. He now works at Google as the director of Google Ideas. *Id.*

[138] *See* Google, Management Team, https://www.google.com/about/company/facts/management/ (last visited Aug. 14, 2013).

[139] *See* LESSIG, CODE 2.0, *supra* note 104, at 72.

strongly evokes the increasingly pervasive role that Super-Intermediaries play in wielding quasi-governmental power over citizens.[140] Indeed, critics of the "global surveillance industry" such as WikiLeaks founder Julian Assange caution that the "internet, our greatest tool of emancipation, has been transformed into the most dangerous facilitator of totalitarianism we have ever seen."[141]

Second, the book's text suggests a strong focus on the power of internet intermediaries. As the authors state in the introduction, "Never before in history have so many people, from so many places, had so much *power* at their fingertips."[142] Although at times the authors treat the question of power as being between individuals and governments,[143] the authors also note the power of key intermediaries: "modern technology platforms, such as Google, Facebook, Amazon and Apple, are even more powerful than most people realize."[144] Indeed, textual analysis of the book's main text shows the following number of hits for relevant terms:

[140] *Id.* at 73 (stating that "[v]alues from the East become integrated with the West").

[141] JULIAN ASSANGE WITH JACOB APPELBAUM ET AL., CYPHERPUNKS: FREEDOM AND THE FUTURE OF THE INTERNET 1 (2012).

[142] SCHMIDT & COHEN, *supra* note 19, at 4 (emphasis added).

[143] *Id.* at 9 (asking "[w]ho will be more powerful in the future, the citizen or the state?").

[144] *Id.*

Table 3: Frequency in Main Text of Terms in *The New Digital Age*

Search term	**Total in main text:**
"secur" (i.e., "secure," "secures," "security")	179
"power" (i.e., "power," "powerful," "empower," "empowerment")	142
"priva" (i.e., "private," "privacy")	88
"responsib" (i.e., "responsible," "responsibility," "responsibilities")	44
"relig" (i.e., "religion," "religious")	23
"copyright" (i.e., "copyright," "copyrights," "copyrighted")	22
"property" (i.e., "property," "intellectual property")	22
"express" (i.e., "express," "expression," "free expression")	21
"speech" (i.e., "speech," "free speech")	18
"human right" (i.e., "human right," "human rights")	4

As shown by Table 3, formatives of "power" appear over 140 times in the main text. Along similar lines, variants of "security"—a concept that relies on the assertion of intermediary power over hackers, spammers, trolls, and other miscreants—appears even more often, appearing nearly 180 times. In stark contrast, formatives for affirmative societal values besides security appear far less often, including variants of terms evoking: "privacy" (88); "religion" (23); "copyright" (22); "property" (22), "expression" (21); and "speech" (18). Most significantly for this article, variants of "responsibility" appear only 44 times, and variants of "human rights" appear only four times.[145]

Although a more detailed examination of *The New Digital Age* is beyond this article,[146] it is hard to come away from this textual analysis without concluding that these two authors are primarily concerned with the *power* of large internet intermediaries. Perhaps it is inevitable that power is to become a major focal point in cyberlaw scholarship. Considering Professor Yochai Benkler's observation that internet users tend to congregate around a small subset of the

[145] *See also* VAIDHYANATHAN, *supra* note 5, at 3, 4, 6, 14 (noting Google's power).

[146] Such an endeavor would be worthy of a critical book review.

sites available online,[147] he expresses concern that this consolidation presents a serious challenge to the claim that "Internet communications . . . meaningfully decentralize democratic discourse."[148] Professor Jacqueline Lipton suggests that a unifying framework for cyberlaw can be found by focusing on the "global nature" of the internet and the third-party intermediaries that facilitate it.[149] Professor Derek Bambauer notes that when governments co-opt intermediaries with "dominant market positions," the costs of information access increase, and the "efficacy of circumvention" decreases."[150]

Such concerns may shed additional light on the admission in *The New Digital Age* that "the companies responsible for the architecture of the virtual world will shoulder much of the blame for the less welcome developments in our futures."[151] With these thoughts in mind, this subpart provides a theoretical foundation for the stakeholder framework, provides qualifications to flesh it out, and addresses the question of why we should care about identifying Super-Intermediaries.

1. Theoretical Underpinnings

Table 4, below, provides a theoretically oriented view of the *framework* and *features* used to describe Super-Intermediaries. By organizing the nine features under three distinct categories, Table 4 emphasizes that the framework and features explored in this article are ultimately geared towards measuring the *actual power* of internet intermediaries.

---

[147] "In other words, the rich get richer." BENKLER, *supra* note 47, at 244.

[148] *Id.* at 241. Looking to power laws, Benkler notes that most sites have few-to-no links, a small number have a moderate amount, and "a tiny number have a very large number." *Id.* at 244. Conclusion? "The implication for democracy that comes most immediately to mind is dismal." *Id.* at 245.

[149] Lipton, *supra* note 26, at 1341-42.

[150] Derek E. Bambauer, *Censorship v3.1*, IEEE INTERNET COMPUTING, at 29 (May/June 2013) [hereinafter Bambauer, *Censorship v.3.1*].

[151] SCHMIDT & COHEN, *supra* note 19, at 65.

Table 4: Using Features of Super-Intermediaries to Assess Actual Power

	Users	**Legal Actors**	**Reputation**
Features	Interactivity Networking Personalization	Governmental Private Internal	Political activity Ubiquity Hero/villain ambiguity
Relationship	Self-affiliates	Scrutiny of intermediary	General public
Interest	Reliance	Disruption to rights	Perceived power

The first category focuses on *users* of intermediaries. As noted above,[152] it looks to the degree to which an intermediary is interactive, provides networking, and permits personalization. Users of intermediaries are stakeholders who choose to *self-affiliate* with the intermediary, and therefore often have a strong *reliance* interest in the availability of the intermediary's services. For example, in addition to simply viewing videos, YouTube users can comment on videos and embed YouTube videos in other sites. Motivated users can go even further by creating YouTube channels to build a following or create a business.[153] Similarly, Facebook users create personalized networks, can follow people, and can post and view content. But the more powerful the intermediary, the fewer practical choices interested users might have, and the more users are locked in to the services. People may complain about Facebook, but the service's one billion-plus users make it hard for its users to switch. Thus, Facebook remains the predominant social network of its type despite common complaints over matters such as privacy or changes to its interface.[154] Because many users put tremendous time into posting

[152] *See supra* Part I.B.1.

[153] One example of such a user is the "reigning queen of YouTube," Jenna Marbles, who obtains over a "million views every single day and more money than she had ever seen before in her life." *See* Amy O'Leary, *The Woman With 1 Billion Clicks, Jenna Marbles*, N.Y. TIMES (Apr. 13, 2013), http://www.nytimes.com/2013/04/14/fashion/jenna-marbles.html.

[154] *See, e.g.*, *Mark Zuckerberg's Sister Complains of Facebook Privacy Issues*, FOXNEWS.COM, Dec. 26, 2012, http://www.foxnews.com/tech/2012/12/26/mark-zuckerbergs-sister-complains-facebook-privacy-issues; *Hatred of Timeline Causes Satisfaction with Facebook to Plummet*, FOXNEWS.COM, July 18, 2012, http://www.foxnews.com/tech/2012/07/18/hatred-timeline-causes-satisfaction-

content, building an online reputation, and building networks, users are subject to "lock-in" *reliance* interests in the continuation of the service.

The second category focuses on *legal actors* who may *scrutinize* or challenge the conduct of an intermediary.[155] Legal challengers may be governmental, private, or even internal, as described above.[156] Such actors (at least governmental and private challengers) are not necessarily concerned about relying on the continuation of such services, but are instead concerned about the actual or potential *disruption* to claimed rights and interests.[157] Thus, governments are concerned about various types of speech. Property owners are often deeply upset over copyright and trademark infringement occurring online. Even the intermediaries themselves often take significant steps to self-regulate in order to preempt or deflect claims. These actions are not rooted in a reliance interest but rather constitute reactions to the disruptive effect of major intermediaries.

The final category focuses on an intermediary's *reputation* to the *general public* at large. As such, this category may overlap somewhat with the first two categories. However, whereas the first two categories focus on the experiences of individual stakeholders, the last category takes a more macroscopic view of public reaction to an intermediary in terms of *perceived power*. It looks to the degree to which the intermediary is ever-present in the mind of society.[158] Thus, from this broader perspective, relevant features are the degree of political activity, the intermediary's ubiquity, and the degree to

---

with-facebook-to-plummet.

[155] *See supra* Part I.B.2.

[156] *Id.*

[157] Professor Russell Weaver notes that "some commentators have suggested that the Internet is more challenger-oriented and is more geared toward disrupting the existing power structure." WEAVER, *supra* note 10, at 100 (internal quotes omitted).

[158] Martin Heidegger has analogous ideas regarding tools, suggesting in *Being and Time* that we do not think of tools until they present themselves to us, such as when a tool is broken. MARTIN HEIDEGGER, BEING AND TIME 102-07 (John Macquarrie & Edward Robinson tr. 1962). Indeed, it may turn out that Heidegger's observations shed a crucial light on the nature of cyberspace and the current drive towards regulating it.

which segments of society view the provider as hero or villain. Political activity, such as that by Google, may suggest actual political power. Equally so, the ubiquitous presence of big intermediaries in traditional media, such as television and movies, suggests that such services play a central role in modern culture. Finally, a great degree of ambiguity regarding the hero or villain status of such services further suggests that the public has reservations over the perceived power of the providers.

Secondary considerations beyond those noted above may be additionally relevant in determining Super-Intermediary status.[159] For example, the framework and features avoid direct incorporation of *profitability* or *economic power*. To be sure, some of the features indirectly embrace economic concerns, such as the ability to make campaign contributions or to provide highly interactive technology on a large scale. But a Super-Intermediary need not have economic power in terms of large revenues or profits. Indeed, many of the top Super-Intermediaries lack profitability, or lacked profitability in their early years of operation on their way to "super" status.[160] As Professor Benkler notes in *The Wealth of Networks*, "the structure of the Web means that money is neither necessary nor sufficient to grab attention."[161] Thus, to the extent some Super-Intermediaries ultimately become economic powerhouses, it may be because of their innovations as Super-Intermediaries, rather than the reverse.[162] Also

---

[159] *Cf.* Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966) (noting "secondary considerations" to the analysis of whether a patent is invalid for being obvious); KSR Int'l Co. v. Teleflex Inc. 550 U.S. 398, 415 (2007) (courts may look to secondary considerations "where appropriate").

[160] *See, e.g.*, Matt Marshall, *Venture Capitalist Vinod Khosla is Moving to a Part-Time Role to Pursue Philanthropic Interests in India and to Spend More Time with His Family*, SAN JOSE MERCURY NEWS (Feb. 14, 2004), at 1C, *available* at 2004 WLNR 19565918 (stating in 2004 that Google had not yet turned a profit); Ben Woodhead, *A Struggling Model*, AUSTRALIAN FIN. REV. (Aug. 15, 2009), at 24, *available at* 2009 WLNR 27792594 (stating in 2009 that "like Twitter and Facebook, Google-owned YouTube hasn't turned a profit yet").

[161] BENKLER, *supra* note 47, at 254.

[162] *Cf.* SCHMIDT & COHEN, *supra* note 19, at 101 (regarding users, stating that "size matters less" and that technology "allows smaller actors to have outsized impacts"). As Rebecca MacKinnon notes, internet companies are powerful not just by selling goods, but also because they "provide and shape the digital spaces

worth noting is that Super-Intermediary revenue models do not typically rely on direct monetization out of the pockets of users.[163] Thus, what matters in here is not *market* power, but *mediation* power, namely, a central role in the intermediation of information on the internet for users, disruptions to rights-owners, and a pervasive reputation. Therefore, profitability is not a particularly compelling litmus test, although great profit may be relevant in a secondary sense when the profit bears a direct nexus to stakeholder features.

2. Additional Observations

Additional observations may be made regarding the stakeholder framework and features. First, the label of Super-Intermediary depends on the nature of the intermediary and not the nature of the platform on which it is used. It does not matter whether the intermediary is found only through a computer, or via an application on a smartphone. Indeed, the most pervasive intermediaries of today are available—often seamlessly—through both internet browsers and smartphone apps.

Second, the determination of Super-Intermediary status as envisioned in this article looks to the totality of circumstances, and no one feature is determinative. For example, although high interactivity is a common feature in a Super-Intermediary, it is not by itself sufficient. For example, MySpace—a highly interactive social-networking site—is likely no longer a Super-Intermediary due to an ever-shrinking user base, reducing the extent and value of its network. This also leads to a lower reputation factor, considering that the smaller network has a reduced degree of ubiquity. Thus, a social network using Web 2.0 technology is not necessarily a Super-Intermediary. The same observation may be made in reverse: a

---

upon which citizens increasingly depend." MACKINNON, *supra* note 14, at 11. I would argue that the foundation for Super-Intermediary power is the crafting of such spaces, and any profitability later obtained by selling goods, services, or advertising may be a consequence of creating a core internet space.

[163] Google, YouTube, Facebook, and Twitter provide their core services for free. Money is instead primarily made through third parties, such as advertisers.

Super-Intermediary need not be a social network or use extensive Web 2.0 technology. With a stark white screen, the Google search engine is nevertheless a Super-Intermediary.[164] Even though it may rank relatively low in terms of networkability, the Google search engine is still a powerful service. Its search results can be highly individualized.[165] Moreover, it is a constant target of legal scrutiny, leading it to institute extensive procedures for handling intellectual-property claims. It is also the subject of incredible ubiquity and legal scrutiny: just one example would be antitrust complaints instituted against Google (and later settled) by the Federal Trade Commission.[166] Indeed, despite Google's mantra of "don't be evil," it is regularly cast as a villain.[167]

Third, there may be positive and negative feedback loops between the nine features.[168] A positive feedback loop exists when output increases input. Thus, an increase in networking and interactivity may in turn invite increased legal scrutiny via lawsuits and takedowns. This in turn may encourage the intermediary to boost its political activity to persuade lawmakers and the public of the intermediary's point of view. All of this in the aggregate may constitute a positive feedback loop, boosting the intermediary's presence in the public's consciousness. Conversely, a decline of an intermediary in

---

[164] For an interesting story about Google's long-standing mission of keeping its home page clean and uncluttered, one should read a blog posting by then-VP of Search Products & User Experience Marissa Mayer regarding the number of words on the Google homepage. *See* Marissa Mayer, *What comes next in this series? 13, 33, 53, 61, 37, 28...*, GOOGLE: OFFICIAL BLOG (July 03, 2008), http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series-13-33-53.html (noting considerations going into limiting home page to 28 words).

[165] Indeed, Google has been criticized by some for its practice of personalizing search results. *See supra* note 70 (collecting sources).

[166] Grant Gross, *Google, FTC settle antitrust case*, PC WORLD (Jan. 13, 2013), http://www.pcworld.com/article/2023662/google-ftc-settle-antitrust-case.html.

[167] *See* Rob Enderle, *Has Google Crossed Over Into True Evil?*, TECHNEWSWORLD (Aug. 27, 2012), http://www.technewsworld.com/story/76001.html; James B. Stewart, *The Line Between 'Aggressive' and 'Evil'*, N.Y. TIMES (Jan. 4, 2013), http://www.nytimes.com/2013/01/05/business/google-finds-a-line-between-aggressive-and-evil.html.

[168] *Cf.* Nathenson, *Civil Procedures*, *supra* note 86, at 918-19 (discussing feedback loops in private copyright enforcement).

the public's eye—a loss of reputation—can lead to a loss of user interaction and network-creation. This can lead to less content-generation, leading to fewer legal demands. Eventually, the intermediary may become a secondary player (MySpace) or cease operations (Friendster). This suggests that for internet intermediaries, success breeds success, and failure breeds failure.[169] The dynamic nature of intermediary power is illustrated by the reality that Super-Intermediary power may be attained and lost over time. Yesterday's Super-Intermediaries—Napster and AOL—are minor players on today's internet. The same fate may someday visit Google, Facebook, or Twitter.

3. Examples

Naming today's Super-Intermediaries is an admittedly subjective task,[170] but they likely include Google's search engine as well as Google-owned YouTube. Additional providers probably include Twitter, Facebook, eBay, and Amazon.[171] For present purposes, line-drawing is unnecessary. However, it should be noted that the greater the power of the intermediary, the more likely there are no practicable alternatives to the service provider. Despite the existence of Bing and Yahoo, most people today use Google. Facebook retains its position as the provider of choice for building networks, despite the continued existence of LinkedIn for professional net-

---

[169] *See* Lemley & McGowan, *supra* note 64, at 491 ("Goods constitute virtual networks when they provide inherent value to consumers that increases with the number of additional users of identical and/or interoperable goods.").

[170] Indeed, an earlier draft of this article attempted to rate intermediaries feature-by-feature, and then to rank them. The subjectivity of the rating for each feature made it quickly apparent that this would be a problematic endeavor. It would therefore appear that the features and the label Super-Intermediary are instead "fuzzy" and quite debatable. Having said that, the features and framework are intended to provide a method of examining individual intermediaries to determine whether their degree of overall power merits Super-Intermediary status.

[171] As noted previously, this article focuses on intermediaries who interface directly with users by providing services such as content hosting, searching, and applications, leaving to the side actors that provide other services, such as conduit providers. *See supra* note 30 and accompanying text.

working, MySpace in altered form, and Google+. The power that comes to such providers makes it all the more important for them to take steps to respect human rights, and to be transparent about their processes that implicate those rights.[172] Further, this article does not argue that such obligations should be limited to Super-Intermediaries. The proposals made here are not intended as prescriptions to be embodied in positive law, but instead as process principles to be used by intermediaries of any size, super or small, to guide their conduct when they consider removing speech.[173]

However, the article does suggest—as does the article's opening quote—that the greater the power of an intermediary, the greater the social responsibility.[174] Professors Jonathan Zittrain and

---

[172] "In the long run, if social networking services are going to be compatible with democracy, activism, and human rights, their approach to governance must evolve." MACKINNON, *supra* note 14, at 164.

[173] For example, one colleague suggested to the author that Ripoff Report might be considered a Super-Intermediary. This colleague is of course right that Ripoff Report has received a fair amount of media attention and has been sued a number of times: in the past five years, six times as a defendant in federal court, and pursuant to another Bloomberg search, 39 overall docket listings in state and federal trial and appellate courts in the same period. Ripoff Report offers aggrieved businesses small solace through the right to post a free rebuttal or pay for an arbitration. *See* Ripoff Report, *Set the Record Straight | Arbitration Program*, http://www.ripoffreport.com/Arbitration.aspx. This provides a minor, though to most businesses, unsatisfying private form of enforcement. It is unknown to the author how many rebuttals or arbitrations are actually filed, but it is hard to imagine them coming close to the millions of takedowns sent to major intermediaries such as Google and Google-owned YouTube.

Regardless, it is doubtful that the reputation features of Ripoff Report come close to that of other intermediaries. For example, a Google search for "ripoff report" leads to 706 thousand hits, a significant amount. But searches for major players far outnumber that figure: Facebook (10.89 billion), Twitter (7.71 billion), Google (5.79 billion), and YouTube (3.86 billion). Thus, it is doubtful that Ripoff Report is a Super-Intermediary to the broader public. Having said that, as noted in the main text, the recommendations made in the article, particularly the Digital Due Process principles in Part V.E, can provide guidance for intermediaries of any significant size. As these principles are intended as voluntary and flexible best practices, the article makes the modest claim that the more powerful a provider is, the more it ought to engage in such practices. That is not to suggest that lesser intermediaries such as Ripoff Report should not.

[174] *See supra* text accompanying note 1; *see also* Balleste, *supra* note 9, at 250

John Palfrey point out that "[w]hen public and private actors combine to restrict the publication of and access to online content, . . . the hackles of human rights activists are understandably raised."[175] Rebecca MacKinnon further says that an internet intermediary is not like a big company making "sportswear or toothpaste," but is instead a company whose services "relate[] directly to the empowerment of citizens."[176] Thus, Super-Intermediaries may have responsibilities quite different from other large companies in other market segments.

There are ample precedents for expecting especial obligations on non-state actors who build important networks or provide societal services, especially regarding those with significant power.[177] Securities laws provide numerous duties on businesses that sell stock.[178] Telecommunications laws[179] and utilities laws[180] regulate important industries that provide backbone utilities. Antitrust laws prohibit certain monopolies as well as contracts in restraint of trade.[181] Food and drug laws regulate which substances may be sold for human consumption.[182] In each case, major actors may possess significant power due to their market positions. In addition, the law prescribes

("Under the umbrella of Internet governance, the private sector is seen as an active and powerful player.").

[175] Jonathan Zittrain& John Palfrey, *Internet Filtering: The Politics and Mechanisms of Control*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 29, 49 (Ronald Deibert et al. eds., 2008) [hereinafter ACCESS DENIED].

[176] MACKINNON, *supra* note 14, at 171-72.

[177] *See* MUELLER, *supra* note 37, at 205 (discussing literature noting that "the more central private actors, the ones with governance responsibilities, are seen as assuming state-like powers in content regulation while being exempt from the state's due process and constitutional constraints").

[178] *See, e.g.*, Securities Exchange Act of 1934, 15 U.S.C. §§ 78a-78pp (2006 & Supp. IV 2010); Securities Act of 1933, 15 U.S.C. §§ 77a-77aa (2006 & Supp. IV 2011).

[179] *See, e.g.*, Communications Act of 1934, 47 U.S.C. § 151 et seq. (2006).

[180] *See, e.g.*, Atomic Energy Act of 1954, 42 U.S.C. §§ 2011-2297h-13 (2006).

[181] *See, e.g.*, Clayton Antitrust Act, 15 U.S.C. §§ 12-27, 29 U.S.C. §§ 52-53 (2006); Sherman Antitrust Act, 15 U.S.C. §§ 1-7 (2006).

[182] *See, e.g.*, Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301-399 (2006).

obligations. But again: having said that, this article does not go so far as to recommend legal prescriptions. Rather, it asks which obligations a Super-Intermediary should assume as a matter of social responsibility. Julian Assange asks, "In the new space of the internet what would be the mediator of coercive force?"[183] Indeed, when code functions as law, complete with the algorithms that enforce the judgments of internet intermediaries, a Super-Intermediary exercises quasi-state power over or digital personas and information.[184] Moreover, when a Super-Intermediary "does something adequately and relatively cheaply in the service of the public," then government and other public institutions may be "relieved of pressure" to perform such tasks.[185]

Finally, one might ask why the present framework focuses on big internet consumer intermediaries. Major television and media providers choose which stories to run and decline to run others. Might the obligations discussed in this article run beyond internet intermediaries to newspapers and television networks? Beyond the obvious response that such industries are beyond the scope of this article, it should be noted that there is a critical difference between traditional media, such as television and newspapers, and internet intermediaries, such as Google and Facebook. With the former, the media self-select the stories to run. With the latter, substantial por-

---

[183] ASSANGE, *supra* note 141, at 3.

[184] *See id.* at 55 (noting "the blurring of the state and corporation") (statement of Jacob Appelbaum).

[185] *See* VAIDHYANATHAN, *supra* note 5, at 6. One example of a private intermediary fulfilling such a role may be the Internet Archive's Wayback Machine, which provides a database of the historical World Wide Web. *See* Internet Archive, http://www.archive.org (last visited Aug. 15, 2013). However, the Wayback Machine's database is incomplete and not easily searchable. Further, because the Internet Archive provides a partial archive of the Web, there appears to be little pressure on the Library of Congress or the Archivist of the United States to take a leading role in providing a more complete and searchable database. Even though the Section 108 Study Group proposed changes to copyright law to encourage broader web archiving, Congress has passed no bills. *See* UNITED STATES COPYRIGHT OFFICE AND THE NAT'L DIGITAL INFORMATION INFRASTRUCTURE AND PRESERVATION PROGRAM OF THE LIBRARY OF CONGRESS, THE SECTION 108 STUDY GROUP REPORT 80-87 (2008), http://www.section108.gov/docs/Sec108StudyGroupReport.pdf.

tions of online content are provided (in the case of social networks or user-generated content) or derived (as is partially the case for search engines) from users of those services. Thus, the nature of the relevant stakeholders, and the relationships between them, are likely different from those relating to traditional media.[186]

II. The Innocence of Muslims *Video*

This Part provides background on the *Innocence of Muslims* video, the reactions of those who were hired to create it, the resulting protests and violence, and finally, Google's handling of demands to remove the video.

A. The Video

Two videos were posted to YouTube by someone with the user name "sam bacile" in July of 2012.[187] The first, *The Real Life of Muhammad*, was posted on July 1,[188] and the second, *Muhammad Movie Trailer*, was posted on July 2.[189] The film itself was apparently filmed under the name *Desert Warrior*, and possibly shown once in June 2012 at Hollywood's Vine Theater.[190] Online can be found an allegedly original script for *Desert Warrior*, one that tells the story of a false prophet named "'George,' a corrupt man who founds Islam and goes on a bloodthirsty rampage in the ancient Middle

---

[186] Having said that, traditional media ought to consider increased transparency as well. Indeed, modern media appears to be struggling in the post-Wikileaks era, where the "traditional" norms of careful story choosing and editing appear to be challenged by "leaks" sites that are less reticent to publicize materials.

[187] *See* Sam Bacile Channel, YouTube, http://www.youtube.com/channel/UC4DjVszAn4GAyzgsjtkJONg (last visited July 18, 2013).

[188] Sam Bacile, *The Real Life of Muhammad*, http://www.youtube.com/watch?v=LoBwR9KEGUc (posted July 1, 2012).

[189] Sam Bacile, *Muhammad Movie Trailer*, http://www.youtube.com/watch?v=qmodVun16Q4 (posted July 2, 2012) [hereinafter *Innocence of Muslims*].

[190] *Anti-Islam Film's Producer is on Federal Probation*, THE SMOKING GUN (Sept. 13, 2012), http://www.thesmokinggun.com/documents/crime/anti-islam-film-producer-764091.

East."[191]

The full film is not known to be available online. The two videos are each less than fourteen minutes long and similar in content, so this narrative will focus on *Muhammad Movie Trailer*, which is the more viewed of the two versions.[192] The plot is so disjointed that it is at times difficult to follow the "story," if there really is one to relate.[193] The video shows an angry mob of Muslims in modern Egypt looting a pharmacy run by a Coptic Christian man, and then killing a young woman wearing a cross.[194] The police deliberately fail to intercede, and later falsely blame Coptic Christians for the melee. The father, explaining the events to his daughter, appears to blame Islamic terrorism, and the narrative suddenly shifts to ancient times, "and a very inaccurate story of Muhammad's life begins."[195]

After the shift to the past, the "plot" becomes difficult to follow, and mostly consists of a series of disjointed vignettes. Essentially, it depicts Muhammad "as an imbecile and as a false prophet."[196] The video treats him as a "womanizing fraud."[197] Further,

---

[191] *See* Adrian Chen, *Here Is the Original Script for Innocence of Muslims*, GAWKER (Sept. 18, 2012), http://gawker.com/5944290/here-is-the-original-script-for-innocence-of-muslims.

[192] As of this writing, *Muhammad Movie Trailer* has been viewed over 5 million times, whereas *The Real Life of Muhammad* has been viewed less than 250,000 times.

[193] One commentator's reaction to the video is pithy and well-taken: "The acting is terrible, the plotting non-existent, the cinematography amateur, and the tone vicious and bigoted. It's like The Birth of a Nation as directed by Ed Wood." Stephen Daisley, *Innocence of Muslims: A Review*, THE COMMENTATOR (Sept. 12, 2012), http://www.thecommentator.com/article/1657/innocence_of_muslims_a_review.

[194] The account in this paragraph is taken from the author's observations of the video, as well as from helpful guidance from Chen, *supra* note 191.

[195] *See* Chen, *supra* note 191.

[196] *See* Eyder Peralta, *What We Know About 'Sam Bacile,' The Man Behind The Muhammad Movie*, NPR (Sept. 12, 2012), http://www.npr.org/blogs/thetwo-way/2012/09/12/161003427/what-we-know-about-sam-bacile-the-man-behind-the-muhammad-movie; *see also* Matt Bradley & Dion Nissenbaum, *U.S. Missions Stormed in Libya, Egypt*, WALL. ST. J. (Sept. 12, 2012), http://online.wsj.com/article/SB10000872396390444017504577645681057498266.html.

[197] Bradley & Nissenbaum, *supra* note 196.

"[c]ontravening the Islamic prohibition of portraying the prophet, clips from the film show him not only as flesh and blood—but as a homosexual son of undetermined patrimony, who rises to advocate child slavery and extramarital sex, for himself, in the name of religion."[198] "Muhammad" eats flesh from a bone, fails to wear undergarments in the presence of a woman, and places his head in a sexually suggestive position while a woman removes her head covering.[199] He gazes at a work animal—a donkey or mule—and proclaims, "And this shall be the first Muslim animal!"[200] An older man tells a woman that he will make a book for "Muhammad" by taking materials from the Torah and New Testament, and "mix[ing] them into false verses."[201] "Muhammad" later states that he might commit suicide, and in another scene, approves the selling of children into slavery in order to buy swords and horses. He further expresses his intention to sleep with the wife of another man.

Other scenes contain similarly scandalous material, such as a man asking "Is the messenger of God gay?" and "Is the Master dominant or submissive?"[202] The dialogue also includes a number of obvious overdubs.[203] For example, the actor portrayed as Muhammad is shown gnawing meat from a large bone as a partially overdubbed voice says "Muhammad! Muhammad the bastard! Your lady

---

[198] *Id.*

[199] *See Innocence of Muslims*, *supra* note 189.

[200] *Id.*

[201] *Id.*

[202] *Id.*

[203] *See* Sarah Abdurrahman, *Why Are All the Religious References in "Innocence of Muslims" Dubbed? [Updated]*, ON THE MEDIA (Sept. 12, 2012), http://www.onthemedia.org/blogs/on-the-media/2012/sep/12/religious-references-innocence-muslims-dubbed. Another source notes:

> In the English language version of the trailer, direct references to Muhammad appear to be the result of post-production changes to the movie. Either actors aren't seen when the name "Muhammad" is spoken in the overdubbed sound, or they appear to be mouthing something else as the name of the prophet is spoken.

Stephen Braun & Gillian Flaccus, *California Man Confirms Role In Anti-Islam Film*, ASSOC. PRESS (Sept. 13, 2012), http://bigstory.ap.org/article/california-man-confirms-role-anti-islam-film.

summons you!"[204] At another point, an overdubbed woman asks "Is your Muhammad a child molester?"[205] Other examples of overdubbing include:

- "Islamic Egyptian police arrested 1400 Christians."[206]
- "*His name is Muhammad.* And we can call him 'the father unknown.'"[207]
- "And in all my young life *I have not seen such a murderous thug as Muhammad*."[208]

The video includes additional examples of cruelty, as it shows "Muhammad" aging and gaining more power. Although this account is not exhaustive, any such attempt would be futile because the plot is close to incomprehensible. The reaction of the actors and of the Islamic world, however, is much clearer as discussed below.

B. Response of Actors in the Video

Unsurprisingly, the actors appearing in *Innocence of Muslims* were horrified to learn of the overdubs, some fearful of reprisal. A joint statement issued by the actors stated "they were misled about the project and said some of their dialogue was crudely dubbed

---

[204] *Innocence of Muslims*, *supra* note 189; Abdurrahman, *supra* note 203.

[205] *Innocence of Muslims*, *supra* note 189; Abdurrahman, *supra* note 203.

[206] *Innocence of Muslims*, *supra* note 189; Abdurrahman, *supra* note 203.

[207] Only the italicized portion appears to be overdubbed. *Innocence of Muslims*, *supra* note 189; Abdurrahman, *supra* note 203.

[208] Only the italicized portion appears to be overdubbed. *Innocence of Muslims*, *supra* note 189; Abdurrahman, *supra* note 203. In this excerpt, lip-reading suggests that the actress is speaking all of the words quoted above except for "Muhammad"; however, the italicized portion appears to be out of sync and overdubbed. Thus, the italicized portion appears to be an overdub with the substitution of "Muhammad" for another word, apparently "George" or "you." The phrase apparently spoken by the actress during filming was "And in all my young life, I have not seen such a murderous thug as *George*" or perhaps "as *you*."

during post-production."[209] Most notably, actress Cindy Lee Garcia publicly decried the film and attempted to force YouTube to remove the video.[210] Garcia stated she had been given a small portion of the script for a film entitled "Desert Warriors" and "had no idea she was participating in an offensive spoof" about Muhammad.[211] In fact, Garcia plays the character whose voice was overdubbed to state "Is your Muhammad a child molester?"[212]

During filming, Muhammad was called "Master George," with "Muhammad" dubbed in post-production," said Garcia.[213] She was "horrified when she saw the end product, and when protesters in Libya killed four U.S. Embassy employees."[214] She later filed suit against YouTube in Los Angeles Superior Court alleging fraud, invasion of privacy, and other claims;[215] a temporary restraining order was denied.[216] She subsequently filed a second lawsuit alleging copyright infringement, arguing that she owns the copyright to her scenes in the video and that the altered audio constitutes an infringement.[217]

---

[209] Braun & Flaccus, *supra* note 203; *see also* Phil Willon & Rebecca Keegan, *'Innocence of Muslims': Mystery shrouds film's California origins*, L.A. TIMES (Sept. 12, 2012), http://articles.latimes.com/2012/sep/12/world/la-fg-libya-filmmaker-20120913.

[210] Adrien Chen, *'It Makes Me Sick': Actress in Muhammed Movie Says She Was Deceived, Had No Idea It Was About Islam*, GAWKER (Sept. 12, 2012), http://gawker.com/5942748/it-makes-me-sick-actress-in-muhammed-movie-says-she-was-deceived-had-no-idea-it-was-about-islam; *see also* Edward Lee, *Can Copyright or YouTube Save Cindy Lee Garcia From "Innocence of Muslims" Video Fallout?*, THE HUFFINGTON POST (Oct. 2, 2012), http://www.huffingtonpost.com/edward-lee/youtube-save-cindy-lee_b_1926905.html.

[211] Chen, *supra* note 210.

[212] *See supra* text accompanying note 205.

[213] *See* Chen, *supra* note 210.

[214] *Id.*

[215] *See* Garcia v. Nakoula, No. BC492358 (Cal. Super. Ct. filed Sept. 19, 2012) (complaint).

[216] Miguel Marquez, *Judge: YouTube Doesn't Have to Take Down Anti-Islam Video*, CNN (Sept. 21, 2012), http://www.cnn.com/2012/09/20/tech/california-anti-islam-film.

[217] *Lee*, *supra* note 210. As Professor Edward Lee points out, Garcia's assertion of authorship may fail under the joint-authorship doctrine of copyright law.

Regarding the mysterious creator of the video, the Wall Street Journal spoke in Sept. 2012 to a person identifying himself as Sam Bacile.[218] This person "characterized the film as a political effort to call attention to the hypocrisies of Islam."[219] He "claimed to be the film's writer, director and producer," and claimed to have made a two-hour film in 2011 in California.[220] He claimed to be "Israeli-American and that he raised $5 million from about 100 Jewish donors"; however, the Wall Street Journal later corrected the story, indicating that those claims were not confirmed and should not have been included in the article.[221] "Bacile" (apparently a pseudonym) said the film is "not designed to attack Muslims but to show the destructive ideology of Islam," and that it "reveals in a satirical fashion the life of Muhammad."[222] NPR reported that its "library did not turn up any footprint for Bacile" and "found no property, phone, licenses or court records."[223] According to The Associated Press, "Bacile" appears to be a pseudonym, and attention has since focused on a man named Nakoula Basseley Nakoula, who was arrested for alleged probation violations shortly after the controversy arose in September 2012.[224]

Id.; *see also* Aalmuhammed v. Lee, 202 F.3d 1227 (9th Cir. 1999).

[218] Bradley & Nissenbaum, *supra* note 196.

[219] *Id.*

[220] *Id.*

[221] *Id.* According to NPR, "Bacile" told The Associated Press he was an Israeli Jew and a real estate developer, "but Israeli authorities told the wire service they have no records of him being a citizen." Peralta, *supra* note 196; Braun & Flaccus, *supra* note 203. As Professor Jay Sterling Silver points out, "a cursory attempt to check the facts would have revealed, no Sam Bacile — the alleged creator of the video screed — ever walked the earth." Jay Sterling Silver, *Blaming the Jews: Old Wine in a New Bottle*, TIKKUN DAILY (Sept. 20, 2012), http://www.tikkun.org/tikkundaily/2012/09/20/blaming-the-jews-old-wine-in-a-new-bottle/.

[222] Bradley & Nissenbaum, *supra* note 196.

[223] Peralta, *supra* note 196.

[224] The Associated Press (AP) spoke to someone using the name of Nakoula Basseley Nakoula, who said he was a Coptic Christian and that the film expressed "the concerns of Christian Copts about their treatment by Muslims." Braun & Flaccus, *supra* note 203. According to the AP, Nakoula claimed to have worked on logistics for *Innocence of Muslims* but denied directing the film. *Id.* Nakoula

C. Protests and Violence

Although the videos were posted to YouTube in early July 2012, they did not attract much attention until an Egyptian TV program showed clips, describing them as "the work of Terry Jones, the Florida pastor who has burned Qurans."[225] "Egyptian clerics began widely condemning the footage."[226] There were protests, some violent, and some leading to deaths, in Afghanistan, Algeria, Egypt,[227] the Gaza Strip, India, Iran, Iraq, Lebanon, Libya,[228] Nige-

---

denied posing as Bacile. *Id.* However, "the cell phone number that AP contacted [] to reach the filmmaker who identified himself as Sam Bacile traced to the same address near Los Angeles where AP found Nakoula." *Id.* Further, "[f]ederal court papers said Nakoula's aliases included Nicola *Bacily*, Erwin Salameh and others." *Id.* (emphasis added). According to the AP, Nakoula "pleaded no contest in 2010 to federal bank fraud charges in California" arising from what a prosecutor described as "basically a check-kiting scheme." *Id.*; *see also* Nick Carbone & Madison Gray, *Friends of 'Sam Bacile': A Who's Who of the Innocence of Muslims Film*, TIME NEWSFEED (Sept. 13, 2012), http://newsfeed.time.com/2012/09/13/friends-of-sam-bacile-a-whos-who-of-the-innocence-of-muslims-film-project/ (stating that "[a]ccording to federal attorneys, [Nakouola] was involved in a fraud scheme in which he would set up fake bank accounts using stolen Social Security numbers"). After the *Innocence of Muslims* scandal, federal authorities arrested Nakoula on a probation violation charge, including allegedly making false statements to his probation officer and using aliases. *See Feds Arrest Producer Of Controversial Anti-Islam Film On Probation Violation Charge*, THE SMOKING GUN (Sept. 27, 2012), http://www.thesmokinggun.com/buster/feds-arrest-nakoula-578341. According to *The Smoking Gun*, Nakoula's probation terms included limitations on the use of the Internet without pre-approval of his probation officer. THE SMOKING GUN, *Federal Probation*, *supra* note 190.

[225] Peralta, *supra* note 196. According to the *Wall Street Journal*, Jones was actually only promoting the film, and had planned to "screen the trailer at his church on Sept. 11." *Id.*; *see also* Bradley & Nissenbaum, *supra* note 196.

[226] Bradley & Nissenbaum, *supra* note 196.

[227] "In Cairo, protesters said they rallied to the embassy at the prompting of Islamist Facebook groups and hard-line Salafi preachers who frequently preach on Islamist satellite channels." Bradley & Nissenbaum, *supra* note 196. In addition to the protests, an Egyptian court sentenced seven Christian Egyptian participants in the film to death. *See Innocence of Muslims participants sentenced to death in Egypt*, THE GUARDIAN (Nov. 28, 2012), http://www.guardian.co.uk/world/2012/nov/28/innocence-of-muslims-death-sentence.

[228] There were attacks against the U.S. consulate in Libya, leading to the deaths of Ambassador J. Christopher Stevens and three others. *See* Matthew Lee,

ria, Pakistan,[229] Sudan, Tunisia, Turkey, as well as many other countries around the globe.[230] Many were injured or killed.[231]

D. Google's Handling of the Video

That the video served as a globally disruptive event is unsurprising in retrospect. As Milton Mueller notes, the "rise of an Internet centered in the United States was a disruptive event in the system of international relations formed around communication and information policy."[232] After the controversy erupted, demands ensued for removal of the video. Even the Obama administration took the unprecedented step of suggesting—but not demanding—that

---

Benghazi Attack Report Finds Systematic Management Failures at State Department Led to Inadequate Security, HUFFINGTON POST (Dec. 18, 2012), http://www.huffingtonpost.com/2012/12/18/benghazi-attack-report-state-department_n_2326637.html. Initial reports suggested the attack was tied to a protest. *See, e.g.*, Bradley & Nissenbaum, *supra* note 196; Peralta, *supra* note 196. However, despite initial accounts suggesting that the attack was tied to protests arising from *Innocence of Muslims*, an independent panel charged with investigating the attack concluded that "there was no protest outside the consulate and said responsibility for the incident rested entirely with the terrorists who attacked the mission." *Id.*

[229] *See Death, destruction in Pakistan amid protests tied to anti-Islam film*, CNN (Sept. 21, 2012), http://www.cnn.com/2012/09/21/world/anti-islam-film-protests. One source says at least 19 died. *See* Christopher Zara, *'Innocence of Muslims' Protests: Death Toll Rising In Pakistan*, INT'L BUS. TIMES (Sept. 21, 2012), http://www.ibtimes.com/%E2%80%98innocence-muslims%E2%80%99-protests-death-toll-rising-pakistan-794296.

[230] An interactive map of the protests can be found at *The Daily Beast*, a *Newsweek* publication. *See* Michael Keller & Eliza Shapiro, *Interactive Map: Who's Protesting Where*, THE DAILY BEAST (Sept. 15, 2012), http://www.thedailybeast.com/articles/2012/09/15/interactive-map-who-s-protesting-where.html. Similarly, a helpful timeline can be found at the same site. *See* Michael Keller & Andrew Carter, *Interactive Timeline of Clashes in the Middle East*, THE DAILY BEAST (Sept. 13, 2012), http://www.thedailybeast.com/articles/2012/09/13/interactive-timeline-of-clashes-in-the-middle-east.html.

[231] For example, on Sept. 21, 2012, at least 19 people were reported to have died as a result of protests in Pakistan. *See, e.g.*, Zara, *supra* note 229.

[232] MUELLER, *supra* note 37, at 55.

YouTube remove the video.[233] Google, which owns YouTube, refused the request, stating that "it had already determined that the video did not violate its terms of service regarding hate speech."[234] Google stated that the video would stay up "because it is against the Islam religion but not Muslim people."[235] However, Google did block access around that time in India and Indonesia due to laws in those jurisdictions.[236] It also at that time "temporarily blocked" the video in Egypt and Libya,[237] and blocked it in Singapore and Malaysia.[238] Even months later, the issue was still simmering in Egypt where a "Cairo court ordered the government to block access to the video-sharing Web site YouTube for 30 days for carrying an anti-Islam film that set off deadly riots last year, but the ruling can be appealed and, based on precedent, may not be enforced."[239] The video was restricted in a number of other countries as well, including Russia, Turkey, and Saudi Arabia.[240] From the information currently available, it appears that the video is blocked by using computer techniques that determine the geographical location from which a user is attempting to access the video.[241] If the user is located in a region where the video is banned on YouTube, then the user cannot

---

[233] Claire Cain Miller, *Google Has No Plans to Rethink Video Status*, N.Y. TIMES (Sept. 15, 2012), http://www.nytimes.com/2012/09/15/world/middleeast/google-wont-rethink-anti-islam-videos-status.html.

[234] *Id.*

[235] *Id.*

[236] *Id.*

[237] *Id.*

[238] *Google blocks Singapore access to anti-Islam film*, YAHOO! NEWS (Sept. 21, 2012), sg.news.yahoo.com/singapore-asks-google-block-access-islam-film-054710633.html.

[239] *Egypt Court Orders Block on YouTube Access*, N.Y. TIMES (Feb. 9, 2013), http://www.nytimes.com/2013/02/10/world/middleeast/egypt-court-orders-block-on-youtube-over-anti-islam-video.html.

[240] Google, *Transparency Report, Requests to Remove Content, From Governments: Notable Observations – July to December 2012*, http://www.google.com/transparencyreport/removals/government/ (last visited Sept. 29, 2013).

[241] Ozge Ozbilgin, *YouTube opens Turkish site, giving government more control*, REUTERS (Oct. 2, 2012), http://mobile.reuters.com/article/idUSBRE8910T420121002?irpc=932.

see it.[242]

III. Human Rights Law and Principles

In his 2012 State of the Union Speech, President Barack Obama stated:

> In the Middle East, we will stand with citizens as they demand their universal rights, and support stable transitions to democracy. . . .
>
> We know the process will be messy, and we cannot presume to dictate the course of change in countries like Egypt, but we can — and will — insist on respect for the fundamental rights of all people.[243]

Considering the international scope of most Super-Intermediaries, it is not surprising that they may face difficult speech challenges, ones that fall outside the more litigated box of intellectual property. The *Innocence of Muslims* video is particularly vexing. This Part therefore discusses the International Bill of Human Rights and provisions that are of particular interest to Super-Intermediaries regarding speech and religion. It notes tension between such provisions, and closes by noting a significant industry group that proposes using portions of the International Bill of Human Rights as a model for intermediaries to better respect human rights.

A. The International Bill of Human Rights

Although Super-Intermediaries are not state actors clearly bound by all aspects of human rights law, they exercise considerable

---

[242] *Id.*

[243] President Barack H. Obama, *State of the Union Address* (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

power.[244] As Professor Molly Land notes, "the activities of non-state actors are playing an increasingly central role in regulating access to expression and culture."[245] Thus, even though Super-Intermediaries are non-state actors,[246] there may be compelling principles of self-guidance to be found by looking to international human rights law. Indeed, as Professor Peter Yu states, "many U.N. human rights bodies, nongovernmental organizations, and commentators hold the view that private actors, including content providers, bear some human rights responsibilities."[247] Rebecca MacKinnon chides corporate executives who "argue that human rights are neither their concern nor their responsibility."[248] Awareness of the role of internet intermediaries in the context of human rights law is growing. In 2011, a *Joint Declaration on Freedom of Expression and the Internet* signed by representatives of multiple organizations stated that more attention should be given to "alternative, tailored approaches, which are adapted to the unique characteristics of the Internet" to respond

---

[244] Schmidt and Cohen go so far as to argue that actual states will ultimately develop separate sets of foreign and domestic policies for both realspace and cyberspace. *See* SCHMIDT & COHEN, *supra* note 19, at 255. This may further suggest that Super-Intermediaries are increasingly carving out quasi-state actor status. This reinforces the need to identify Super-Intermediaries and to consider what responsibilities they ought to have. *See also* MACKINNON, *supra* note 14, at 141 (noting that commercial services are not required to uphold the First Amendment or Article 19 of the UDHR).

[245] Molly Land, *Region Codes and Human Rights*, 30 CARDOZO ARTS & ENT. L.J. 275, 281 (2012) [hereinafter Land, *Region Codes*]. Professor Land argues in a recent paper that the drafting history of Article 19(2) of the ICCPR, regarding freedom of expression, suggests that the Article applies directly to non-state actors such as internet intermediaries. *See* Land, *Law of Internet*, supra note 26, at 445-46.

[246] *See supra* notes 36-37 (discussing corporate social responsibility and human rights).

[247] Peter K. Yu, *Region Codes and the Territorial Mess*, 30 CARDOZO ARTS & ENT. L.J. 187, 229 (2012) [hereinafter Yu, *Region Codes*]. Along similar lines, Milton Mueller notes that "the distributed architecture of the Internet and flexibility of information technology" make it difficult for states or any particular private actor to exercise control. MUELLER, *supra* note 37, at 80. This helps to explain why governments have moved towards accepting a "division of responsibility between state and nonstate actors" regarding Internet administration. *Id.*

[248] MACKINNON, *supra* note 14, at xxiii.

to illegal internet content.[249] The *Joint Declaration* also noted the central role of intermediaries, stating that "[s]elf-regulation can be an effective tool in redressing harmful speech, and should be promoted."[250]

To keep focus on the foundational norms of human rights, however, this article will focus primarily on the key documents of human rights as contained in The International Bill of Human Rights, which consists of three major documents along with several protocols.[251] The first document is the Universal Declaration of Human Rights (UDHR), a declaration of the United Nations General Assembly in 1948.[252] The others, the Covenants, are multilateral treaties that elaborate on the UDHR: The International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[253] The two treaties were adopted in 1966 and went into effect in 1976.[254]

The UDHR was "the first occasion on which the organized community of nations had made a Declaration of human rights and fundamental freedoms."[255] Although the UDHR may not represent binding international law, most articles of the document are "widely believed to have acquired the status of customary international law,

---

[249] Joint Declaration on Freedom of Expression and the Internet ¶ 1(d) (adopted June 1, 2011), http://www.osce.org/fom/78309 [hereinafter Joint Declaration]. The *Joint Declaration* was signed by U.N. Special Rapporteur Frank La Rue as well as representatives and holders of special mandates for the Organization for Security and Co-operation in Europe, the Organization of American States, and the African Commission on Human and Peoples' Rights. *Id.* pmbl.; *see also* Michael Karanicolas, *Understanding the Internet as a Human Right*, 10 CAN. J. L. & TECH. 263, 269 (2012).

[250] Joint Declaration, *supra* note 249, ¶ 1(e); *see also* Karanicolas, *supra* note 249, at 269 (discussing Joint Declaration).

[251] *See* Fact Sheet No.2 (Rev.1), The Int'l Bill of Human Rights, at 1, http://www.ohchr.org/Documents/Publications/FactSheet2Rev.1en.pdf [hereinafter Int'l Bill of Human Rights, Fact Sheet].

[252] UDHR, *supra* note 43.

[253] ICCPR, *supra* note 44; ICESCR, *supra* note 45. The International Bill of Human Rights also includes two protocols to the ICCPR. *See* Int'l Bill of Human Rights, Fact Sheet, *supra* note 251, at 1.

[254] *See* ICCPR, *supra* note 44; ICESCR, *supra* note 45.

[255] Int'l Bill of Human Rights, Fact Sheet, *supra* note 251, at 2-3.

and [to] represent[] 'the single most authoritative source of human rights norms.'"[256]

Regarding the covenants, the ICCPR focuses primarily on civil and political rights.[257] A total of 167 states have ratified, acceded, or succeeded to the ICCPR.[258] In addition to the United States, this list includes a number of Islamic states, such as Bahrain, Egypt, Iran, Iraq, Jordan, Lebanon, Libya, Pakistan, Sudan, Syria, and Turkey.[259] Seven nations, including China and Cuba, have signed but not ratified.[260] Saudi Arabia is not a signatory.[261] Also, there are

---

[256] Mirela V. Hristova, *Are Intellectual Property Rights Human Rights?*, 93 J. PAT. & TRADEMARK OFF. SOC'Y 339, 342 (2011) (quoting Paul Torremans, *Is Copyright a Human Right*, 2007 MICH. ST. L. REV. 271, 277 (2007)). As Professor Roza Pati notes, "[t]he focal point of the customary human rights law argument has always been the [UDHR]." ROZA PATI, DUE PROCESS AND INTERNATIONAL TERRORISM: AN INTERNATIONAL LEGAL ANALYSIS 113 (2009). She further concludes that the UDHR's "generality and simplicity" may provide a "rallying" point that is "more effective[] than the hard and detailed law chiseling the scope and limits of each right" in the ICCPR and ICESCR. *Id.* Further, the "great majority" of the UDHR's provisions have been incorporated in state practice or constitutions, meaning "that they can be considered to have been maturing into state obligations under customary international law." *Id.* at 113-14.

[257] The ICCPR focuses on a broad swath of important matters of civil and political rights. A sampling includes protection the right to life (art. 6), prohibitions of torture, slavery, and arbitrary arrest (art. 7-9), and limitations on expulsions of aliens lawfully in a State (art. 13). Int'l Bill of Human Rights, Fact Sheet, *supra* note 251, at 4-5. It also includes provisions regarding due process and equal protection (art. 14-16, 26), privacy (art. 17), freedom of thought, conscience and religion (art. 18), and freedom of opinion and expression (art. 19). *Id.* at 5. It further "calls for the prohibition by law of any propaganda for war and of any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (art. 20)." *Id.* It address the right of assembly and association (art. 21-22), matters of family and protection of children (art. 23-24), and rights regarding public affairs, voting, election, and engaging in public service (art. 25). *Id.* It "also calls for protection of the rights of ethnic, religious and linguistic minorities in the territories of States [sic] parties (art. 27)." *Id.*

[258] International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171, 282, *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en [hereinafter ICCPR Declarations/Reservations].

[259] *Id.*

[260] *Id.*

[261] *Id.*

two optional protocols for the ICCPR, the first of which permits countries to allow persons to complain to the Human Rights Committee (HRC) about violations.[262] To date, 114 countries are parties to this protocol, although the United States has not signed it.[263] With the exception of Libya and Turkey, none of the signatory Islamic states noted above have joined the first optional protocol.[264]

The ICESCR, also a multilateral treaty, focuses primarily on economic, social, and cultural rights.[265] So far, 160 states have ratified, acceded, or succeeded to the ICESCR, including the Islamic states noted above.[266] Another seven nations have signed but have not yet ratified, acceded, or succeeded, including the United States and Cuba.[267] Again, Saudi Arabia is not a signatory.[268]

B. Provisions of Interest to Super-Intermediaries

As noted by Professor Roy Balleste, international human

---

[262] Optional Protocol to the International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 302-05, *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-5&chapter=4&lang=en [hereinafter ICCPR, First Optional Protocol]; *see also* Second Optional Protocol to the International Covenant on Civil and Political Rights, Aiming at the Abolition of the Death Penalty, July 11, 1991, 1642 U.N.T.S. 414, *available at* http://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=IV-12&chapter=4&lang=en.

[263] *See* ICCPR, First Optional Protocol, *supra* note 262.

[264] *Id.*

[265] The ICESCR recognizes a number of rights attendant to economic, social, and cultural matters, such as rights to work, working conditions, and labor organization (art. 6-8), social security, family protection and assistance (art. 9-10), an adequate standard of living with enjoyment of physical and mental health (art. 11-12), education (art. 13-14), and engagement in cultural life (art. 15). *See* ICESCR, *supra* note 45.

[266] International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3, *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-3&chapter=4&lang=en [hereinafter ICESCR Declarations/Reservations].

[267] *Id.*

[268] *Id.*

rights law "complement[s] Internet governance."[269] Professor Peter Yu similarly notes that it is only recently that "policy makers, scholars, and activists" have paid attention to the implications of intellectual property on human rights.[270] Although Super-Intermediaries are not state actors,[271] a number of provisions in the International Bill of Human Rights would appear to have analogous bearing on Super-Intermediaries. For example, privacy is addressed in Article 12 of the UDHR[272] and Article 17 of the ICCPR.[273] These provisions may have bearing regarding privacy violations by Super-Intermediaries that cavalierly misappropriate user information, or change privacy policies to user detriment. Property rights are also addressed, in Article 17 of the UDHR,[274] and perhaps also in UDHR Article 27(2)[275] and ICESCR Article 15(1).[276]

---

[269] Balleste, *supra* note 9, at 254.

[270] Peter K. Yu, *Intellectual Property and Human Rights in the Nonmultilateral Era*, 64 FLA. L. REV. 1045, 1049 (2012) [hereinafter Yu, *Nonmultilateral Era*] (citing LAURENCE R. HELFER & GRAEME W. AUSTIN, HUMAN RIGHTS AND INTELLECTUAL PROPERTY: MAPPING THE GLOBAL INTERFACE 1 (2011)).

[271] *Cf.* Yu, *Region Codes*, *supra* note 247, at 229 (noting that "[u]nder the ICESCR, only states can be held accountable for violating their human rights obligations").

[272] UDHR Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." UDHR, *supra* note 43, at art. 12.

[273] ICCPR Article 17 states:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR, *supra* note 44, at art. 17.

[274] UDHR Article 17 states: "1. Everyone has the right to own property alone as well as in association with others. 2. No one shall be arbitrarily deprived of his property." UDHR, *supra* note 43, art. 17.

[275] UDHR Article 27(2) states: "Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author." UDHR, *supra* note 43, art. 27(2). Professor Madhavi Sunder notes that such rights are also recognized in "countless other human rights instruments." MADHAVI SUNDER, FROM GOODS TO A GOOD LIFE:

INTELLECTUAL PROPERTY AND SOCIAL JUSTICE 90 (2012).

[276] ICESCR Article 15(1) states:

> 1. The States Parties to the present Covenant recognize the right of everyone:
>
> (a) To take part in cultural life;
>
> (b) To enjoy the benefits of scientific progress and its applications;
>
> (c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

ICESCR, *supra* note 45, art. 15(1). Article 15(1)(c) appears to include moral rights such as the *droit moral* found in Continental intellectual property systems. It could also arguably require protection of intellectual property rights. However, a U.N. Committee has stated that the human right contained in Article 15(1)(c) is distinguishable from "most legal entitlements recognized in intellectual property systems." United Nations Economic and Social Council, Comm. on Economic, Social and Cultural Rights, at 2, Gen'l Cmt. No. 17, 35th sess., Nov. 2005, *available at* http://www.unhchr.ch/tbs/doc.nsf/898586b1dc7b4043c1256a450044f331/03902145edbbe797c125711500584ea8/$FILE/G0640060.pdf. The report continues:

> Human rights are fundamental as they are inherent to the human person as such, whereas intellectual property rights are first and foremost means by which States seek to provide incentives for inventiveness and creativity, encourage the dissemination of creative and innovative productions, as well as the development of cultural identities, and preserve the integrity of scientific, literary and artistic productions for the benefit of society as a whole.

Id. Thus, whereas human rights are "timeless expression of fundamental entitlements of the human person," intellectual property rights are typically "of a temporary nature, and can be revoked, licensed or assigned." *Id.*; *see also* Yu, *Nonmultilateral Era*, *supra* note 270, at 1052-54 (discussing General Comment 17).

In the author's view, it is not important for purposes of this article whether or not the ICESCR can or should be read to embrace a human right to intellectual property protection. Indeed, at this point of time, intellectual property rights are extremely well-developed as a matter of positive law. Additionally, Super-Intermediaries tend to have advanced processes for recognizing and attempting to respect intellectual property rights. *See supra* text accompanying notes 86-103; *infra* Part IV.B (further discussing codes of information control). The dilemma facing Super-Intermediaries is thus *not* a lack of intellectual-property controls; it is instead developing processes and code to deal with disputes *other* than those arising under intellectual property laws. Thus, the main text focuses primarily on the tension between speech and religion. Having said that, it should be noted that Professor Sunder argues that "[h]uman rights are a principal source for delimiting intellectual property, just simply expanding it." SUNDER, *supra* note 275, at 101-

Considering this article's discussion of *Innocence of Muslims*, it is interesting to consider the International Bill of Human Rights' treatment of freedom of expression and freedom of religion. Regarding freedom of expression, Article 19 of the UDHR states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[277]

On its face, this statement is a worthy principle of free speech. Similarly, Article 19(2) of the ICCPR states:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[278]

Again, this statement is admirable. However, the rights delimited in ICCPR Article 19(2) appear to be subject to restrictions in ICCPR Article 19(3):

> The exercise of the rights provided for in paragraph 2 of

02.

[277] UDHR, *supra* note 43, at art. 19; *see also* Balleste, *supra* note 9, at 239 (noting that final report of the Geneva Phase of the WSIS in 2003 "reaffirmed Articles 19 and 29" of the UDHR).

[278] ICCPR, *supra* note 44, at art. 19(2); *see also* Balleste, *supra* note 9, at 242 (noting that "[t]hanks to the power of the Internet, human rights have increasingly been discussed around the world," including Article 19(2)). In a fascinating paper addressing the drafting history of ICCPR Article 19(2), Professor Molly Land points out that Article 19(2) protects not just expression, "but also its medium." Land, *Law of Internet*, supra note 26, at 401. It would therefore protect, among other things, the "right to seek information and to access technology." *Id.* at 418.

> this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.[279]

Interestingly, the rights are conditioned upon "special duties and responsibilities," evoking the vow of "great responsibility" noted at the beginning of this article.[280] Of more pressing concern, however, is the palpable tension between Articles 19(2) and 19(3), which would permit law to limit the freedom of expression in favor of protection, for example, of the "reputations of others" or of morals.[281] Could this permit laws limiting public criticism or commentary? Could it permit the prohibition of truthful speech that nevertheless harms a person's reputation?

The quandary and the tension both deepen when one considers the provisions regarding religion. Article 18 of the UDHR states:

> Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.[282]

Like the UDHR's provision on speech, its language regarding religion appears to be a very good thing, and on its face does not create a conflict. Much of the same can be said about Article 18(1)

---

[279] ICCPR, *supra* note 44, at art. 19(3).

[280] *See supra* text accompanying note 1.

[281] *Compare* ICCPR, *supra* note 44, at art. 19(2), *with* ICCPR, *supra* note 44, at art. 19(3).

[282] UDHR, *supra* note 43, at art. 18.

of the ICCPR:

> Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching.[283]

Again, Article 18(1) of the ICCPR does not expressly conflict with the speech provisions found in Article 19(2) of the ICCPR. However, the tensions expand geometrically when we turn to Article 20(2) of the ICCPR:

> Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.[284]

To sum up, there may be considerable tension within the ICCPR regarding speech in two ways.[285] The next two subsections

---

[283] ICCPR, *supra* note 44, at art. 18(1).

[284] *Id.* at art. 20(2). Along somewhat similar lines, Article 18(3) of the ICCPR provides:

> Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others.

Id. at art. 18(3). Professor Peter Yu points to similar tensions within human rights law, such as "internal" conflicts "between rights protecting the human rights attributes of intellectual property and other forms of human rights." Yu, *Nonmultilateral Era*, *supra* note 270, at 1095-96; *see also* Peter K. Yu, *Reconceptualizing Intellectual Property Interests in a Human Rights Framework*, 40 U.C. DAVIS L. REV. 1039, 1078 (2007) (noting approaches taken by scholars to internal conflicts).

[285] Moreover, "[t]he ICCPR does not contain any provisions giving International Human Rights treaty bodies—including the [Human Rights Council] and the [International Court of Justice]—the authority to promulgate binding legal interpretations of the various International Human Rights Treaties." Davie Mennie, Note, *The Role of the International Covenant on Civil and Political Rights in the*

will respectively address tensions between ICCPR Articles 19(2) and (3), and between ICCPR Articles 19(2) and 20(2):

1. Expression Comes with "Responsibilities" and "Restrictions"

Thus, we see yet another version of the power/responsibilities mantra: here, it is the ICCPR stating that the right of expression comes with "responsibilities."[286] The human right to freedom of expression is a qualified one, contingent upon responsibilities that permit restrictions for the: 1) rights of others; 2) reputations of others; 3) protection of national security; 4) protection of public order; 5) public health; and 6) morals.[287] As Professor Roza Pati notes, "as in all catalogs of basic rights, the ICCPR provides the possibility of restricting rights for reasons of overriding general public interest or overriding interests of others, thereby circumscribing the legal ambit of individual freedom."[288] Professor Pati further points out, however, that the HRC "stresses that the core of the right should not be jeopardized" by restrictions on the freedom of expression.[289]

For any internet service provider, literal application of these requirements would decimate the ability to provide large swaths of internet speech. For instance, consider number two, reputations of

---

Israeli-Palestinian Conflict: Should Israel's Obligations under the Covenant Extend to Gaza and the Other Occupied Palestinian Territories?, 21 TRANSNAT'L L. & CONTEMP. PROBS. 511, 535 (2012) (discussing Michael J. Dennis, *Non-Application of Civil and Political Rights Treaties Extraterritorially During Times of International Armed Conflict*, 40 ISR. L. REV. 453, 458-60 (2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1032167).

[286] ICCPR, *supra* note 44, at art. 19(3).

[287] *Id.*

[288] Roza Pati, *Rights and Their Limits: The Constitution for Europe in International and Comparative Legal Perspective*, 23 BERKELEY J. INT'L L. 223, 242-43 (2005).

[289] *Id.* at 246 (discussing ICCPR Human Rights Committee, General Comment 10, Article 19 (Nineteenth session, 1983), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1, at 133 (May 12, 1994), *available at* http://www.unhchr.ch/tbs/doc.nsf/0/ca12c3a4ea8d6c53c1256d500056e56f/$FILE/G0441302.pdf).

others. It is often impossible for an internet intermediary to know whether speech posted online by a user is defamatory.[290] But on its face, ICCPR Article 19(3)(a) could be understood to prohibit speech that harms reputations *even if true*. In addition, the fourth restriction, protection of public order, could be read to prohibit speech critical of governmental officials. The same might be said of number six, protection of morals, which could arguably be read to prohibit speech critical of majoritarian interests regarding religion, culture, or gender orientation.[291]

---

[290] *Cf., e.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

> If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.

Id. at 333.

[291] As one author put it, "[t]hese loopholes, unfortunately, afford states great latitude in formulating justifications for silencing speech." Geoffrey A. Hoffman, *In Search of an International Human Right to Receive Information*, 25 LOY. L.A. INT'L & COMP. L. REV. 165, 172 (2003). In comparison, the European Convention's speech provision, Article 10, has some additional protection. Whereas Article 10 is somewhat similar to Articles 19(2) and (3) of the ICCPR in permitting restrictions on speech, in contrast, Article 10 includes the more stringent requirement that a restriction of expression be "necessary in a democratic society." *Id.* at 175; *see also* European Convention on Human Rights, art. 10(2), Nov. 4, 1950, 213 U.N.T.S. 221, *available at* http://www.echr.coe.int/Documents/Convention_ENG.pdf.

Although ICCPR Article 19(3) has a "necessity" requirement, the requirement is not expressly conditioned on democratic ideals, and since it is tied to the extremely broad protected subject matter (morals, public health, public order, reputations of others), the necessity requirement is on its face a very weak limitation on restrictions. But as Professor Madhavi Sunder states, "[f]reedom to participate in cultural life stands at the very core of *liberty*." SUNDER, *supra* note 275, at 11 (emphasis in original). Accordingly, restrictions on the freedom of expression, a critical component in participating in culture whether as creator or consumer, should be written narrowly and be narrowly construed.

Under ICCPR Article 19(3), "states can impose reasonable limits on expression as long as these limits satisfy the requirements of human rights law."[292] However, it should be noted that the U.N. Special Rapporteur Frank La Rue has stated that Article 19(3)'s restrictions on speech should not be broadly construed, and should instead be subject to a 3-part test:

> (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and
>
> (b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and
>
> (c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).[293]

Although La Rue's three-part test is a helpful limitation of the language of Article 19(3), it remains a problematic provision. At least from an American perspective, it is extremely doubtful that even La Rue's narrowed interpretation—which would still allow speech restrictions for matters "of public health or morals"—would pass muster under the First Amendment.[294] Indeed, the United

---

[292] Land, *Region Codes*, *supra* note 245, at 280.

[293] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc.A/HRC/17/27 (May 16, 2011) (Frank La Rue), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf; *see also Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/14/23, ¶¶ 72-87 (Apr. 20, 2010) (Frank La Rue), http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf (also discussing ICCPR Article 19(3)); MACKINNON, *supra* note 14, at 199 (discussing 2011 report); Land, *Region Codes*, *supra* note 245, at 280 (discussing same).

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

States' ratification was subject to a number of reservations, declarations, understandings, including the declaration that the ICCPR would not affect the scope of freedom of expression under the Constitution.[295]

2. Expression Rights and Criticism of Religion

There are additional reasons to take care regarding using the ICCPR as a model for Super-Intermediaries, particularly in the context of the *Innocence of Muslims* video. As noted previously, although the ICCPR provides a right of expression in Article 19(2), that right may be subject to Article 20(2), which provides: "[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."[296] On its face, this is very strong language, which would appear to require member states to put into effect implementing legislation that would prohibit such speech. Unsurprisingly, the United States took a reservation against Article 20, stating that "article 20 does not authorize or require legislation or other action by the United States that would restrict the right of free speech and association protected by

---

[295] "The United States declares that it will continue to adhere to the requirements and constraints of its Constitution in respect to all such restrictions and limitations [that might otherwise be permitted under the ICCPR]." U.S. reservations, declarations, and understandings, International Covenant on Civil and Political Rights, 138 Cong. Rec. S4781-01 (daily ed., April 2, 1992); The Senate further stated that "the United States declares that the provisions of Articles 1 through 27 of the Covenant are not self-executing." *Id.*; *see also* ICCPR Declarations/Reservations, *supra* note 258 (noting reservations of United States); U.N. Hum. Rts. Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, ¶ 596-606, U.N. Doc. CCPR/C/81/Add.4 (Aug. 24, 1994) (detailing U.S. reservation to Article 20(2)).

[296] ICCPR, *supra* note 44, art. 20(2). In fact, Professor Peter Danchin argues that "[n]othing in the Covenant on Civil and Political Rights supports the view that article 19 is necessarily hierarchically superior to article 18 and, conversely, article 20(2) in fact *requires* states to prohibit by law advocacy of religious hatred rising to the level of inciting discrimination, hostility or violence." Peter G. Danchin, *Of Prophets and Proselytes: Freedom of Religion and the Conflict of Rights in International Law*, 49 HARV. INT'L L.J. 249, 293 (2008).

the Constitution and laws of the United States."[297]

Others have written about the problematic nature of Article 20(2) or the issue of defamation of religion.[298] One scholar notes that under the ICCPR, "there is clearly a certain degree of international consensus that the right of freedom of religion must, in order to be meaningfully protected, entail a right to be free from insults and offense directed at one's religious practices, beliefs or teachings."[299] Others are more direct, with one stating "Article 20(2) constitutes a clear restriction on hate speech,"[300] and that under the record of disputes heard by the HRC, it appears "that under the ICCPR *hate speech restrictions are not considered anti-democratic*."[301]

---

[297] U.S. Reservations, Declarations, and Understandings, International Covenant on Civil and Political Rights, 138 Cong. Rec. S4781-01 (daily ed., April 2, 1992).

[298] *See* Robert C. Blitt, *Defamation of Religion: Rumors of its Death are Greatly Exaggerated*, 62 CASE W. RES. L. REV. 347 (2011); Danchin, *supra* note 296; Puja Kapai & Anne S. Y. Cheung, *Hanging in a Balance: Freedom of Expression and Religion*, 15 BUFF. HUM. RTS. L. REV. 41 (2009); Leonard A. Leo et al., *Protecting Religions from "Defamation": A Threat to Universal Human Rights Standards*, 34 HARV. J.L. & PUB. POL'Y 769 (2011); Qasim Rashid, *Pakistan's Failed Commitment: How Pakistan's Institutionalized Persecution of the Ahmadiyya Muslim Community Violates the International Covenant on Civil and Political Rights*, 11 RICH. J. GLOBAL L. & BUS. 1 (2011); Javaid Rehman & Stephanie E. Berry*, Is "Defamation of Religions" Passé? The United Nations, Organisation of Islamic Cooperation, and Islamic State Practices: Lessons from Pakistan*, 44 GEO. WASH. INT'L L. REV. 431 (2012); Jeroen Temperman, *Freedom of Expression and Religious Sensitivities in Pluralist Societies: Facing the Challenge of Extreme Speech*, 2011 B.Y.U. L. REV. 729.

[299] Kapai & Cheung, *supra* note 298, at 49; *see also* Danchin, *supra* note 296, at 288 (stating that although the ICCPR does not expressly ban attacks on injury to religious feelings, pointing reader towards ICCPR Articles 19(3) and 20(2)).

[300] Robin Edger, *Are Hate Speech Provisions Anti-Democratic?: An International Perspective*, 26 AM. U. INT'L L. REV. 119, 131 (2010).

[301] *Id.* at 134 (emphasis added) (describing disputes brought regarding government action in Canada and France). It should be noted, however, that the Special Rapporteur on Freedom of Religion or Belief noted that Article 20 "was drafted against the historical background of the horrors committed by the Nazi regime during the Second World War," and therefore, "expressions should only be prohibited under article 20 if they constitute incitement to imminent acts of violence or discrimination against a specific individual or group." U.N. Special

Yet another scholar notes the "challenge of dealing with religious sensitivities in pluralist societies" and that one may search the European Convention "in vain" for a provision equivalent to Article 20(2).[302] Interestingly, the HRC claims in General Comment 11 that the prohibitions on advocacy of religious hatred in Article 20 "are fully compatible with the right of freedom of expression as contained in article 19, the exercise of which carries with it special duties and responsibilities."[303] In contrast, Professor Peter Danchin states that this "assertion is open to question," considering reservations like that of the United States, which took reservation on the grounds that Article 20(2) infringes on freedom of expression.[304] He further notes that in the United States, "the First Amendment permits the limitation of expression intended, and likely, to result in imminent violence but not in the case of the incitement to discrimination or hostility or expression not likely to result in imminent violence," a "considerably narrower limitation of expression" than that required by Article 20(2).[305]

Rapporteur on Freedom of Religion or Belief and U.N. Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, Report Further to Human Rights Council Decision 1/107 on Incitement to Racial and Religious Hatred and the Promotion of Tolerance, ¶¶ 47, U.N. Doc. A/HRC/2/3 (Sept. 20, 2006), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G06/139/90/PDF/G0613990.pdf?OpenElement; *see also* Leo et al., *supra* note 298, at 779 (discussing report of Special Rapporteur).

[302] Temperman, *supra* note 298, at 738; *see also* European Convention on Human Rights, *supra* note 291, at art. 10(2).

[303] Human Rights Committee, General Comment 11, Article 20 (Nineteenth session, 1983), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1, at 134 (May 12, 1994), *available at* http://www.unhchr.ch/tbs/doc.nsf/0/ca12c3a4ea8d6c53c1256d500056e56f/$FILE/G0441302.pdf.

[304] Danchin, *supra* note 296, at 290 (citing U.N. Hum. Rts. Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, ¶ 597, U.N. Doc. CCPR/C/81/Add.4 (Aug. 24, 1994) (U.S.)).

[305] *Id.* at 291.

C. International Disagreement and "Defamation of Religion"

To some extent, reservations create a document that is not consistent in meaning or effect.[306] As previously stated, the United States takes a significant reservation regarding freedom of speech and ICCPR Article 20(2).[307] Analogously, a large number of western countries—Belgium, Denmark, Finland, Iceland, Ireland, Luxembourg, Netherlands, New Zealand, Norway, Sweden, and Switzerland, took various exceptions to Article 20(1), which prohibits propaganda for war.[308] Most of the exceptions were rooted in concerns over freedom of expression.[309] However, it appears that the United

---

[306] *See* Yu, *Nonmultilateral Era*, *supra* note 270, at 1063 ("Despite decades of efforts establishing the international human rights system, countries have yet to agree on the nature, scope, and meaning of human rights obligations."); *see also* Vienna Convention on the Law of Treaties, art. 19(c), May 23, 1969, 1155 U.N.T.S. 331, *available at* http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf (stating that reservations may not be "incompatible with the object and purpose of the treaty").

[307] *See supra* notes 295-97 and accompanying text.

[308] One example is Belgium:

> The Belgian Government declares that it does not consider itself obligated to enact legislation in the field covered by article 20, paragraph 1, and that article 20 as a whole shall be applied taking into account the rights to freedom of thought and religion, freedom of opinion and freedom of assembly and association [declared in provisions of the UDHR and ICCPR].

ICCPR Declarations/Reservations, *supra* note 258. Another example is Iceland, which took reservation to "Article 20, paragraph 1, with reference to the fact that a prohibition against propaganda for war could limit the freedom of expression." *Id.* Yet another example is Ireland:

> Ireland accepts the principle in paragraph 1 of article 20 and implements it as far as it is practicable. Having regard to the difficulties in formulating a specific offence capable of adjudication at a national level in such a form as to reflect the general principles of law recognised by the community of nations as well as the right to freedom of expression, Ireland reserves the right to postpone consideration of the possibility of introducing some legislative addition to, or variation of, existing law until such time as it may consider that such is necessary for the attainment of the objective of paragraph 1 of article 20.

Id.

[309] *Id.*

States is the only country to maintain a clear objection to Article 20(2).[310]

There are additional considerations beyond the face of the treaty that belie the international legal force of this provision of the ICCPR. For one, important stakeholders to this issue are not signatories. As noted, Islamic countries signing the ICCPR include Bahrain, Egypt, Iran, Iraq, Jordan, Lebanon, Libya, Pakistan, Sudan, Syria, and Turkey.[311] However, Islamic countries not signing include Saudi Arabia, as well as Malaysia, Oman, and the United Arab Emirates.[312]

Unsurprisingly and additionally, United Nations bodies have repeatedly addressed defamation of religion: for over a dozen years, Islamic states succeeded in obtaining passage of resolutions by United Nations bodies against defamation of religion, over dissent typically coming from western states.[313] In 2011, however, Resolution 16/18 of the U.N. Human Rights Council (UNHRC)[314] "[broke] the longstanding UNHRC practice of endorsing an annual resolution explicitly decrying defamation of religions."[315] Regardless, the

---

[310] Australia took a reservation, but only to assert that its existing legislation was sufficient to satisfy treaty obligations. *Id.* Liechtenstein and Switzerland had previously reserved the right to adopt a criminal provision to meet Article 20(2), but later withdrew their reservations. *Id.*

[311] ICCPR Declarations/Reservations, *supra* note 258.

[312] *Id.* It should be noted that Bahrain and Mauritania have made reservations to the ICCPR based on Sharia law. *Id.* Pakistan made a number of reservations based on Sharia law, including reservations to Article 19, to the consternation of a number of Western countries. *Id.* Most of Pakistan's reservations were withdrawn in 2011. *See Pakistan Decides to Withdraw Most of Reservations on ICCPR, UNCAT*, The Nation (June 23, 2011), http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/national/23-Jun-2011/Pakistan-decides-to-withdraw-most-of-reservations-on-ICCPR-UNCAT.

[313] *See* Blitt, *supra* note 298, at 347. After the first resolution in 1999, member states of the Organization for Islamic Cooperation "proclaimed that the motivation for insulting Islam stemmed only from the desire 'to generate conflict with Islamic peoples' and flatly asserted that 'the right to freedom of thought, opinion and expression could in no case justify blasphemy.'" *Id.* at 352.

[314] Human Rights Council Res. 16/18, Combating Intolerance, Negative Stereotyping and Stigmatization of, and Discrimination, Incitement to Violence and Violence Against, Persons Based on Religion or Belief, 16th Sess., Mar. 24, 2011, U.N. Doc. A/HRC/RES/16/18 (Apr. 12, 2011).

[315] Blitt, *supra* note 298, at 361 (discussing UNHRC Res. 16/18).

tension continues. As Professor Robert Blitt argues, although "defamation of religion *per se* might be on hiatus from the UN, absent additional clarification" the dispute will continue, risking the enablement of "an alternative framework for governments to continue justifying domestic measures that punish the exercise of freedom of expression and freedom of religion or belief in the name of protecting one or more select religious beliefs."[316]

Similarly, Professor Peter Danchin notes the approaches taken by the United States, European countries, and Islamic countries regarding these types of issues. Danchin's comments might be characterized as describing a sliding scale, with the United States placing priority on freedom of expression at one end, and Islamic countries giving primacy to preventing defamation of religion at the other.[317] In the middle is Europe, where "there has generally been a greater sensitivity shown to these countervailing factors and a genuine (albeit inconclusive) attempt to reconcile the competing claims of right at issue with regard to both the historical context of European intergroup relations and the relevant international human rights instruments."[318] Put differently, the world has not reached agreement regarding speech that might be characterized as defamatory of religion.[319]

D. Global Network Initiative

Might private actors do better? In 2008, a group of technology-minded entities, along with "human rights groups, socially responsible investors, and academics" formed the Global Network

---

[316] *Id.* at 351-52; *see also* Rehman & Berry, *supra* note 298, at 433 (noting "a continuing trend on the part of the OIC and its members towards the banning and criminalization of all forms of 'defamation of religions' and protecting and promoting analogous domestic anti-blasphemy laws").

[317] Danchin, *supra* note 191, at 282-83.

[318] *Id.* at 292.

[319] *See* Jillian C. York, *2012 in Review: How Blasphemy Laws Are Stifling Free Expression Worldwide*, EFF DEEPLINKS BLOG (Dec. 24, 2012), https://www.eff.org/deeplinks/2012/12/2012-review-how-blasphemy-laws-are-stifling-free-expression-worldwide.

Initiative (GNI).[320] As Rebecca MacKinnon describes it, the key challenge for the GNI is "daunting": "Given that there is basically no country on earth where government is not pressuring companies to do things that arguably infringe on citizens' rights, how do companies take practical steps to protect their customers' and users' rights to free expression and privacy?"[321]

The GNI's participants include technology companies such as original members Google, Microsoft, and Yahoo, as well as advocacy groups such as the Berkman Center for Internet & Society, and the Center for Democracy & Technology.[322] Facebook only recently joined the GNI, and Twitter does not appear to be affiliated.[323] Nevertheless—and serving as another sign of Facebook's and Twitter's status as ubiquitous Super-Intermediaries—the GNI homepage has Facebook and Twitter links displayed prominently on its homepage.[324]

---

[320] GNI, http://globalnetworkinitiative.org (last visited July 14, 2013); MACKINNON, *supra* note 14, at 179.

[321] MACKINNON, *supra* note 14, at 180. MacKinnon, herself a founding member of the GNI, *see id.*, appears to suggest that the GNI may be a way to service the Guiding Principles on Business and Human Rights, approved in 2011 by the U.N. Human Rights Council. *See id.* at 184-85. The Principles look to businesses committing to protect human rights, developing a human-rights due-diligence process, and initiating processes to remediate adverse human rights impacts. *Id.* at 185; *see also* U.N. Human Rights Council, *Guiding Principles on Business and Human Rights* (2011), *available at* http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[322] GNI, *Participants*, http://www.globalnetworkinitiative.org/participants/index.php (last visited July 14, 2013). The Electronic Frontier Foundation once belonged, but resigned due to concerns over the impact of the NSA on the GNI's corporate members. *See* Electronic Frontier Foundation, *EFF Resigns from Global Network Initiative*, EFF.ORG (Oct. 10, 2013), http://www.eff.org/press/releases/eff-resigns-global-network-initiative.

[323] According to Evgeny Morozov, Twitter refused to join the GNI. MOROZOV, *supra* note 23, at 22-23. Facebook initially refused to join as well, offering the "bizarre excuse" of a "lack of resources." *Id.* at 23. Facebook joined the GNI in 2013. *See* GNI, *Facebook Joins the Global Network Initiative* (May 22, 2013), http://www.globalnetworkinitiative.org/news/facebook-joins-global-network-initiative.

[324] GNI, http://globalnetworkinitiative.org (last visited July 14, 2013).

Whether one terms the GNI as an NGO,[325] or simply an industry-based interest group, the mission of the GNI is to deal with the "pressure" that "ICT [information and communications technology] companies increasingly face [from] governments to act in ways that may impact the fundamental human rights of privacy and freedom of expression."[326] Its goals are 1) to provide ICT companies with a framework "rooted in international standards"; 2) to ensure accountability of ICT companies "through independent assessment"; 3) to enable "opportunities for policy engagement"; and 4) to create "shared learning opportunities."[327] The GNI includes some of the most powerful actors in the world of information and communications technology. It ascribes to principles of human rights law as found in the International Bill of Human Rights, specifically, principles "based on internationally recognized laws and standards for human rights" (GNI Principles), including the UDHR, the ICCPR, and the ICESCR."[328] Additionally, the GNI has written an extensive framework for governance, accountability and learning,[329] and implementation guidelines.[330]

---

[325] "There is no international law which provides an authoritative definition of non-governmental organizations in general[,] and there is no generally agreed upon definition of human rights NGOs among scholars, either." Buhm-Suk Baek, *Rhris, Nhris And Human Rights NGOs*, 24 FLA. J. INT'L L. 235, 239 (2012) (quoting *Menno T. Kamminga, The Evolving Status of NGOs under International Law: A Threat to the Inter-State System?, in* NON-STATE ACTORS AND HUMAN RIGHTS 93, 95 (Philip Alston ed., 2005)). Buhm-Suk Baek suggests that "human rights NGOs should have four basic elements, that is, they should be: 1) non-profit, 2) independent—specifically without interference from governments, 3) people-based, and 4) devoted to the promotion and protection of human rights." *Id.* By this definition, the GNI may be fairly termed a human-rights NGO, although its members are internet and technology companies rather than individuals.

[326] GNI, *About Us*, http://www.globalnetworkinitiative.org/about/index.php (last visited July 14, 2013).

[327] *Id.*

[328] GNI, *Principles*, https://globalnetworkinitiative.org/principles/index.php (last visited July 14, 2013); *see also* MOROZOV, *supra* note 23, at 23 (noting UDHR's role in GNI).

[329] GNI, *Governance, Accountability, & Learning Framework*, https://globalnetworkinitiative.org/governanceframework/index.php (last visited July 14, 2013).

[330] GNI, *Implementation Guidelines*, https://globalnetworkinitiative.org/implementationguidelines/index.php (last visited July 14, 2013).

The GNI Principles are interesting for what they include, as well as for what they omit. Included are principles of Freedom of Expression and Privacy. Although privacy is a worthy topic on its own, the discussion here will focus on speech. The GNI Principles state: "[f]reedom of opinion and expression is a human right and guarantor of human dignity. The right to freedom of opinion and expression includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[331] This echoes UDHR Article 19 and ICCPR Article 19(2).[332]

The GNI Principles also acknowledge the need to sometimes restrict speech: "[t]he right to freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards. These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose."[333] This echoes the ICCPR's restrictions on expression arising from the responsibilities attendant to the right of expression contained in Article 19(3).[334] A footnote indicates that the "narrowly defined circumstances" permitting restrictions should be incorporated from ICCPR Article 19 regarding "actions necessary to preserve national security and public order, protect public health or morals, or safeguard the rights or reputations of others."[335]

The GNI Principles attempt to take care to limit the scope of speech restrictions:

> Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on free-

---

[331] GNI, *Principles*, *supra* note 328.

[332] Indeed, "Freedom of Expression" is defined by the GNI Principles by using Article 19 of the UDHR and Article 19 of the ICCPR. *Id.*, Annex A; *see also supra* Part III.B.

[333] GNI, *Principles*, *supra* note 328 (footnotes omitted).

[334] ICCPR, *supra* note 44, at art. 19(3).

[335] GNI, *Principles*, *supra* note 328, at Annex B n.5.

> dom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.
>
> Participating companies will respect and protect the freedom of expression rights of their users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.[336]

Regarding the standards used to distinguish permissible from impermissible restrictions, the GNI Principles point to "further interpretations issued by international human rights bodies, including the Human Rights Committee and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression."[337] It would appear, then, for example, that the GNI intends to incorporate the three-part test that limits speech restrictions, as stated by Special Rapporteur La Rue.[338] The GNI also cites the Johannesburg Principles on National Security, Freedom of Expression and Access to Information as a further example of limitations on restrictions of the freedom of expression.[339] Additionally, the Implementation Guidelines for the GNI Principles incorporate important considerations of transparency regarding governmental demands for removal of speech.[340] An accountability system will help to watch

---

[336] GNI, *Principles*, *supra* note 328 (footnotes omitted).

[337] *Id.* at Annex B n.5.

[338] *See* text accompanying note 293.

[339] GNI, *Principles*, *supra* note 328, at Annex B n.7; *see also* The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (adopted Oct. 1, 1995), http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf. The main thrust of the Johannesburg Principles is to limit governmental use of "national security" as a pretext for restricting the freedom of expression. *See id.* pmbl.; *see generally* ARTICLE 19: DEFENDING FREEDOM OF EXPRESSION AND INFORMATION, http://www.article19.org/ (last visited July 14, 2013).

[340] "Participating companies will encourage governments to be specific,

member service providers to make sure they are complying with the GNI Principles.

These processes represent a needed development of a human-rights framework for Super Intermediaries. Although one must retain concerns over the scope of the restrictions in ICCPR Article 19, the GNI members are taking care to note that restrictions ought to be interpreted quite narrowly. Done properly, such a system might go a long way towards providing accountability and transparency on governmental demands for speech removal, as well as removals done solely by intermediaries.[341] However, it is not entirely clear how strongly companies will comply with the GNI Principles. For example, Evgeny Morozov claims that Microsoft "does not fully adhere to the spirit" of the GNI with its search engine in the Middle East, risking turning the GNI into little more than a "publicity stunt."[342]

Further, as noted, the GNI Principles are interesting for what they omit. As they state, the "specific scope of these Principles is limited to freedom of expression and privacy."[343] Thus, the GNI Principles do not import the International Bill of Human Rights *carte blanche*. Significantly absent from the GNI Principles is any mention of religion or of hate speech concerning religion, or for that matter any language similar to ICCPR 20(2), which prohibits "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence."[344] This omission is surely not an accident. First, many significant GNI members are from the United States, a country that has rejected ICCPR 20(2). Second, the

---

transparent and consistent in the demands, laws and regulations ('government restrictions') that are issued to restrict freedom of expression online." GNI, *Implementation Guidelines*, *supra* note 330.

[341] But as Lawrence Lessig notes, bare transparency is insufficient if it does not provide the public with the information needed to see what is actually happening. LAWRENCE LESSIG, REPUBLIC, LOST: HOW MONEY CORRUPTS CONGRESS—AND A PLAN TO STOP IT 260 (2011); *see also* Lawrence Lessig, *Against Transparency*, NEW REPUBLIC (Oct. 9, 2009), http://www.newrepublic.com/article/books-and-arts/against-transparency [hereinafter Lessig, *Against Transparency*] (criticizing "naked transparency movement").

[342] MOROZOV, *supra* note 23, at 217.

[343] GNI, *Principles*, *supra* note 328.

[344] ICCPR, *supra* note 44, art. 20(2); *see also supra* Part III.B.2.

omission is unsurprising in light of the long-standing dispute before the United Nations regarding "defamation of religion."[345] Indeed, nearly all of the participants in the GNI are western companies and western-oriented advocacy groups, and as such, are more likely to favor western values.[346] This may open the GNI up to charges of western bias in disputes such as the inflammatory *Innocence of Muslims* video. Regardless, organizations like the GNI provide an important step in right direction for establishing dialogue and collaboration between the industry, "investors, civil society organizations, academics and other stakeholders" to work with governments.[347]

Finally, it should be noted that in order for a group like the GNI to have a deeper impact on the public mind, there needs to be wider participation. Although the listing of members includes Google, Microsoft, and Yahoo, a number of very high-profile Super-Intermediaries are absent. Facebook only recently joined, and Twitter is absent.[348] Also absent are eBay and Amazon.[349] Even though Google's presence is an important asset for the GNI, it is important that the members include more Super-Intermediaries. For her part, Rebecca MacKinnon notes criticisms levied against the GNI, such as insufficiently broad international membership, being overly narrow in scope, and "setting the bar too low for companies," but notes the current lack of "other functioning alternatives."[350] Professor Anupam Chander notes the GNI's limited membership, that it lacks

---

[345] *See supra* Part III.B.2.

[346] The GNI site includes a statement condemning the violence arising from the *Innocence of Muslims* video and noting the importance of multi-stakeholder collaboration. GNI, *Collaborating on Controversial Content and Difficult Decisions* (Sept. 25, 2012), https://globalnetworkinitiative.org/news/collaborating-controversial-content-and-difficult-decisions.

[347] GNI, *Principles*, *supra* note 328.

[348] *See* GNI, *Participants*, *supra* note 322.

[349] *See id.*

[350] MACKINNON, *supra* note 14, at 186; *see also* Colin Maclay, *Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net?*, *in* ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 87, 97-102 (Ronald Deibert et al. eds., 2010) (noting concerns about the GNI, such as lack of broader participation, absent metrics for accountability, concerns about transparent channels of communication, and more).

enforcement mechanisms beyond "naming and shaming," and that its members are subject to local and foreign laws that may trump its principles.[351] Chander therefore suggests giving the GNI principles the force of law through a "Global Media Freedom Act."[352]

IV. Code and Content Regulation

Part IV turns to the processes by which Super-Intermediaries regulate content. It starts by first examining the long-standing "exceptionalism" dispute over internet regulation, one that unfortunately allowed intellectual property to become the "tail" that "wags the dog" of internet policy. As a result, much of the *public* attention to internet regulation—whether by positive law or internal code—has focused on intellectual property to the exclusion of other types of expression. This Part then turns to the codes and processes used by Super-Intermediaries to regulate content.

A. Intellectual Property Wagging the Dog

Many of the efforts to regulate the internet and internet intermediaries have focused on intellectual property, often to the exclusion of most any anything else.[353] As Professor Milton Mueller notes in a chapter entitled "IP versus IP," the term "IP" refers to *both* "intellectual property" and "Internet protocol."[354] He further notes the oddity that problems of intellectual property are "rarely if ever grouped together and understood holistically as an aspect of Internet governance,"[355] even though "[c]ontention around intellectual prop-

---

[351] Chander, *supra* note 36, at 38; *see also* Land, *Law of Internet*, *supra* note 26, at 449 (noting that international law influences states through pressure, shame, socialization, monitoring, and more).

[352] Chander, *supra* note 36, at 39.

[353] Professor Roy Balleste makes a similar point regarding security and human rights, suggesting that "governments have argued that they must place national security first." Balleste, *supra* note 9, at 248.

[354] MUELLER, *supra* note 37, at 129.

[355] *Id.* at 130. Similarly, Professor Peter Yu addresses "external" and "inter-

erty emerges as one of the key drivers of the global politics of Internet governance."[356] Similarly, Professor Julie Cohen notes that creating a normative theory for open networks "requires more than a theory of intellectual property or telecommunications."[357] Professor Greg Lastowka notes that trademark law—a form of intellectual property law—remains "[o]ne of the few areas of law that seems to retain some supervisory control" over Google, but expresses deep concern that trademark law is not really sufficient to serve as a "general regulator of information practices like search results."[358]

But there is much more to internet law than intellectual property. Although a detailed recitation of the broader and long-standing debate over territoriality is beyond the scope of this article (and has been oft-discussed), a few key points are worth noting regarding the question of whether the internet *can* be territorially regulated, and if so, whether it *ought* to.[359] So-called "exceptionalists" believe that the internet either cannot or should not be regulated geographically, whereas "unexceptionalists" believe that it can or should.[360] Rather than reciting the history of the debate, or attempting the unenviable task of resolving it, this article instead seeks to make the descriptive claim that the issue of internet regulation has been driven primarily by fears over piracy of intellectual property. Thus, a few highlights

---

nal" conflicts between intellectual property protection and human rights. *See* Yu, *Nonmultilateral Era*, *supra* note 270, at 1091-96.

[356] MUELLER, *supra* note 37, at 132.

[357] Julie E. Cohen, *Network Stories*, 70 LAW & CONTEMP. PROBS. 91, 94 (2007).

[358] Lastowka, *supra* note 70, at 1359, 1410.

[359] *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200 (1998); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 443 (2003); *see also* Ira Steven Nathenson, *Best Practices for the Law of the Horse: Teaching Cyberlaw and Illuminating Law Through Online Simulations*, 28 SANTA CLARA COMP. & HIGH TECH. L.J. 657, 663-64 & n.7 (2012) [hereinafter Nathenson, *Best Practices*] (describing debate and listing illustrative sources).

[360] *See* David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365, 1367-69 (2002) (coining terms "exceptionalists" and "unexceptionalists"); *see also* MUELLER, *supra* note 37, at 2-4 (describing the debate and criticisms of both positions); DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE (2009).

of the broader rhetoric from the debate may be quite illustrative. In 1996, John Perry Barlow, a co-founder of the Electronic Frontier Foundation, wrote the famous *A Declaration of Independence in Cyberspace*.[361] As he declared,

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[362]

Barlow, of course, takes a sharp stance against territorial regulation by geographically based governments, falling squarely into the exceptionalist camp. It would appear that he makes both the descriptive claim that the internet cannot be regulated geographically, as well as the normative statement that it should not be regulated by territorial sovereigns.[363]

---

[361] John Perry Barlow, *A Declaration of Independence in Cyberspace* (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

[362] *Id.*

[363] For a parodic rejoinder to Barlow's *Declaration*, see *A Declaration of the Interdependence of Cyberspace* by Daniel Castro and the Information Technology and Innovation Foundation ("ITIF"):

> Libertarians of the Virtual World, you gray-bearded detractors of government and sovereignty, we too come from Cyberspace. On behalf of the future, we ask you of the past to leave us alone. Your declaration of independence rings false, and your stale principles are a threat to progress.
>
> The Internet has no elected government, nor is it likely to have one, but this does not mean it is not governed. The Internet is ruled, as are all

Interestingly, Barlow's discussion of the internet raises issues much broader than that of property, declaring that "legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."[364] Although Barlow is not speaking in terms of human rights law, one could look at his Declaration from that perspective. From the viewpoint of the International Bill of Human Rights, it would appear that Barlow is concerned with a broad swath of human conduct and human values, going far beyond property,[365] to include additional human rights such as those contained in the International Bill of Human Rights, such as freedom of expression,[366] personal dignity,[367] and freedom of movement.[368]

Unfortunately, the reality of internet regulation is that much of the attention of Super-Intermediaries has been to focus on proper-

---

> technologies, not only by the norms and beliefs of its users, but also by the laws and values of the societies in which they live.

Daniel Castro & ITIF, *A Declaration of the Interdependence of Cyberspace*, *available at* COMPUTERWORLD (Feb. 8, 2013), http://www.computerworld.com/s/article/9236603/A_Declaration_of_the_Interdependence_of_Cyberspace. Castro's rebuttal accuses Barlow of "[c]asting aside the Universal Declaration of Human Rights" through "proclaim[ing] that any ideas or property you can steal from others should be yours to reproduce and distribute freely in cyberspace. We reject the fiction that the Internet gives you the freedom to disregard basic human rights of property, expression, identity and movement." *Id.* Although there is plenty to criticize in Barlow's *Declaration*, Castro seems to misread Barlow. First, Barlow appears to treat freedom of expression as a fundamental value, stating "[w]e are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity." Barlow, *supra* note 361. Second, Barlow does not appear to reject human rights principles, but rather to reject territorial application of them by governments.

[364] Barlow, *supra* note 361.

[365] *Cf.* UDHR, *supra* note 43, at art. 17 (property); *id.* at art. 27 (moral interest); ICESCR, *supra* note 45, at art. 15(1)(c) (moral and material interests).

[366] *Cf.* UDHR, *supra* note 43, at art. 19 (freedom expression); ICCPR, *supra* note 44, at art. 19(2) (same).

[367] *Cf.* UDHR, *supra* note 43, at art. 1 (human dignity); ICCPR, *supra* note 44, pmbl. (same).

[368] *Cf.* UDHR, *supra* note 43, at art. 13 (freedom of movement and to leave a State); ICCPR, *supra* note 44, at art. 12 (same).

ty, namely, intellectual property.[369] In an early essay that unfortunately set much of the tone for the debate over internet regulation, Seventh Circuit Judge Frank H. Easterbrook attacked cyberlaw as nothing more than a "law of the horse."[370] Notably, Easterbrook's short essay was on the topic of "Property and Cyberspace," so the bulk of his discussion regarded methods of developing rules for intellectual property on the internet.[371] Although it would be an overstatement to say that Easterbrook' focus on property materially shaped the discussion over internet regulation, there is little doubt that his article fostered significant discussion on the question of whether cyberlaw is a discrete topic; in turn, his "is there a cyberlaw" question may have unintentionally influenced the discussion for years to come.[372]

Whether Easterbrook's framing of the issue truly shaped the debate over internet regulation, or simply coincided with it, the reality is that—at least in the mind of this author—an inordinate portion of the regulatory attention that *lawmakers* have foisted on Super-Intermediaries focuses on intellectual property. Early regulatory efforts attempted to cover a broad swath of online issues with mixed results. For instance, the Communications Decency Act (CDA)[373] and Child Online Protection Act (COPA)[374] regulated

---

[369] "[T]he IP vs. IP struggles exceed the ICANN controversies in their shaping impact on Internet governance." MUELLER, *supra* note 37, at 130.

[370] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207 (1996); *see also* Lipton, *supra* note 26, at 1340-41 (criticizing effects of Easterbrook's article on cyberlaw scholarship); Nathenson, *Best Practices*, *supra* note 359, at 733-741 (criticizing Easterbrook's attack on a number of bases, including being a flawed metaphor). Similarly important definitional issues arise in the field of internet governance. Professor Roy Balleste says that internet governance focuses on "issues associated with intellectual property, content control and the bounds of jurisdiction," and as such is, "in essence, a broader subject of study than Cyberlaw." Balleste, *supra* note 9, at 227 n.2.

[371] Easterbrook, *supra* note 370, at 208-17.

[372] *See* Nathenson, *Best Practices*, *supra* note 359, at 732-41 (responding to Easterbrook's descriptive and normative claims).

[373] *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 882, 885 (1997) (striking down portions of CDA).

[374] *See* Ashcroft v. ACLU, 542 U.S. 656, 673 (2004) (affirming grant of preliminary injunction against COPA); ACLU v. Mukasey, 534 F.3d 181, 184

certain classes of online pornography. Congress also passed the Children's Internet Protection Act (CIPA), which required public libraries to install and utilize Internet filters as condition for the receipt of federal subsidies.[375] The Supreme Court of the United States ultimately struck down portions of the CDA and upheld an injunction against the enforcement of COPA; however, the Court upheld CIPA against a First Amendment challenge.[376]

The two statutes with perhaps the most significant impact on the development of online services—as well as Super-Intermediaries' over-focus on intellectual property—are the so-called immunity provision of the CDA,[377] and the notice-and-takedown provision of the Digital Millennium Copyright Act (DMCA).[378] The CDA's immunity provision, entitled "Protection for private blocking and screening of offensive material" was actually intended to encourage service providers to *filter* offensive material at their own behest without fear of being labeled a "publisher" and thus open to defamation liability.[379] Accordingly, Section 230 of Title 47 provides that "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information" provided by a content provider.[380]

Courts have generally interpreted Section 230 as creating immunity from liability for defamation and a number of other claims.[381] Although Congress apparently hoped the statute would

---

(2009) (affirming permanent injunction against COPA).

[375] *See* U.S. v. American Library Ass'n, Inc., 539 U.S. 194, 214 (2003) (upholding CIPA).

[376] *See Ashcroft*, 542 U.S. at 673; *Am. Library Ass'n*, 539 U.S. at 214; *Reno*, 521 U.S. at 882, 885; *Mukasey*, 534 F.3d at 184.

[377] 47 U.S.C. § 230 (2000).

[378] 17 U.S.C. § 512 (2010).

[379] The policies noted in the statute include "remov[ing] disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4) (2000).

[380] *Id.* § 230(c)(1).

[381] *See, e.g.*, Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997); *see also* David S. Ardia, *Free Speech Savior or Shield For Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decen-*

give service providers the safety they needed to make "family-friendly" websites, the reality is that Section 230 has been more of a carrot without a stick, permitting service providers to ignore online defamation without great fear of liability.[382]

Congress has also had great impact on the development of service providers through Section 512 of Title 17, the notice-and-takedown provision of the DMCA. Section 512 provides, *inter alia*, a qualified safe harbor against monetary liability for service providers who expeditiously remove claimed copyright infringement upon receipt of proper notification.[383] Here, Congress provided both a carrot (safe harbor) and a stick (loss of safe harbor), which had a much greater impact on spurring service providers into action.

Thus, CDA Section 230 and DMCA Section 512 tell a "tale of two cities,"[384] one that intertwines to tell a far bigger story. Section 230 gave service providers general license to ignore development of procedures or tools to monitor speech,[385] whereas Section 512 encouraged them to pay serious attention to developing processes to respond to copyright claims.[386] Today, numerous service pro-

---

cy Act, 43 LOY. L.A. L. REV. 373 (2010).

[382] One court, expressing dismay at the incentives that the immunity grants service providers, stated "[i]f it were writing on a clean slate, this Court would agree with plaintiffs . . . But Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others." Blumenthal v. Drudge, 992 F. Supp. 44, 51-52 (D.D.C. 1998).

[383] 17 U.S.C. § 512(c) (2010).

[384] CHARLES DICKENS, TALE OF TWO CITIES (1859).

[385] This is not to suggest that the author believes that the CDA used a wrongful approach, or that Congress should have instituted notice-based liability for defamation as it did with copyright claims. Indeed, the specter of permitting notice of claimed defamation to trigger a duty for takedown would easily lead to a "heckler's veto." *See Zeran*, 129 F.3d at 333 (holding that "liability upon notice has a chilling effect on the freedom of Internet speech"). Instead, the article acknowledges that the law has had demonstrable effects on the development of online services.

[386] Indeed, speaking as an academic author, it may be fair to say that the study of "cyberlaw" has become so subsumed within the broader realm of intellectual property that at times it seems that the field is suffering an identity crisis. Notably, at the 2012 AALS Midyear joint meeting of the sections of intellectual property, internet law, and biosciences, Professor Paul Ohm, serving as moderator, asked a

viders now list agents for service of copyright takedown notices.[387] The *Chilling Effects* database is filled to the brim with examples of such notices.[388] Moreover, although Section 512 provides safe harbor only for copyright, many service providers have used it by analogy via "quasi-DMCA" takedown processes that permit takedown for a wide variety of intellectual property claims.[389] More recently, Congress turned its attention to regulating intellectual property on the internet via the ill-fated Stop Online Piracy Act (SOPA),[390] and equally doomed Protect IP Act (PIPA).[391] Speaking broadly, the bills were aimed at cutting off "funding, advertising, links or other assistance" to "foreign-based websites that sell pirated movies, music and other products."[392] After fierce public opposition from advocacy groups and powerful internet intermediaries, the bills stalled.

As the foregoing discussion suggests, intellectual property law has increasingly dominated regulatory efforts of lawmakers; equally so, it has dominated the attentions of Super-Intermediaries, who have implemented takedown provisions, created quasi-DMCA regimes, and even instituted automated filtering mechanisms to quell copyright concerns.[393] Nicole Wong, Vice President and Deputy

---

panel of experts whether cyberlaw was dead. *See* 2012 AALS Midyear Conference, *Workshop on When Technology Disrupts Law: How do IP, Internet and Bio Law Adapt?*, Berkeley, CA (June 2012).

[387] *See* U.S. Copyright Office, *Service Provider Agents*, http://www.copyright.gov/onlinesp/list/a_agents.html (last visited July 14, 2013).

[388] *See supra* text accompanying notes 90-91 (observing that there are over 143 thousand takedown notices on *Chilling Effects*).

[389] For instance, Cafepress (which allows users to design, make, and sell t-shirts, mugs, and the like) has a takedown policy covering a broad and non-exclusive listing of claims: "intellectual property rights (such as copyright, trademark, trade dress and right of publicity)." CafePress.com, Intellectual Property Rights Policy, http://www.cafepress.com/cp/info/help/index.aspx?page=iprights.aspx (last visited July 14, 2013).

[390] Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

[391] Protect IP Act, S. 968, 112th Cong. (2011).

[392] *See* Amy Schatz, *What Is SOPA Anyway? A Guide to Understanding the Online Piracy Bill*, WALL ST. J. (Jan. 18, 2012), http://online.wsj.com/article/SB10001424052970203735304577167261853938938.html.

[393] *See* Nathenson, *Civil Procedures*, *supra* note 86, at 936-40 (discussing automated filtering).

General Counsel of Google, correctly notes that whereas there is a "significant legal infrastructure for protecting intellectual property," there is a "lack of a similar infrastructure for platforms of free expression, . . . an area where we believe that in the past the legislation has not paid enough attention."[394] The hyper-focus of government and corporations on intellectual property is disturbing. As Professor Mueller notes, the technology used for protecting intellectual property has been or can be easily drafted for use by the national security state.[395]

It would therefore appear that Super-Intermediaries may have put far less effort, or at least far less *visible* effort, into the processes by which they deal with difficult non-propertied speech disputes, particularly incendiary matters like the *Innocence of Muslims* video. This is to a large extent understandable, considering that many prescriptions are reactionary, addressing a problem after a paradigm-challenging event occurs. But perhaps *Innocence of Muslims* is one of those disputes, i.e., one that prompts consideration on how to react when such events inevitably arise again.[396] The GNI, commenting on the outrage, notes the need for "robust" discussion to occur "among all participants about potential implications for free expression as well as possible lessons to be learned."[397] The editors of the volume *Access Contested* suggest that we are now living in a fourth phase of cyberspace controls, namely, one in which "contest over access has burst into the open" between open-internet advocates and the governments and corporations "who feel it is now legitimate for them to exercise power openly in this domain."[398]

---

[394] MACKINNON, *supra* note 14, at 100 (statements of Nicole Wong, Vice President and Deputy General Counsel of Google).

[395] MUELLER, *supra* note 37, at 156.

[396] Of course, as the adage goes, "hard cases make bad law." But as the ever-prescient Justice Stevens wryly noted, sometimes easy cases make for bad law as well. *See* Burnham v. Superior Court, 495 U.S. 604, 640 n.* (1990) (Stevens, J., concurring in the judgment) (noting in personal jurisdiction case "Perhaps the adage about hard cases making bad law should be revised to cover easy cases").

[397] GNI, *Collaborating*, *supra* note 346.

[398] Ronald Deibert et al., *Toward the Fourth Phase of Cyberspace Controls*, *in* ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 3, 14 (Ronald Deibert et al. eds., 2011). The first three phases were

Because content controls are becoming so widely used, it is high time for Super-Intermediaries to explore more deeply the interplay between the law of intermediaries and human rights law.[399] In *Ashby v. France*,[400] the European Court of Human Rights found that a conviction under French copyright law was subject to the right of expression under Article 10 of the European Convention.[401] The applicants, three fashion photographers, had been convicted of copyright infringement after posting certain pictures to a website, and fined €255,000.[402] Ultimately, the European Court of Justice denied the applicant on the merits, finding that the domestic court in France had found an appropriate balance between Article 10 (protecting freedom of expression) and Article 1 to the First Protocol (protecting property, which can include intellectual property).[403] The Court similarly rejected a claim by co-founders convicted of operating the Pirate Bay website used for downloading copyrighted files.[404] Although the Swedish copyright convictions interfered with the human right of expression, Swedish authorities had "weighty reasons" for

---

the open commons (through 2000), access denied (through 2005), and access controlled (through 2010). *See id.* at 6-14.

[399] There are a number of scholars now working in this important new field. *See, e.g.*, Land, *Region Codes*, *supra* note 245; Yu, *Region Codes*, *supra* note 247.

[400] Ashby Donald et al. v. France, Appl. nr.36769/08 (Eur. Ct. H.R. Jan. 10, 2013), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-115845.

[401] Charles Swan, *When Does Freedom of Speech Trump Copyright?*, THE GUARDIAN (Feb. 13, 2013), http://www.guardian.co.uk/media-network/media-network-blog/2013/feb/13/freedom-speech-trump-copyright; Dirk Voorhoof & Inger Høedt-Rasmussen, *ECHR: Copyright vs. Freedom of Expression*, KLUWER COPYRIGHT BLOG (Jan. 25, 2013), http://kluwercopyrightblog.com/2013/01/25/echr-copyright-vs-freedom-of-expression/.

[402] Voorhoof & Høedt-Rasmussen, *supra* note 401.

[403] *Id.* As stated previously in this article, Article 10 of the European Convention appears to be in at least one way to be preferable to ICCPR Article 19 due to the requirement that a restriction on speech be "necessary in a democratic society." European Convention on Human Rights, *supra* note 291, art. 10(2); *see also supra* note 291.

[404] *See* Neij & Sunde Kolmisoppi v. Sweden, Appl. no. 40397/12 (Eur. Ct. H.R. Feb. 19, 2013), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-117513.

the prosecution.[405]

B. The Codes of Information Control

This subsection discusses methods of content control.[406] It looks first to "realspace" controls, i.e., regulation via external human lawmakers or internal human decision-makers. It then turns to technological controls, such as the domain name system, geolocation, and other uses of software or hardware to regulate content. Finally, it considers hybridized controls, a combination of realspace and technological processes.

1. Realspace Controls

Although the internet is often called "cyberspace," we interact with it in the real world, i.e., "realspace." Thus, although we often speak of "code" as both constituting *and* regulating the internet, many controls of online content take place in realspace. This subsection examines two categories: lawmaker regulation and extralegal regulation.

a. Lawmaker Regulation

A first type of lawmaker regulation is legislation, whether issued by Congress or other governmental actors.[407] As noted previ-

---

[405] As the court stated, "[s]ince the Swedish authorities were under an obligation to protect the plaintiffs' property rights in accordance with the Copyright Act and the Convention, the Court finds that there were weighty reasons for the restriction of the applicants' freedom of expression." *Id.* at 9-11.

[406] *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 158-64 (2012) (discussing six categories of "pervasively distributed copyright enforcement" grouped by the behaviors targeted by each grouping); *see also* Pasquale, *supra* note 17, at 112 (stating that Google "has become a de facto lawmaker for many aspects of life on the Internet").

[407] Of course, official lawmakers include far more than Congresspersons and

ously, Congress has acted repeatedly to attempt to regulate online content, such as through the CDA, DMCA, COPA, CIPA, SOPA, PIPA, and more.[408] Although Congress' attempts to restrict online content are often criticized, the legislative process is subject to oversight through veto,[409] judicial review,[410] and elections. However, as the focus of this article looks beyond national borders, it must be recalled that lawmaking bodies across the globe can vary significantly in the levels of formality of decision-making as well as the level of transparency in their proceedings.

A second form of lawmaker-based content control is adjudication, which takes a variety of forms, such as the traditional lawsuit between adverse parties. At its best, adjudication provides ample opportunity for a formal and transparent system, subject to formal rules of procedure and evidence, an impartial adjudicator, and adverse parties. Adjudication at its best is also highly transparent, including public proceedings, public judgment, and in many cases, written decisions. It is also, of course, more expensive and time-consuming. Other forms of adjudication may include arbitration, a prime example being the Uniform Domain Name Dispute Resolution Policy (UDRP), which permits quick and inexpensive arbitration of

---

judges. Beyond the obvious example of administrative agencies, sometimes the executive acts in her or his own capacity. *See* Michael Daniel, *Improving the Security of the Nation's Critical Infrastructure*, THE WHITE HOUSE BLOG (Feb. 13, 2013), http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure?utm_source=related (noting executive order regarding cybersecurity). Legislatures and adjudicators are discussed above to provide paradigmatic examples of what is in fact a large set of official lawmakers.

[408] *See supra* text accompanying notes 373-92.

[409] For example, the Obama administration hinted that it would not support and that it might veto the SOPA bill as drafted: "While we believe that online piracy by foreign websites is a serious problem that requires a serious legislative response, we will not support legislation that reduces freedom of expression, increases cybersecurity risk, or undermines the dynamic, innovative global Internet." Macon Phillips, *Obama Administration Responds to We the People Petitions on SOPA and Online Piracy*, THE WHITE HOUSE BLOG (Jan. 14, 2012), http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-online-piracy.

[410] *See supra* text accompanying notes 375-76 (noting the Supreme Court's constitutionality determinations on the CDA, COPA, and CIPA).

domain-name disputes.[411] Although UDRP proceedings are not open to the public, UDRP decisions are generally published.[412]

The previous two paragraphs will likely strike the reader as being somewhat obvious, so obvious that perhaps they need not be stated. Yet it is important to recall that "code" in the sense of computer code is not the only regulator of online content.[413] Moreover, although American formal legal lawmaking and legal process may often represent a good example of formal and transparent regulation, this is not always the case worldwide. A Super-Intermediary may face demands of governmental officials in other countries where power is centralized, where legal processes are lacking in formality or transparency, or for that matter, where opportunities are lacking for meaningful participation by affected parties or other stakeholders.

Another reason for noting the role of lawmaker-based regulation is to provide the groundwork for a more important observation: in a pragmatic sense, official lawmaking plays a small role in the day-to-day determination of what stays online and what is removed. For one thing, significant amounts of online content may be technically unlawful, but nevertheless go unremedied. One reason pointed out by Professor John Tehranian is the "gap" between positive law and online norms of behavior that renders illegal conduct rampant, regardless of the threat of ruinous monetary liability for the conduct.[414] Another reason, noted by Professor Tim Wu, is that much

---

[411] Internet Corporation for Assigned Names and Numbers, *Uniform Domain-Name Dispute-Resolution Policy*, www.icann.org/en/udrp/udrp.htm.

[412] Internet Corporation for Assigned Names and Numbers, *Rules for Uniform Domain Name Dispute Resolution Policy*, Rule 16(b), http://www.icann.org/en/help/dndr/udrp/rules.

[413] As Professor Lawrence Lessig notes, just as "code" regulates, so do "law," "norms," and "markets." *See* LESSIG, CODE 2.0, *supra* note 104, at 86-90; Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662-64 (1998). Professor Julie Cohen argues that Lessig's "modalities are resources available to be harnessed, sometimes singly but more often in combination, in the service of particular agendas advanced by socially embedded actors." COHEN, *supra* note 406, at 156. Cohen concludes that although scholars remain interested in Lessig's modalities, they have paid far too little attention to "the social and institutional contexts within which [the modalities] are embedded." *Id.* at 185.

[414] *See* John Tehranian, *Infringement Nation*: *Copyright Reform and the Law/Norm Gap*, 2007 UTAH L. REV. 537, 543 (2007). Professor Tehranian de-

arguable infringement is "tolerated" by content owners for a variety of reasons, such as "laziness or enforcement costs, a desire to create goodwill, or a calculation that the infringement creates an economic complement to the copyrighted work."[415]

b. Extra-Legal Regulation

In reality, most content-control decisions are made without the direct involvement of governmental authorities. Many of those extra-legal decisions still occur in realspace. First, Super-Intermediaries may self-regulate using employees or contractors. Second, intermediaries often take down content based on demands submitted by intellectual property owners.

i. Internal Self-Regulation

To the extent that regulation takes place regarding online content—whether protected by intellectual property or other legal regimes—it is often done using extra-legal techniques. Such tech-

---

scribes a "hypothetical" law professor named "John" who, over the course of a day engaging in common online infringement, accumulates over $12 million in possible copyright liability, or over the course of a year, an astounding $4.544 *billion*. *See id.* at 543-48; *see also* JOHN TEHRANIAN, INFRINGEMENT NATION: COPYRIGHT 2.0 AND YOU 2-4 (2011) (same). Lest anyone doubt the plausibility of Tehranian's numbers, Jammie Thomas-Rasset was found liable for downloading 24 songs, and at one point, ordered to pay $1.92 million for the illegal downloads. *See* Capitol Records Inc. v. Thomas-Rasset, 680 F. Supp. 2d 1045, 1049-50 (D. Minn. 2010). Indeed, in the copyright infringement case brought by the music industry against file-sharing software creator LimeWire, the theoretical amount of statutory copyright damages might have been $72 *trillion* dollars, a figure greater than "the value of everything produced in the world in an entire year, the entire output of all 7 billion human beings." Tim Worstall, *The RIAA: Do Not Believe a Word They Say, Ever, For They're Claiming $72 Trillion in Damages. Updated, See Correction*, FORBES (May 24, 2012), http://www.forbes.com/sites/timworstall/2012/05/24/the-riaa-do-not-believe-a-word-they-say-ever-for-theyre-claiming-72-trillion-in-damages/.

[415] Tim Wu, *Tolerated Use*, 31 COLUM. J. L. & ARTS 617, 619 (2008) (addressing "tolerated use").

niques may rely on internal self-guided regulation, such as the use of a system administrator, a monitor, or other employees who review the system for wrongful content. For example, the webmaster of a blog might moderate user comments.[416] A larger entity may have a whole department of persons who comb the site for abuse, regardless of whether the content is brought to the intermediary's attention.[417] The CDA was drafted to encourage intermediaries to engage in such self-examination through a provision that has been interpreted to provide immunity against defamation and other claims.[418] However, CDA immunity applies regardless of whether a provider chooses to review its site, giving some providers little incentive to scrutinize user content.[419] Moreover, service providers may rightfully fear reviewing their own services lest they gain notice of intellectual property infringement.[420] Further, because internal review mecha-

[416] For example, popular blogging software WordPress permits website owners to block user comments until they are approved. *See* WordPress.org, *Features*, http://wordpress.org/about/features (last visited Sept. 1, 2013).

[417] *See* Citron & Norton, *supra* note 8, at 1477.

[418] *See supra* text accompanying notes 377-82.

[419] *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) (holding that "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process"); Blumenthal v. Drudge, 992 F. Supp. 44, 52-53 (D.D.C. 1998) (holding that AOL took "advantage of all the benefits [under the CDA] without accepting any of the burdens that Congress intended, [but that] the statutory language is clear").

[420] Regarding copyright law, Section 512 provides that the safe harbor is lost when the service provider either gains actual knowledge that material on the network is infringing, or "red flag" knowledge, i.e., "in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent." 17 U.S.C. § 512(c)(1)(A)(i), (ii) (2010); *see also* Viacom, Int'l Inc., v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012) (holding that "the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person"). Regarding contributory trademark infringement, the Second Circuit agreed with the holding of the district court that "generalized knowledge [by eBay of user infringement] is insufficient, and that the law demands more specific knowledge of individual instances of infringement and infringing sellers before imposing a burden upon eBay to remedy the problem." Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93, 107 (2d Cir. 2010). In both cases, the danger of gaining actual knowledge of specific infringement, or sufficient knowledge to trigger a "red flag," may be

nisms are not widely publicized, it is difficult to know how much self-initiated internal self-regulation takes place.

ii. External Input

What might be more common than *internal* self-regulation is regulation relying on *external* input, namely 1) demands from rights-holders; and 2) abuse mechanisms that require user reports. The levels of formality and transparency in such processes can vary significantly.

The first type of external input is a *demand* from an aggrieved rights-holder. Regarding such demands, Super-Intermediaries dedicate tremendous resources towards handling intellectual property claims sent either by cease-and-desist letters or via takedown notices.[421] The basis for a cease-and-desist is typically substantive intellectual property law. In comparison, a takedown notice is sent to an intermediary who provides hosting to the alleged direct infringer, and demands that the service provider remove the allegedly infringing content.[422] The direct basis for transmission of

---

sufficient to disincentivize extensive internal self-regulation by Super-Intermediaries, who are often entities offering a high degree of interactivity and networkability that can provide users with a platform to potentially infringe. *See supra* text accompanying notes 60-68.

[421] A cease-and-desist letter is a written communication sent to an alleged wrongdoer, typically demanding that the wrongdoer cease its unlawful conduct. As such, it is a direct communication between the claimant and the alleged wrongdoer. *See* Nathenson, *Civil Procedures*, *supra* note 86, at 923 (discussing direct copyright enforcement via cease-and-desist letter). In comparison, a takedown notice is sent from the claimant to an intermediary, demanding that the intermediary remove or disable the disputed content. *See* 17 U.S.C. 512(c)(3) (2010) (detailing requirements for copyright takedown notices); *see also* Nathenson, *Civil Procedures*, *supra* note 86, at 928 (discussing indirect copyright enforcement via takedown notice).

[422] The Copyright Act provides subscribers with the right to send a counter-notice demanding put-back. *See* 17 U.S.C. 512(g)(3) (2010). However, this right appears to be rarely employed. *See* Urban & Quilter, *supra* note 89, at 679-80 (finding only seven counter-notifications in Chilling Effects dataset). Reasons may include: 1) most takedown demands likely concern genuine copyright infringement; 2) the "mistake or misidentification" requirement for a counter-notice

the takedown notice is either: 1) the DMCA's safe harbor, which is lost if the service provider does not expeditiously remove or disable copyrighted content pursuant to a proper takedown notice;[423] or 2) the service provider's own "quasi-DMCA" policy crafted by the provider.[424] In turn, the DMCA's takedown provision and a provider's quasi-DMCA policy are both crafted against the backdrop of substantive intellectual property law. Such processes can suffer from a significant lack of transparency. Of additional help, some Super-Intermediaries, notably Google and Twitter, forward takedown requests to the *Chilling Effects Clearinghouse*.[425]

Notably, major intermediaries such as Google, Facebook, Microsoft, Twitter, and Yahoo are increasingly publishing transparency reports on matters such as takedowns or law-enforcement requests.[426] However, the amount of information provided varies significantly: for example, Google (which owns YouTube) provides a tremendous amount of information on both governmental and private requests,[427] whereas Facebook's report is much more limited, providing aggregate information on the governments requesting user

---

is unclear; and 3) subscribers are chilled by requirements that the counter-notice be signed under penalty of perjury, that it reveal the subscriber's name and address, and that the subscriber consent to jurisdiction. *See* Nathenson, *Safety Dance*, *supra* note 61, at 124-25, 161-62.

[423] *See* 17 U.S.C. § 512(c)(1)(C) (2010).

[424] *See supra* text accompanying notes 92-95.

[425] *See* Berkman Center for Internet & Society at Harvard Law School, *Intern with the Chilling Effects Clearinghouse*, http://cyber.law.harvard.edu/wg_home/ce_internships (last visited July 14, 2013) (noting that Google forwards takedowns to *Chilling Effects*); Twitter, *Copyright Notices: DMCA takedown and counter notices*, https://transparency.twitter.com/copyright-notices (last visited July 14, 2013).

[426] *See* Facebook, *Global Government Requests Report*, https://www.facebook.com/about/government_requests (last visited Sept. 20, 2013); Google, *Google Transparency Report*, https://www.google.com/transparencyreport/ (last visited July 14, 2013); Microsoft, *2012 Law Enforcement Requests Report*, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (last visited July 14, 2013); Twitter, *Twitter Transparency Report*, https://transparency.twitter.com/ (last visited July 14, 2013); Yahoo!, *Transparency Report Overview*, http://info.yahoo.com/transparency-report/ (last visited Sept. 20, 2013).

[427] *See* Google, *Google Transparency Report*, *supra* note 426.

information, the number of requests, the number of users or accounts specified, and the percentage of requests where Facebook was legally required to disclose information.[428]

Super-Intermediaries dedicate tremendous resources to responding to intellectual-property claims. For example, on March 2, 2013, Google reported that it had received requests to remove 13 million URLs for the previous month alone due to copyright requests from over 2700 copyright owners.[429] The Recording Industry of America *alone* demanded takedown of over 2.5 million URLs from 87 domains.[430] The Walt Disney Co. demanded takedown of nearly 180 thousand URLs from 518 domains.[431]

In comparison to copyright demands sent by copyright owners or their agents, demands from courts and governmental officials around the world are paltry. Over a six-month period ending June 30, 2012, Google reported only 12,776 demands from courts and governmental officials worldwide.[432] Such demands may be for "many different reasons," such as "defamation" or violations of "local laws prohibiting hate speech or adult content" pursuant to laws that "vary by country" depending on the "legal context of a given jurisdiction."[433] The largest percentage categories of demands were privacy and security (22%), defamation (10%), and governmental demands for removal due to copyright (7%).[434] Regarding categories

---

[428] *See* Facebook, *Global Government Requests Report*, *supra* note 426.

[429] Google, *Copyright Removal Requests – Transparency Report* (Mar. 2, 2013), http://www.google.com/transparencyreport/removals/copyright/.

[430] Google, *Top Reporting Organizations – Removal Requests – Google Transparency Report* (March 3, 2013), http://www.google.com/transparencyreport/removals/copyright/reporters/?r=last-month.

[431] *Id.* A review of the listing indicates that many of the entities issuing demands are not the copyright owners themselves but entities that are apparently acting as agents on behalf of the copyright owners. *Id.* This is permitted under the DMCA. *See* 17 U.S.C. § 512(c)(3)(A)(vi) (2010).

[432] Google, *Government Removal Requests – Google Transparency Report*, http://www.google.com/transparencyreport/removals/government/?metric=items (last visited Mar. 3, 2013).

[433] *Id.*

[434] *Id.* During the six-month period, the percentage of requests by category included: privacy and security (22%), defamation (10%), copyright (7%), government criticism (1%), and national security (1%). *Id.* Hate speech, impersonation,

relevant to *Innocence of Muslims*, a miniscule percentage of the requests concerned matters of national security, violence, or hate speech, totaling one percent or less for each category.[435] Moreover, of the countries sending governmental demands to Google, the only countries with sizeable Islamic populations were Turkey and India; in comparison, the *United States* was the top issuer of governmental demands.[436]

As noted, a second type of external input that Super-Intermediaries may use is an *abuse* or *customer service department*. For example, eBay has been noted to use 4,000 employees devoted to "trust and safety," 200 of whom "focus exclusively on combating infringement," sometimes leading to the arrest of counterfeiters.[437] It is common for intermediaries, and particularly Super-Intermediaries, to have abuse departments that review complaints of improper content, and policies regarding content that is prohibited or restricted.[438] Similarly, YouTube has "Community Guidelines" that prohibit more than just copyright infringement. Also prohibited are a variety of topics such as: pornography or content that is sexually explicit; animal abuse, drug abuse, or bomb making; graphic or gratuitous violence; accidents or dead bodies; stalking, threats, or harassment; and more.[439] Regarding hate speech, YouTube states:

> We encourage free speech and defend everyone's right

---

adult content, trademark, violence, religious offense, electoral law, and "Other" garnered less than 1% each. *Id.*

[435] *Id.*

[436] Google, *Countries – Google Transparency Report*, http://www.google.com/transparencyreport/removals/government/countries/?t=table (last visited Mar. 3, 2013).

[437] Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 476 (S.D.N.Y. 2008), *aff'd in part, rev'd in part*, 600 F.3d 93 (2d Cir. 2009).

[438] For instance, eBay lists policies for offensive and adult material. *See* eBay, *Offensive Material Policy*, http://pages.ebay.com/help/policies/offensive.html (last visited July 14, 2013); eBay, *Adult Only Category Policy*, http://pages.ebay.com/help/policies/adult-only.html (last visited July 14, 2013).

[439] YouTube, Community Guidelines, http://www.youtube.com/t/community_guidelines (last visited Sept. 28, 2013).

> to express unpopular points of view. But we don't permit hate speech (speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity).[440]

The Community Guidelines further indicate:

> "Hate speech" refers to content that promotes hatred against members of a protected group. For instance, racist or sexist content may be considered hate speech. Sometimes there is a fine line between what is and what is not considered hate speech. For instance, it is generally okay to criticize a nation, but not okay to make insulting generalizations about people of a particular nationality.[441]

Additionally, YouTube's Terms of Service reserve the right to decide when content (other than copyright infringement) is in violation, and that it "may at any time, without prior notice and in its sole discretion, remove such Content and/or terminate a user's account."[442]

Although intermediaries such as YouTube, Facebook, and others extend "significant staff and energy addressing" complaints of abuse, their practices "remain unclear."[443] As one source notes, after a video is flagged, YouTube leaves the video up, puts up an age gate, or removes the video.[444] But the source further notes that YouTube

---

[440] *Id.*

[441] *Id.*

[442] YouTube, *Terms of Service*, ¶ 7.B, http://www.youtube.com/t/terms (last visited Sept. 18, 2013); *see also* MACKINNON, *supra* note 14, at 99 (noting that although many issues are resolved by Google's "clear-cut" internal procedures, political issues are typically referred to Google VP and Deputy General Counsel Nicole Wong).

[443] Citron & Norton, *supra* note 8, at 1477.

[444] Peter Ha, *Not Safe For YouTube: How Google Draws the Line Between Porn and Art (NSFW)*, GIZMODO (Apr. 8, 2013), http://gizmodo.com/5993806/not-safe-for-youtube-how-google-draws-the-line-between-porn-and-art.

will not divulge what it looks for when reviewing a video, arguably providing "a tacit admission that there are no rules or guidelines that could possibly separate pornography from art."[445] Speaking more generally, another source states that "intermediaries that address hate speech . . . rarely define key terms like 'hateful' or 'racist' speech with specificity" in their Terms of Service or Community Guidelines, making it difficult to discern rules regarding which speech is acceptable.[446]

2. Technological Controls

Whereas the previous section addressed types of *realspace* controls, this subsection addresses a second significant category of information-content control: the use of *technological* controls, such as computer code, hardware, or both in combination. As regulator, technological controls can run the gamut from sledgehammer to sharpened blade. Examples include the domain name system, geolocation, various types of filtering, and application-level controls. The end result may be that the *internet* will eventually become a series of balkanized *internets*, with content varying significantly around the world. Below are examples.[447]

a. Domain Name System

One method by which a Super-Intermediary can regulate content is through the domain name system ("DNS").[448] Although one may normally think of domain names as .COM, .ORG, and other

---

[445] *Id.*

[446] Citron & Norton, *supra* note 8, at 1458.

[447] A good source describing the wide variety of techniques used would be Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering*, *in* ACCESS DENIED, *supra* note 175, at 57. The paper describes techniques such as TCP/IP header filtering, TCP/IP content filtering, DNS tampering, HTTP proxy filtering, and more. *See id.* at 58-65.

[448] *See* SCHMIDT & COHEN, *supra* note 19, at 84 (discussing DNS blocking).

generic variants,[449] the DNS also provides for country-code domains such as .US (United States), .FR (France), .DE (Germany), .EG (Egypt), .LY (Libya), .SA (Saudi Arabia), and so on.[450] Country-code domains permit online service providers to craft versions of their sites for the tastes and laws of each country. Thus, Amazon runs a British site at amazon.co.uk, and eBay has a French site at ebay.fr. The content available at such sites can differ significantly. They can also be used to limit speech deemed illegal or inappropriate for a particular region. For instance, a search for Adolf Hitler's *Mein Kampf* in the American/general eBay.com turned up 234 hits, many of which were for the actual book,[451] whereas the same search run in the French eBay.fr turned up only 31 hits, none of which appeared to be for the book.[452] Similarly, Google does not permit Nazi propaganda on its German search site, Google.de, where such materials are illegal.[453]

The availability of country-code domain names provides significant incentives for service providers to tailor their content to local tastes and laws. From a freedom of expression perspective, country domains are a mixed bag. Speech of interest to an audience in a particular country may be omitted by the Super-Intermediary from its country-tailored site out of fear of angering governmental authorities and losing business in the target country. In fact, the increasingly common use of tailored country-code sites may make repressive governments more willing to make overarching demands for content removal. Thus, rather than facing the wrath of blocking YouTube.com entirely, a government could point to the fact that

---

[449] Domains ending with .COM, .ORG, .NET, .GOV and other generic terms are "generic top-level domains," or "gTLDs."

[450] Domains ending with a country code are "country-code top-level domains," or "ccTLDs." Thus, the popular Bit.ly tool for shortening internet URLs is actually run through a Libyan ccTLD. *See* Bit.ly, *bitly: Do more with your links*, https://bit.ly.

[451] Search on eBay.com for "mein kampf" (Mar. 3, 2013).

[452] Search on eBay.fr for "mein kampf" (Mar. 3, 2013).

[453] Craig Timberg, *Google's Restricting of Anti-Muslim Video Shows Role of Web Firms as Free-Speech Arbiters*, WASH. POST: BUSINESS (Sept. 14, 2012), http://articles.washingtonpost.com/2012-09-14/business/35494603_1_free-speech-anti-muslim-video-search-algorithm.

YouTube has a country-code top-level domain as evidencing the intermediary's ability and willingness to provide "appropriate" content in that region.

b. Geolocation

Another significant method of technological control is through the use of geolocation, or technology that aids a service provider in determining where a user appears to be located. A principal method of geolocation is determining the geographic location of the "Internet Protocol" (IP) address corresponding to the user.[454] Pursuant to the internet's underlying TCP/IP protocol, all packets of information sent or received are tagged with the numerical IP address of the sender and recipient.[455] In fact, domain names are nothing more than alphanumeric mnemonics that correspond to the numerical IP address of the service providing the corresponding access (such as a website or email service).[456] Determining the IP address of a user thus permits a Super-Intermediary to tailor content for the user, either making it available, providing an altered version, or blocking it entirely.

For instance, in *UEJF & LICRA v. Yahoo! Inc.*,[457] a French court ordered Yahoo! Inc. to prevent internet users based in France from accessing auctions of Nazi memorabilia through an auction service then available on Yahoo.[458] The court held that Yahoo "is in

---

[454] Other methods worthy of mention include mapping wi-fi networks, using GPS, or some combination. *See* Steven J. Vaughan-Nichols, *How Google—and everyone else—gets Wi-Fi location data*, ZDNET (Nov. 16, 2011), http://www.zdnet.com/blog/networking/how-google-and-everyone-else-gets-wi-fi-location-data/1664.

[455] Microsoft Support, *Understanding TCP/IP Addressing and Subnetting Basics*, http://support.microsoft.com/kb/164015 (last visited Apr. 18, 2013).

[456] Go Daddy Support, *How Do Domain Names Work?* (Apr. 30, 2011), http://support.godaddy.com/help/article/327/how-do-domain-names-work.

[457] Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000, *translation available at* http://www.lapres.net/yahen.html.

[458] *Id.*

a position to identify the geographical origin of the site which is coming to visit, based on the IP address of the caller, which should therefore enable it to prohibit surfers from France" from accessing Nazi memorabilia.[459] The case provides a significant example of the difficult choices Super-Intermediaries face regarding the tension between freedom of expression and religious hatred. As noted previously, eBay's offering of *Mein Kampf* differs significantly between its American and French sites, no doubt due to French law and the *UEJF & LICRA* decision.[460] Google has also taken action regarding religious content even when it faces no affirmative legal obligation. In 2004, the top hit for "Jew" was an anti-Semitic website, and searches for "Holocaust" or "Jew" led to first-page results for Holocaust denial sites.[461] Google placed a notice on the search-result page for "Jew" explaining how its algorithm works.[462]

Based on research to date, YouTube appears to be using IP geolocation to filter content in certain Islamic countries with the *Innocence of Muslims* video. If somebody from an IP address in the United States goes to the Turkish YouTube site, www.youtube.com.tr, the user is redirected to a Turkish version of the site run at the main youtube.com domain.[463] If one searches this Turkish version of the site for "Innocence of Muslims," one is able to access the video in full. But according to reports, if one tries the same thing from countries where the video is restricted by YouTube,

---

[459] *Id.* The actual court order is much broader, stating the court orders "Yahoo! Inc. to take such measures as will dissuade and render impossible any and all consultation on Yahoo.com of the auction service for Nazi objects as well as any other site or service which makes apologies of Nazism or questions of the existence of Nazi crimes." *Id.* However, the court's discussion appears to make clear that the injunction is intended to be limited to auctions aimed at French users. *Id.*

[460] *See supra* text accompanying notes 451-52.

[461] VAIDHYANATHAN, *supra* note 5, at 64-65. Unlike the United States, where Google is not required to remove such materials, in Germany and France, Google is required to "block anti-Semitic and other hate-filled sites." *Id.* at 47. Similarly, in Egypt, India, and Thailand, Google "actively removes links to content that offends the state." *Id.*

[462] *Id.* at 65.

[463] *See* YouTube Turkish site, http://www.youtube.com/?gl=TR&hl=tr (found via redirection from www.youtube.com.tr).

the video will likely be blocked.[464] This is likely the result of IP address geolocation and not the functioning of a country-code domain name.[465] As evidence, a report from Reuters about YouTube Turkey states "[a] YouTube spokeswoman said Internet users *browsing on a Turkish IP address* would automatically be redirected to the 'youtube.com.tr' domain."[466] This suggests that *any* user using an IP address from a country where the video is banned will not be able to view the video at all, regardless of whether the user attempts to access the video through YouTube.com (U.S. and general) or YouTube.com.tr (Turkey).[467]

---

[464] YouTube's website indicates that certain videos may be unavailable in some countries "in order to comply with local laws." YouTube, *Video Not Available in My Country*, *available at* https://support.google.com/youtube/answer/92571?hl=en-uk (last visited Sept. 20, 2013). One source further notes that "[w]here YouTube is localised with country-specific versions of the site, Google [which owns YouTube] routinely accepts government requests to restrict local access to content that clearly violates local laws," and that "Google has restricted access to Innocence of Muslims in Saudi Arabia, Jordan, India, Indonesia, Malaysia and Singapore on these grounds." Brian Pellot, *Has Innocence of Muslims Ended the Innocence of YouTube?*, FREE SPEECH DEBATE (Sept. 26, 2012), http://freespeechdebate.com/en/discuss/has-innocence-of-muslims-ended-the-innocence-of-youtube; *see also* Jessica Phelan, *Egypt Orders YouTube Blocked Over 'Innocence of Muslims' Video*, GLOBAL POST (Feb. 9, 2013), http://www.globalpost.com/dispatch/news/regions/middle-east/egypt/130209/youtube-blocked-egypt-innocence-of-muslims-video (noting that YouTube restricted local access to the video).

[465] *See* Jerusha Burnett, Note, *Geographically Restricted Streaming Content and Evasion of Geolocation: The Applicability of the Copyright Anticircumvention Rules*, 19 MICH. TELECOMM. & TECH. L. REV. 461, 466 (2013) (explaining IP geolocation).

[466] *See* Ozbilgin, *supra* note 241; *see also* Land, *Law of Internet*, supra note 26, at 452-53 (noting that after Turkey blocked YouTube due to other videos, Google decided to block YouTube videos in Turkey that violated Turkish law).

[467] In contrast, Google.com does not appear to restrict content from its search engine in the same way. Thus, if a user from Turkey tries to search Google.com for the video, the video would apparently appear in the results. However, if a user with a Turkish IP address then tried to click through from the search engine to the YouTube site, the video apparently will not be accessible. Instead, a message will inform the user that the video is not available for viewing on YouTube in that region. Thus, although the Google.com search engine is less limited than YouTube, one apparently still faces the roadblock of IP address geolocation for the video, since YouTube content must be viewed on a YouTube site.

c. Firewalls, Filters, and Deep-Packet Inspection

Another type of control is the use of physical or technological means to block or filter content at major points in internet infrastructure, such as "backbone" providers.[468] Such controls might be used for a large area or a smaller area, such as a local internet service provider.[469] A crude example would be severing the cables providing internet service into a country. However, disconnecting major cables could prevent much of a country from accessing all or major portions of the internet, would be quickly noticed, and may be undesirable even for authoritarian states that permit their citizens to engage in more innocuous activities on the internet.[470] More likely to be employed are hardware or software "firewalls" that restrict or limit access to disapproved sites or materials in a geographic region. Such technology may involve "deep-packet inspection" (DPI), which examines data as it runs through the internet, taking actions such as preventing it from reaching its destination.[471]

The most famous firewall, of course, is the so-called "Great Firewall of China,"[472] which the Chinese government uses to try to prevent access to many popular western sites, such as Facebook.com,

---

[468] *See* ANDREW BLUM, TUBES: A JOURNEY TO THE CENTER OF THE INTERNET 14 (2012) (explaining the *physical* structure of the internet, such as the "backbone architecture," which serves as the "key links between cities").

[469] Egypt has only a "limited number of Internet service providers," perhaps as few as four, making it "relatively easy for the government to close the Internet" during the Arab Spring. WEAVER, *supra* note 10, at 79. Libya also "tried to sever Internet access." *Id.* at 83.

[470] "In reality, as the situations in Iran and Egypt reveal, governments are reluctant to completely shut down the Internet," because it is "too important for commerce and other non protest activities" such as communicating with family and friends. *Id.*

[471] *See* MACKINNON, *supra* note 14, at 58; MUELLER, *supra* note 37, at 151; SCHMIDT & COHEN, *supra* note 19, at 84.

[472] *See* MACKINNON, *supra* note 14, at 34-40 (discussing Great Firewall and Chinese censorship); VAIDHYANATHAN, *supra* note 5, at 124-28 (discussing Chinese censorship including the Great Firewall); Richard Clayton et al., *Ignoring the Great Firewall of China*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 273 (2007) (describing the Great Firewall and discussing possible ways of evading such censorship).

YouTube.com, and Twitter.com.[473] Google.com is often blocked, but sometimes not.[474] In contrast, eBay.com appears to be available in China.[475] Rather than being "sturdy and impenetrable," China's filtering is "fluid and situational."[476] Ironically, the site of a premier advocacy of openness on the Internet, the Electronic Frontier Foundation (EFF), is not screened by the Great Firewall.[477] This does not suggest that the Chinese government views the EFF favorably, but rather, that the EFF is probably not on China's radar, in contrast to Super-Intermediaries whose activities may more directly frustrate governmental interests. The potential uses of filters, firewalls, and DPI can vary significantly, with one report of the Chinese government filtering specific hashtags on Weibo (the Chinese equivalent of Twitter) province-by-province.[478]

d. Application-Level Controls

Additionally, intermediaries—and particularly Super-Intermediaries—may use a variety of application-level technological controls. By this term, the article refers to how the website or "app" behaves from the perspective of a user. Here are four significant examples.[479] First, an intermediary might geographically filter what

---

[473] Based on tests updated July 19, 2013, none of these sites were accessible in Beijing, Shenzen, Inner Mongolia, Heilongjiang Province, and Yunnan Province. *See* Greatfirewallofchina.org, http://www.greatfirewallofchina.org/ (last visited Aug. 15, 2013).

[474] Based on tests conducted July 19, 2013, google.com was accessible in Beijing, Shenzen, Inner Mongolia, Heilongjiang Province, and Yunnan Province. *See* Greatfirewallofchina.org, *supra* note 473. The same search conducted on August 15, 2013 showed that google.com failed or timed out in each province. *Id.*

[475] Based on tests updated July 19, 2013, ebay.com was accessible in Beijing, Shenzen, Inner Mongolia, Heilongjiang Province, and Yunnan Province. *See* Greatfirewallofchina.org, *supra* note 473.

[476] VAIDHYANATHAN, *supra* note 5, at 125.

[477] Based on tests updated July 19, 2013, eff.org was accessible in Beijing, Shenzen, Inner Mongolia, Heilongjiang Province, and Yunnan Province. *See* Greatfirewallofchina.org, *supra* note 473.

[478] ASSANGE, *supra* note 141, at 118 (statement of Jérémie Zimmermann).

[479] There are other worthy examples, such as 1) requiring users to create

the user may see as part of her or his experience. This is essentially what YouTube appears to be doing with *Innocence of Muslims*, apparently filtering content based on the user's geographical IP address.

Second, intermediaries may embed technology into their websites and applications to enable user complaints. As noted above, many sites allow users to click on a button to flag or report content that may be inappropriate.[480] For instance, on YouTube one can click on a "flag" icon that reveals reporting options, such as sexual content, violent or repulsive content, hateful or abusive content, harmful dangerous acts, child abuse, spam or misleading, infringement, and more.[481] YouTube states that "[f]lagged videos and users are reviewed by YouTube staff 24 hours a day, seven days a week to determine whether they violate Community Guideline[s]."[482] At this point, the technological control—the flag—triggers a realspace review by a person working for YouTube to determine compliance with Community Guidelines.[483]

---

account names with passwords for access or more complete access; and 2) installing spam filters into email systems. Service providers may also suspend or terminate abusers or repeat infringers, and as of this writing, intermediaries are rolling out the so-called "six strikes" system. *See* Cyrus Farivar, *Here's What an Actual "Six Strikes" Copyright Alert Looks Like*, ARS TECHNICA (Feb. 27, 2013), http://arstechnica.com/tech-policy/2013/02/heres-what-an-actual-six-strikes-copyright-alert-looks-like. As suspension, termination, or intermediate solutions such as "copyright sensitivity training" are done after the fact rather than as a part of active content control, they are worth mentioning here only in passing. Also, users themselves can choose to filter content as well through parental controls and browser-based pop-up filters, but such choices are made by the user and not the service provider.

[480] *See supra* notes 437-45 (discussing realspace controls). To be sure, the line between a realspace control and a technological control may be subtle, and such processes can be combined. Here, the "flag" control is initiated by a realspace person, but relies on underlying technology. In turn, any final decision to remove flagged content is made by people working for the intermediary.

[481] To view the quoted text, log into YouTube.com and pull up any video. Then click on the flag icon. The quoted text will appear below a laundry list of flaggable issues.

[482] *Id.*

[483] One source states that Google removes a YouTube video even if just "a few people flag them as inappropriate." VAIDHYANATHAN, *supra* note 5, at 150.

A third example of technological control is automated filtering.[484] For example, eBay uses a "fraud engine" that uses filters to ferret out listings where counterfeiting may exist.[485] Additionally, YouTube uses a "Content Identification" system that permits copyright owners to submit audio and video files; YouTube then uses those files to create digital "fingerprints" that can be used by copyright owners to block, track, or monetize what otherwise might be copyright infringement.[486] The Content ID system has been harshly criticized for blocking lawful fair uses of content, and for having an appeals process that does not work effectively.[487]

Fourth, Google's search engine provides an "autocomplete" feature that suggests searches depending on what is being typed into the search field. However, some suggestions that one would expect to show up do not, and therefore appear to be blocked at the application level by Google. This may make content harder for users to find. Thus, a report in 2012 stated that "Google has quietly expanded its list of censored search phrases with the addition of The Pirate Bay's domain names," "prevent[ing] popular keywords from appearing in Google's Instant and Autocomplete search services, while the pages themselves remain indexed."[488] This filtering is not limited to intellectual property matters, but may include matters of social or

---

[484] Professor Julie Cohen notes that "copyright industries have leaned heavily on Internet intermediaries to adopt protocols designed to screen out infringing content," even though such filters are not required by the DMCA. COHEN, *supra* note 406, at 163; *see also* Nathenson, *Civil Procedures*, *supra* note 86, at 936-40 (discussing automated filtering).

[485] *See supra* text accompanying notes 99-100.

[486] YouTube, *Content ID*, http://www.youtube.com/t/contentid.

[487] *See* Nathenson, *Civil Procedures*, *supra* note 86, at 939; *see also* Thabet Alfishawi, *Improving Content ID*, YOUTUBE (Oct. 3, 2012), http://youtube-global.blogspot.com/2012/10/improving-content-id.html.

[488] Ernesto, *Google Adds Pirate Bay Domains to Censorship List*, TORRENTFREAK, http://torrentfreak.com/google-adds-pirate-bay-domains-to-censorship-list-120910/ (last visited July 14, 2013). One source notes that over a one-year period, Google received requests to remove 870,923 Pirate Bay URLs from the Google search engine. Ernesto, *The Pirate Bay Moves to .GL Domain in Anticipation of Domain Seizure*, TORRENT FREAK (Apr. 9, 2013), https://torrentfreak.com/the-pirate-bay-moves-to-gl-domain-in-anticipation-of-domain-seizure-130409/.

political concern. For example, at the time of this writing, if one types in "Google suc" or "NBC suc," the autocomplete feature suggests "Google sucks" and "NBC sucks." But, if one types in "Viacom suc," you do not get the suggested search "Viacom sucks," you get "Viacom success." But if one types the entire phrase "Viacom sucks" and hits enter, Google shows numerous results. One must wonder whether this difference is due to the vagaries of Google's algorithm, or is instead due to long-standing litigation between Google and Viacom over YouTube. But to the best of the author's knowledge, we don't know, suggesting that filtering of search-engine suggestions lacks significant transparency.[489]

3. Hybrid Controls

To refine the discussion above, it should be noted that information-content management can also be done through *hybrid* controls that combine multiple forms of content management. Here are some examples. First, a country-code domain name may be combined with IP address geolocation to make it extremely difficult for users to access prohibited information. This permits the service provider to tailor its results for a particular country and to frustrate users who want to access locally blocked content. Thus, it would appear that if users with Turkish IP addresses want to see *Innocence of Muslims*, they cannot do so using normal means of access, regardless of whether they visit YouTube.com.tr or YouTube.com.[490]

Second, intermediaries may use technological and realspace controls in tandem.[491] Thus, Facebook receives two million reports

---

[489] One source reported in July 2013 that iPhones do not autocorrect misspellings of charged words such as "'abortion,' 'rape,' 'ammo,' and 'bullet.'" Michael Keller, *The Apple 'Kill List': What Your iPhone Doesn't Want You to Type* (June 16, 2013), THE DAILY BEAST, http://www.thedailybeast.com/articles/2013/07/16/the-apple-kill-list-what-your-iphone-doesn-t-want-you-to-type.html.

[490] For a discussion of circumvention tools, see *infra* text accompanying notes 615-18.

[491] *See* MACKINNON, *supra* note 14, at 153 (noting that Facebook uses "human and automated enforcement" to control spammers and criminals).

per week from users regarding potentially abusive content.[492] Because some abusive content is not reported, and because only twenty percent of reported content falls within Facebook's definition of abusiveness, Facebook uses multiple processes, such as software that identifies image patterns, keywords, and communication patterns, along with review by human staff.[493] Similarly, YouTube combines automated and human review as a partial means for protecting copyrights. Thus, if YouTube blocks user content pursuant to its Content ID program, the user may dispute the blockage. At that point, YouTube notifies the copyright owner, who must then initiate the more traditional DMCA takedown process to seek removal. As a result, a realspace information control (takedown notices) is built on top of a technological information control (Content ID). Although the dispute process is intended to provide a safety valve to users, YouTube has apparently been inconsistent regarding the process for users to dispute the blocking of their videos.[494]

V. What Should We Do?

In light of this article's discussion of Super-Intermediaries,[495] of the tensions regarding the right of expression in the International

---

[492] MACKINNON, *supra* note 14, at 154.

[493] *Id.*

[494] In 2012, YouTube claimed to "introduce[] an appeals process that gives eligible users a new choice when dealing with a rejected dispute. When the user files an appeal, a content owner has two options: release the claim or file a formal DMCA notification." Thabet Alfishawi, *Improving Content ID*, YOUTUBE BLOG (Oct. 3, 2012), http://youtube-global.blogspot.com/2012/10/improving-content-id.html. YouTube stated "[p]rior to today, if a content owner rejected that dispute, the user was left with no recourse for certain types of Content ID claims (e.g., monetize claims)." This is an odd claim for YouTube to make, as it had at least as early as 2010 promoted its use of the DMCA notice and put-back process as an adjunct to Content ID. *See* Nathenson, *Civil Procedures*, *supra* note 86, at 941-42 (noting that if a user disputes a Content ID block, the copyright owner will have to "'submit a copyright takedown notice'" (quoting *Copyright Claim Disputes*, YOUTUBE, http://www.google.com/support/youtube/bin/answer.py?answer=83768 (last visited Dec. 20, 2010))).

[495] *See supra* Part I.

Bill of Human Rights,[496] and of the overlapping and oftentimes non-transparent nature of Super-Intermediary content regulation,[497] Part V attempts to address what, if anything, might be done with difficult speech scenarios such as those raised by *Innocence of Muslims*.[498]

Several preliminary points must be made. First, as noted, this article does not make a normative claim about how to balance free expression with concerns such as defamation of religion. Having said that, the author has little doubt that his perspective is typical of western academics, and his inclination towards treating expression as a primary value has likely infected the analysis herein in ways that the author himself may not entirely recognize. For that, the author apologizes, but hopes that he has been careful to present a balanced discussion. Second, the article does not make a descriptive claim that identifies "hate speech," "defamation of religion," or other categories of potentially offensive speech. Not only is that beyond the scope of the present article, but considering the international scope of the issues presented, might be an empty task. Third, this Part does not address whether the problem should be handled through public law legislation such as the proposed Global Online Freedom Act, as such laws are unlikely to provide global guidance and may lead to other problems.[499]

With those caveats, this Part explores a number of approaches Super-Intermediaries might take when again confronted with difficult and incendiary content such as *Innocence of Muslims*. First, it will ask whether Super-Intermediaries should do nothing, and simply follow current practices. Second, it will consider a community-based approach, as suggested by Professor Tim Wu.[500] Third, it will con-

---

[496] *See supra* Part III.

[497] *See supra* Part IV.

[498] *See supra* Part II.

[499] *See* Global Online Freedom Act of 2007, H.R. 275, 110th Cong. § 201 (2007); *see also* MACKINNON, *supra* note 14, at 174 (noting that "one-size-fits-all" approaches such as the abortive "Global Online Freedom Act" are likely to be impossible); Bambauer, *Cybersieves*, *supra* note 39, at 425-27.

[500] Tim Wu, *When Censorship Makes Sense: How YouTube Should Police Hate Speech*, NEW REPUBLIC (Sept. 18, 2012), http://www.tnr.com/blog/plank/107404/when-censorship-makes-sense-how-youtube-should-police-hate-speech. Professor Edward Lee also provides interesting commentary on

sider whether dispute-resolution bodies might be an appropriate solution. Fourth, it asks whether a technological approach such as automated filtering might be appropriate. Finally, the article will conclude with a normative claim, namely, a number of *process*-based guiding principles, or guidelines for *Digital Due Process*, that might be of assistance to Super-Intermediaries facing scrutiny for speech that is lawful in one region, but illegal or inflammatory in another. Notably, the article suggests the Digital Due Process is more likely to be satisfied through a *combination* of code-based processes and realspace processes with human involvement.

A. Nothing

One approach is that Super-Intermediaries do nothing different. This is not to say that they should do *nothing* at all, or that they should never remove questionable content. Instead, it means that they continue with the current pastiche of realspace and technological controls as discussed in Part IV. Indeed, under their current approach, Super-Intermediaries will typically remove content when ordered to do so by a governmental authority. But this approach is incomplete: there is little doubt that the *Innocence of Muslims* video represents a "watershed" moment in the development of the Internet. Therefore, the time may be ripe to demand greater transparency from intermediaries that remove content, and from governments and private parties that seek such removals.

---

whether *Innocence of Muslims* actress Cindy Lee Crawford might be able to use intellectual property law, namely the right of publicity, to seek relief over the dissemination of the video. *See Lee*, *supra* note 210. Of course, Professor Lee does not suggest that intellectual property law would be a panacea for all cases, since the ability to assert intellectual property claims is limited to the owner or an appropriate licensee. Here, in contrast, the issue is the broader question of how Super-Intermediaries might handle claims of religious, racial, cultural, or ethnic offense when the potential claimants are diffuse, lack standing, and may not agree on the appropriate reaction.

B. Communities

Professor Tim Wu has proposed an interesting solution to deal with matters like *Innocence of Muslims*. He suggests the creation of "a process that relies on a community, either of regional experts or the serious users of YouTube."[501] In such a system,

> Community members would (as they do now) flag dangerous or illegal videos for deletion. Google would decide the easy cases itself, and turn the hard cases over to the community, which would aim for a rough consensus. Such a system would be an early-warning signal that might have prevented riots in the first place.[502]

Regarding the process itself, Professor Wu says:

> Like now, any user could nominate a video for deletion, and if it fell clearly within the categories above, it would be speedily deleted. But for the hard questions, Google could demand that the nominator argue its case to either a global (for all of YouTube) or regional (for country specific sites) community forum. YouTube users of good standing—those that actually upload videos on a consistent basis—would be allowed to comment, until some kind of rough consensus is reached.[503]

Professor Wu's suggestion ought to be taken seriously, but by his own admission, the proposal raises theoretical and practical objections. The chosen community might be too restrictive, too loose, or simply might not attract sufficient numbers of responsible people.[504] He therefore suggests looking to the model of Wikipedia,

---

[501] Wu, *supra* note 500.
[502] *Id.*
[503] *Id.*
[504] *Id.*

where "any user can propose the deletion of a page that does not fit Wikipedia's content guidelines."[505] Such a proposal leads to debate "until a rough consensus is reached, which it usually is."[506] He notes that although Wikipedia's approach is not perfect, "it has kept Wikipedia from becoming Spampedia, a forum for ideological projects, or simply a tool for marketing companies who want to flog unknown products."[507] He acknowledges that attracting responsible YouTubers might be problematic, in which case it might be preferable to set up "regionalized panels of good citizens, acting as judges, who would be willing to opine on the hard questions, the way that panels of prominent authors decide what words should be in the American Heritage Dictionary."[508]

There is much to admire in Professor Wu's approach, but the observations made in this article regarding territoriality and human rights law further complicate his wikified proposal.[509] For one thing, it must be noted that Wikipedia is written in numerous different languages: according to the English Wikipedia entry about Wikipedia viewed in July 2013, there are "30 million articles in 286 languages."[510] Moreover, the articles in the different language-versions of Wikipedia can vary considerably.[511] For instance, the English-

---

[505] *Id.*; *see also* Citron & Norton, *supra* note 8, at 1480 (noting that the "Wikipedia model may prove helpful to intermediaries" setting up systems to respond to abuse reports).

[506] Wu, *supra* note 500.

[507] *Id.*

[508] *Id.*

[509] Professor Molly Land addresses analogous concerns in an article that asks whether volunteers could be used to peer-produce human rights reporting. *See* Molly Beutz Land, *Peer Producing Human Rights*, 46 ALBERTA L. REV. 1115 (2009) [hereinafter Land, *Peer Producing*]. She argues that open models of peer production might increase participation but would reduce accuracy; therefore, she suggests using a fact-finding model with limited participation. *Id.* at 1117; *see also* Molly Beutz Land, *Networked Activism*, 33 HARV. HUM. RTS. J. 205, 223 (2009) (noting that power law creates "an inverse relationship between meaningful participation and broad mobilization").

[510] Wikipedia, *Wikipedia*, http://en.wikipedia.org/wiki/Wikipedia (last visited July 18, 2013).

[511] Additionally, "[e]ach different language version of Wikipedia forms its own policies, enforcement schemes, and norms." JONATHAN ZITTRAIN, THE

language article on *Innocence of Muslims* is quite different from the French-language article on *L'Innocence des Musulmans*.[512] Thus, the social architecture and decision-making processes in Wikipedia may implicitly incorporate the existence of some of the social values that are likely to be common within a language group.

But even then, not all members of a language group automatically share identical values on matters such as speech or religion.[513] Professor Roy Balleste, writing with Joanna Kulesza, points to the modern nation-state as a development emerging from the Peace of Westphalia in 1648, which ended the Thirty Years War.[514] The modern "nation state" would thus be a "communit[y] formed by individuals with joint values, history and culture rather than solely by a single sovereign's exercise of power over a group of individuals."[515] Their observations provide additional fodder for the difficulty of trying to use "community" as a basis for resolving disputes over politically or religiously charged speech. From a world perspective, it is difficult, and perhaps impossible, to find joint values, history, and culture on a level of specificity that permits resolving issues like *Innocence of Muslims*. Even within the territorial borders of a na-

---

FUTURE OF THE INTERNET—AND HOW TO STOP IT 143-44 (2008).

[512] *Compare* Wikipedia, *Innocence of Muslims*, http://en.wikipedia.org/wiki/Innocence_of_muslims (last visited July 14, 2013), *with* Wikipédia, *L'Innocence des Musulmans*, http://fr.wikipedia.org/wiki/Innocence_of_Muslims (last visited July 14, 2013).

[513] Languages tend to be one of the great groupings in social ordering that lead to social interchanges that can foster meetings of the minds. However, one need only look to the political and social discord over the past century in the United States on matters such as civil rights, abortion, and race relations to realize that a shared language is no guarantee of accord. Moreover, when languages vary, the potential for value-disconnects may increase. Indeed, disputes over Wikipedia content are likely to be resolved by persons speaking the same language, whereas disputes regarding YouTube videos may be more likely to transcend languages, making the Wikipedia model a problematic solution.

[514] Roy Balleste & Joanna Kulesza, *Signs and Portents in Cyberspace: The Rise of Jus Internet as a New Order in International Law*, 23 FORDHAM INTELL. PROP. MEDIA &ENT. L.J. 1311, 1316-17 (2013); see also MACKINNON, *supra* note 14, at 12 (discussing Treaty of Westphalia).

[515] Balleste & Kulesza, *supra* note 514, at 1318 (citing J. Samuel Barkin & Bruce Cronin, *The State and the Nation: Changing Norms and the Rules of Sovereignty in International Relations*, 48 INT'L ORG. 107, 110 (1994)).

tion-state, values, history, culture, language, and much more can diverge significantly.[516] Along analogous lines, Professor Jonathan Zittrain notes that "[u]nlike Wikipedia, no one thinks that Google ought to be 'governed' by its users in some democratic or communitarian way."[517]

Moreover, in Wikipedia, participants can hide behind pseudonyms. Would participants in a YouTube decision-making community also be permitted to retain anonymity?[518] If so, that would encourage some to act honestly.[519] But it would also encourage trolling by devoted troublemakers as well as shills acting on behalf of governments and other interest groups.[520] The alternative of requiring real names is even more troubling.[521] Suppose participants were required to use their real names: any speech issue that is incendiary enough (such as *Innocence of Muslims*) to merit a decision from a user community could expose the participants to reprisals from opponents and government authorities in their home countries.

---

[516] *Cf. id.* at 1315 ("A stronger case can be made that no territorially-based regime may be successfully applied to an aterritorial cyberspace.").

[517] ZITTRAIN, *supra* note 511, at 147.

[518] *See* Land, *Peer Producing*, *supra* note 509, at 1117 (noting potential dangers).

[519] *See* MOROZOV, *supra* note 23, at 271-72 (noting that human rights reporting has generally taken care to avoid revealing information that would permit identification of victims).

[520] *See* Bambauer, *Censorship v.3.1*, *supra* note 150, at 29 (noting China's use of persons employed by the government to post supportive comments); Land, *Peer Producing*, *supra* note 509, at 1127 (noting that public system may invite gaming to produce outcomes).

[521] A Facebook page entitled "We Are All Khaled Said" was suddenly shut down by Facebook without warning because the administrators of the page failed to use their real names. *See* MACKINNON, *supra* note 14, at 151. The page was restored within 24 hours, but only after the page was handed over to another administrator willing to verify a true identity. *Id.*; *see also supra* note 10 (describing Facebook page created in memory of man killed by Egyptian police). The irony of a real-name policy is the plethora of existing fake name accounts on Facebook, such as dozens of users with the rather unlikely name of "Donald Duck." *See* MACKINNON, *supra* note 14, at 156.

C. Monitoring and Dispute-Resolution Bodies

Another potential solution is to assemble monitoring bodies or dispute-resolution bodies akin to the Human Rights Committee of the Office of the United Nations High Commissioner for Human Rights (HRC).[522] Regarding monitoring, state parties are required to submit reports regularly to the HRC on rights implementation.[523] Additionally, the HRC can serve as a dispute-resolution mechanism. Article 41 of the ICCPR envisions inter-state complaints, and the HRC can hear complaints from individuals against countries joining the First Optional Protocol to the ICCPR.[524]

Of course, Super-Intermediaries are not States and are not directly subject to the ICCPR. Regardless, such a mechanism is again problematic. First, who would have standing to assert a claim? Consider that intellectual property rights belong to *owners* who can self-identify. This limits the number of claimants and allows providers to deal with the claimant. But with issues regarding hate speech and defamation of religion, it is *groups* that may be offended, making for a diffuse set of potential claimants.

Second, with incendiary matters such as *Innocence of Muslims*, timely action may be imperative, suggesting that a more streamlined process may be appropriate.

Third, the tensions regarding speech in the ICCPR may make it an unpalatable model for intermediaries, at least to the extent that such a deliberative body might follow the strictures of ICCPR 20(2) regarding inciting hatred against religions.[525] Indeed, it should be recalled that even though the Global Network Initiative's Principles are based on the International Bill of Human Rights including the ICCPR, the Principles omit reference to Article 20, which leaves a potentially significant gap when disputes involve a clash between

---

[522] Office of the United Nations High Commissioner for Human Rights, http://www2.ohchr.org/english/bodies/hrc/ (last visited July 14, 2013).

[523] *Id.*

[524] *Id.*; *see also* ICCPR, *supra* note 44, at art. 41; ICCPR, First Optional Protocol, *supra* note 262.

[525] *See supra* Part III.C.

defamation of religion and freedom of expression.[526]

Fourth, should such a body have the power to issue binding orders against Super-Intermediaries? If such a body solely monitors and issues reports, then it would be up to the intermediaries to comply. But if the body were an actual dispute-resolution tribunal with the power to issue binding judgments, there would have to be enforcement mechanisms, something that large companies with shareholders are unlikely to agree to.[527] If judgments were non-binding, then one must wonder whether a losing intermediary might be tempted to flout the judgment, or to cease participating in disputes before that organization.

This is not to say that there is no value in assembling dispute-resolution bodies.[528] However, any such process should involve multiple stakeholders, including governments, representatives of interested religious, ethnic, racial, and nationality groups, as well as representatives of stakeholder industries, such as other intermediaries.[529] More fundamentally, one might wonder—in an era where code can tailor the information available in each territory—whether a body dedicated to deciding international issues would add significant

---

[526] *See* GNI, *Principles*, *supra* note 328.

[527] *Cf.* Mary Rundle & Malcolm Birdling, *Filtering and the International System: A Question of Commitment*, *in* ACCESS DENIED, *supra* note 175, at 73, 87 (noting that it "remains difficult to secure" state compliance of obligations under the ICCPR).

[528] *But see* MACKINNON, *supra* note 14, at 139 (noting that "the complexities and dilemmas" faced by GNI members mean that they cannot "escape[] all . . . future problems"). One potential model worth considering, but beyond the scope of this article, is the International Centre for Settlement of Investment Disputes (ICSID), "an autonomous international institution established under the Convention on the Settlement of Investment Disputes between States and Nationals of Other States." About ICSID, https://icsid.worldbank.org/ICSID/FrontServlet?requestType=CasesRH&actionVal=ShowHome&pageName=AboutICSID_Home (last visited Sept. 23, 2013). "ICSID was created by the Convention as an impartial international forum providing facilities for the resolution of legal disputes between eligible parties, through conciliation or arbitration procedures." *Id.*

[529] *See* MACKINNON, *supra* note 14, at 202 (stating that "counting on the United Nations" to "protect human rights online has already been proven to be counterproductive").

process with little corresponding gain.[530]

D. Code

Another option is to use code to foster human rights values. Some writers, such as Schmidt and Cohen, continue to repeat the mantra that "technology is neutral," treating it as a "central truth of the technology industry."[531] But nothing could be further from the truth: just like any regulator, code is a form of architecture that can embed values.[532] Evgeny Morozov argues that we cannot give technology "a free pass on ethics" because technology design "simply conceals the ideologies and political agendas of their creators."[533] It therefore cannot be said that all technologies are neutral.[534] Just as

---

[530] For instance, Professor Milton Mueller notes that the Internet Governance Forum has been "dismissed as a meaningless talk shop." MUELLER, *supra* note 37, at 107 (citing ZITTRAIN, *supra* note 511, at 243).

[531] SCHMIDT & COHEN, *supra* note 19, at 66. The "instrumental" view of technology views technology as neutral; in contrast, the "substantive" view rejects technology neutrality. *See* Amy Salyzyn, *A New Lens: Reframing the Conversation about the Use of Video Conferencing in Civil Trials in Ontario*, 50 OSGOODE HALL L.J. 429, 440-41 (2012).

[532] *See* LESSIG, CODE 2.0, *supra* note 104, at 6 ("We can build, or architect, or *code* cyberspace to protect values that we believe are fundamental." (emphasis in original)).

[533] MOROZOV, *supra* note 23, at 298. He similarly decries the idea of "tool neutrality." *Id.*

[534] Citing philosopher Martin Heidegger, Professor Beth Noveck notes that "technology is not neutral but is the reflection of our social values." Beth Simone Noveck, *Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer*, 9 B.U. J. SCI. & TECH. L. 1, 10 (2003) (citing Martin Heidegger, *La Question de la Technique*, in ESSAIS ET CONFÉRENCES (André Préau trans., 1954)). In an English translation, Heidegger says "we are delivered over to [technology] in the worst possible way when we regard it as something neutral; for this conception of it . . . makes us utterly blind to the essence of technology." MARTIN HEIDEGGER, THE QUESTION CONCERNING TECHNOLOGY 4 (William Lovitt trans. 1977); *see also* VAIDHYANATHAN, *supra* note 5, at 62 (noting that "[a]ll information technologies favor some content or users over others," and that "[o]ne cannot design a neutral system"); Jay P. Kesan & Rajiv C. Shah, *Deconstructing Code*, 6 YALE J. L. & TECH. 277, 279 (2004) (stating that "code is not neutral and apolitical but instead embodies the values and motivations of the institutions and

censorship and copyright laws embody societal values to restrict certain kinds of speech, so do code-based filters that block the very same speech. If code is law, then code-as-law embodies norms that foster or frustrate often-conflicting societal values.[535]

Even though code is "no panacea for the world's ills," code can nevertheless have some benefits. Schmidt and Cohen assert that "smart uses of technology can make a world of difference."[536] Professor Molly Land similarly argues that technology companies should "embed 'human rights defaults' into their technology."[537] Indeed, there are numerous ways that code can be used in ways that impact human rights values.[538] As noted, a video-sharing site can include "flag" buttons that permit users to alert providers to potentially inappropriate content.[539] Thus, a user who stumbles across a video with arguable pornography or hate speech could click on the flag button to alert the video site's abuse department. At that point, the video site would have to use human reviewers to determine whether the video is illegal, or if not illegal, whether the video nonetheless violates community guidelines. Equally so, a site might have filters set up that scan user submissions for evidence of prohibited content, such as keywords that suggest that a video might contain pornography.

Once a decision is made by an abuse department to block or limit access to content, additional code might be used. Here are some examples. First, a video might be blocked in its entirety worldwide. Second, a video could remain available, but users might have to first click through a warning screen. Third, a video—with or without warning screens—might be made accessible in some regions but not in others. An intermediary might *try* to do this by tailoring

---

actors building it" (italics removed)).

[535] Julian Assange notes that technology is not neutral, maintaining that we can and must "build the tools of a new democracy." ASSANGE, *supra* note 141, at 151.

[536] SCHMIDT & COHEN, *supra* note 19, at 24.

[537] Land, *Law of Internet*, supra note 26, at 396.

[538] *See* LESSIG, CODE 2.0, *supra* note 104, at 125 (stating that "code embeds certain values or makes certain values impossible").

[539] *See supra* Part IV.B.2.d.

different versions of its site to different country-code domain names, such as having different versions of YouTube at YouTube.com (U.S. and general), YouTube.fr (France), and YouTube.sa (Saudi Arabia). Each site could have different content, depending on local laws, norms, and other factors.

However, the "country-code" approach by itself would be easily circumvented: a user in Saudi Arabia wanting to see *Innocence of Muslims* could simply go to YouTube.com to see the video, even if it is not on the Saudi site. To be clear, I am not suggesting this is a good thing; rather, at this moment, I am describing what can happen. To prevent this kind of circumvention, an intermediary can *additionally* use geolocation—i.e., technology that looks to a user's Internet Protocol address to determine generally where the user is located—to prevent the user from accessing a less-censored version of the site. Thus, if a user in Turkey tries to visit YouTube.com, the use of geolocation can permit YouTube to limit the content *only* to materials approved by YouTube for the Turkish audience. This type of filtering can make it much harder for people lacking more advanced skills to bypass geographic tailoring of internet content.[540]

Since we are discussing how intermediaries might choose to filter content after it is posted, why not take things to the next step: rather than removing content after it is posted, can an intermediary use automated filtering technology to screen for other types of inappropriate content even before the content appears online? To some extent this is already done. YouTube has algorithms to prevent pornography—both adult pornography and child pornography—from appearing online.[541] One way such technology can work is by mak-

---

[540] *See supra* Part IV.B.2.a, IV.B.2.b. Indeed, YouTube appears to use such techniques to restrict the *Innocence of Muslims* video from being viewed in Turkey. *See supra* text accompanying note 466.

[541] *See* Wu, *supra* note 500. Facebook uses Microsoft's PhotoDNA hash technology, and Twitter will soon use it as well. *See* Matt Brian, *Twitter Reportedly Cracking Down on Child Porn with Microsoft PhotoDNA technology*, THE VERGE (July 22, 2013), http://www.theverge.com/2013/7/22/4544616/twitter-microsoft-photodna-child-pornography. Google is reportedly working on industry standards that would facilitate the identification and removal of child pornography. *See* David Barrett, *Google Builds New System to Eradicate Child Porn Images from the Web*, THE TELEGRAPH (June 15, 2013), http://www.telegraph.co.uk/

ing automated comparisons to reference files of known examples of pornography.[542] Another way might be to develop software that recognizes human genitalia or nudity, akin to facial-recognition technology, but which instead recognizes humans who are naked or engaging in sexual activities. Thus, reference files and recognition technology can be used or later developed.

Might such technologies be adapted to pre-screen other forms of content, such as hate speech, or in some Islamic countries, defamation of religion? Although one must be circumspect in predicting future technology, it is difficult to imagine how this might be accomplished. Regarding reference files, one needs a pre-existing file for purposes of comparison. Thus, with any sort of pre-existing content—such as copyrighted movies, or specific, known examples of pornography—the *metes and bounds* of the pre-existing materials are already known. If somebody tries to upload a fresh copy of a known example of copyrighted content or of pornography, a video site could identify its fingerprint and block it. But anything that is new would not match pre-existing reference files. A new video with hate speech, or a new video along the lines of *Innocence of Muslims*, would not be identified through a reference file system of filtering.

What about recognition technology? Might it be possible to create an algorithm that somehow identified hate speech or other types of potentially problematic types of expression? Certainly a site can filter for keywords in a video's title or description. However, it may be difficult, and perhaps impossible, to know from the mere use of the word "Muhammad" in a title or description whether a video is in praise of the prophet, engaging in a slander that may be offensive to Muslims, or is instead a movie review by a young man named Muhammad. Similarly, a video entitled "Violence Against Women" might contain human cruelty, or might be a panel of scholars discussing the legal and societal problems of domestic violence. Equally so, it is difficult to imagine how recognition technology could tell ex

---

technology/google/10122452/Google-builds-new-system-to-eradicate-child-porn-images-from-the-web.html.

[542] Some have circumvented Content ID by doing things such as inverting the video. Also, Content ID has also been used to block content that may well be fair use. *See* Nathenson, *Civil Procedures*, *supra* note 86, at 936-44.

ante—without a pre-existing reference file—whether or not video or audio content violated community guidelines or a country's legal requirements. A video of violence might be a clip from a movie trailer. A video of a man wearing Arabic clothes and saying "my name is Muhammad" may or may not be a portrayal of the Islamic prophet. Simply put, context matters. Perhaps some disputes can never be decided solely by code, especially regarding values that cannot easily be reduced to binary choices.

Although one must speculate, it is likely that any such filtering technology is likely to be grossly underinclusive and overinclusive, missing much potentially relevant content, as well as falsely flagging much that is irrelevant.[543] Further, this will likely always be the case. Whereas literal copying of known fingerprints of copyrights or pornography can be identified with great certainty through simple comparison of an original to a copy, that is not true with *recognition* technology. For recognition technology to help an intermediary to determine what to block automatically, the software would need to be able to make accurate judgments on difficult issues such as violence, harassment, hate speech, and other matters prohibited under community guidelines or local law. Considering that such judgments are oftentimes difficult for courts, it is hard to imagine how such decisions could be programmed.[544]

In short, it may be difficult for intermediaries to use code alone to pre-filter and pre-block many types of content. Instead, the intermediary may need to use additional tools, such as user flagging, governmental and third-party demands, and internal screening, all of which would require an ultimate decision to be made by a human working for the intermediary. In such cases, the ultimate decision-maker would not be *code*, but a human being. However, regardless of whether decisions are made by code, humans, or a combination, perhaps what ultimately matters most are the *processes* used to

---

[543] Unlike well-crafted laws, software tends to lack openness and predictability, instead offering "ruleishness without guaranteeing transparency." James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1734-38 (2005).

[544] Oftentimes, decisions cannot be programmed, particularly on matters requiring "discretion and balancing." Land, *Law of Internet*, supra note 26, at 456.

resolve the dispute. The values of such processes to Digital Due Process are therefore addressed in the final subsection below.

E. Digital Due Process

This final subsection asks whether processes grounded in principles of procedural justice—regardless of whether the processes are embodied in code or realspace—can help. Others have written on the importance of good process regarding internet intermediaries. Rebecca MacKinnon argues forcefully in *Consent of the Networked* that intermediaries have "detailed information" about people, and that "[w]ithout transparency and accountability in the use of this information, democracy will be eroded."[545] Professor Julie Cohen advocates for a "more comprehensive, structural understanding" of how an "information environment can foster, or undermine, capabilities for human flourishing," including the need for operational transparency.[546] Professor Derek Bambauer suggests a "process-based method" to measure the legitimacy of efforts of different countries to limit online materials.[547] In the context of NGOs, Professor Siegfried Wiessner notes the importance of accountability and transparency to an NGO's credibility: "[p]ower, public or private, needs to be checked as intensely as it imposes itself."[548]

1. A Normative Framework for Digital Due Process

Accordingly, let us turn to *Digital Due Process*.[549] Consider-

---

[545] MACKINNON, *supra* note 14, at 81.

[546] COHEN, *supra* note 406, at 224.

[547] Bambauer, *Cybersieves*, *supra* note 39, at 379.

[548] Wiessner, *supra* note 18, at 307, 309-11.

[549] Several other writers have used the phrase "Digital Due Process." For examples, see Land, *Law of Internet*, *supra* note 26, at 448 (using phrase in passing, stating "Article 19(2) therefore provides a basis for increased transparency and accountability for online intermediaries, including the development of digital due process standards"); *see also* Erika Glenn, *Digital Due Process: Using Technology to Ensure Equality When Reciting Miranda Rights to Non-English Speaking*

ing the importance of code processes to the internet, and the fact that Due Process is concerned with, among other things, *process*, Digital Due Process is an idea whose time has come.[550] Digital Due Process would focus on concerns of due process and procedural justice in the digital realm. Because it considers due process in the digital realm, it must consider the roles of not just government, but also the private actors who can have features of power that might rival or even exceed those of realspace governments, at least in relation to the internet. Moreover, by "process," we cannot mean just procedures for litigation, but all matters of process: the code-based processes of software and hardware, and the realspace procedures used by digital actors. Indeed, as will be suggested below, Digital Due Process is likely to be increased when intermediaries consider how code-based processes and realspace-based processes might best work together to increase human dignity and foster human rights.

It might be objected that it is impossible to separate processes relating to speech from the substance of the speech itself.[551] This objection is true to some extent. However, this article has tried to

---

Suspects, 14 HARV. LATINO L. REV. 97 (2011) (title only); Kathryn Elizabeth McCabe, Note, *Just You and Me and Netflix Makes Three: Implications for Allowing "Frictionless Sharing" of Personally Identifiable Information under the Video Privacy Protection Act*, 20 J. INTELL. PROP. L. 413, 417, 435 (2013) (several times in passing). There is also an organization that uses the name as part of its title. *See* Digital Due Process Coalition, *Digital Due Process: Modernizing Surveillance Laws for the Internet Age*, http://www.digitaldueprocess.org (last visited Sept. 25, 2013).

[550] As noted, this article does not recommend a statutory solution: although a statutory prescription may help, the problem is global. *See supra* text accompanying note 499. Notably, Professor Bambauer hypothesizes a statute authorizing governmental orders to require ISPs to block access to specific online material, with "five key features: limited standing, procedural protections, heightened proof requirements, narrow content targeting, and public funding." Bambauer, *Orwell*, *supra* note 39, at 930. Procedural protections would include proper notice, tolling of action for ninety days, regular review of filtering decisions, and a clear and convincing evidence standard of proof. *See id.* at 931-32.

[551] *See* James Grimmelmann, *The Illegal Process: Basic Problems in the Making and Application of Censorship*, 79 U. CHI. L. REV. DIALOGUE 58, 61 (2013) (suggesting that it may be difficult to justify censorship "in the abstract," without considering the actual material being censored, simply on the basis that the censorship was accompanied by good procedure).

remain balanced, avoiding making normative *substantive* claims about what human rights values ought to trump others. This is not to say that procedure and substance are not intertwined: as noted by a member of the House of Representatives, "I'll let you write the substance of a statute, and you let me write the procedure, and I'll screw you every time."[552] In fact, the Constitutional law of speech incorporates procedural elements, such as review under "strict scrutiny," an essentially *procedural* device that shifts the burden of proof to the government.[553]

Accordingly, this article does not make a normative claim about how to balance free expression with other conflicting values. Indeed, Professor Bambauer argues that censorship has become so ubiquitous—whether over pornography, hate speech, copyright infringement, religious content, or political content—that "the contest is no longer about whether censorship is legitimate, but under what conditions."[554] Regardless of how one feels about what, if anything, ought to be censored, Bambauer makes a convincing descriptive argument that differing values regarding freedom of expression are leading to an increasingly fragmented internet.[555] However, Bambauer's focus appears to be more on what *governments* do, such as asking whether the "country admit[s] to filtering the Internet."[556]

---

[552] *Regulatory Reform Act: Hearing on H.R. 2327 Before the H. App. Comm., Before the Subcomm. on Admin. Law and Governmental Regulations of the H. Comm. on the Judiciary*, 98th Cong. 312 (1983) (statement of Rep. John Dingell); *see also* Bambauer, *Cybersieves*, *supra* note 39, at 386 (noting that some scholars resolve normative issues by turning to processes); Nathenson, *Civil Procedures*, *supra* note 86, at 913 (quoting Dingell).

[553] *See, e.g.*, Stephen A. Siegel, *The Origin of the Compelling State Interest Test and Strict Scrutiny*, 48 AM. J. LEGAL HIST. 355, 360 (2006) ("Shifting the burden of proof is an expression of strict scrutiny's assumption that in certain situations the judiciary should not accord the normal presumption of constitutionality to government action.").

[554] Bambauer, *Censorship v.3.1*, *supra* note 150, at 27-28.

[555] Bambauer, *Cybersieves*, *supra* note 39, at 379.

[556] *Id.* at 390; *see also* Bambauer, *Censorship v.3.1*, *supra* note 150, at 28. Examples include governments using unrelated laws as a pretext, paying for filtered access, or convincing intermediaries to restrict content. Bambauer, *Orwell*, *supra* note 39, at 867. Bambauer concludes that "soft censorship" by governments is "less legitimate than hard censorship" enforced directly by governments due to a

Although he is right that *states* ought to admit when they censor the internet,[557] this article looks at content removal and filtering by focusing primarily on the activities of *intermediaries*, regardless of whether the censorship is done at the behest of governments, private actors, or the intermediaries themselves.[558]

Thus, speech/religion clashes such as *Innocence of Muslims* might be better addressed, not through a code-based delineation of human rights values, but rather through a transparent and participatory process that puts much more information out in the open, and in context, permitting greater consistency in application and providing greater accountability.[559] As Google chair Eric Schmidt states in his book with Jared Cohen, the vulnerabilities of users to intermediaries misusing their data "will mandate that technology companies work even harder to earn the trust of their users."[560] Indeed, current events underscore the need for intermediaries to operate in a more transparent manner. Considering the public anger arising from the alleged cooperation of large internet companies with the National Security Agency, Super-Intermediaries have their work cut out for them.[561]

Other authors have considered the role of process and internet

---

lack of procedural protections such as openness and transparency. *Id.* at 867-68.

[557] *See* Bambauer, *Cybersieves*, *supra* note 39, at 393.

[558] *Cf.* Citron & Norton, *supra* note 8, at 1438-39 (noting "potential role" of intermediaries "in voluntarily addressing cyber hate").

[559] *Cf.* MUELLER, *supra* note 37, at 79 (noting the difficulties faced in internet governance by WIPO, which "had little capacity to take into account the different and sometimes competing norms and interests [such as] the impact of intellectual property rules on privacy, development, or freedom of expression").

[560] SCHMIDT & COHEN, *supra* note 19, at 33.

[561] *See, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (discussing involvement of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple in NSA PRISM program); Glenn Greenwald, *How Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN (July 11, 2013), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (discussing Microsoft helping the NSA to circumvent encryption used for Outlook.com).

intermediaries. Professor Bambauer offers a "process-based method" to measure the legitimacy of efforts used by different governments to limit online materials.[562] Bambauer's process framework looks to openness, transparency, narrowness, and accountability: "Censorship is more likely to be legitimate when a government *openly admits* it blocks access to material, *describes clearly* what content it filters, targets prohibited information *precisely*, and arrives at decisions through *accountable* mechanisms of governance."[563]

Similarly, I have also considered the role of procedural justice in the context of private enforcement of copyright.[564] A previous article of mine suggested that even outside of court, procedural justice plays a critical role in ensuring that copyright owners do not overreach their substantive rights when enforcing intellectual property rights, such as through cease-and-desist letters, DMCA takedown notices, or through automated enforcement.[565] Accordingly, this article reiterates and adapts my normative framework for private due process—what I now refer to as Digital Due Process—as a framework that looks to principles of *accuracy*, *participation*, and *transparency*, as shown below.[566]

---

[562] Bambauer, *Cybersieves*, *supra* note 39, at 379.

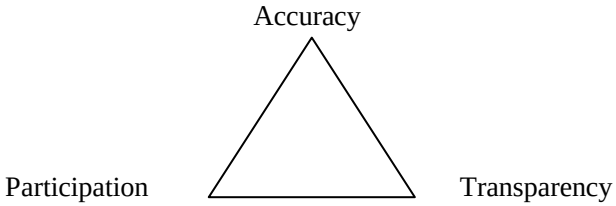
[563] Bambauer, *Orwell*, *supra* note 39, at 873 (emphasis added); *see also* Bambauer, *Cybersieves*, *supra* note 39. It would appear that Bambauer's first and second process principles are not so easily separable. For a government to *admit* to censorship (first principle) begs the question of *describing* what is being filtered (second principle). Regardless, his writings ably underscore the need for scholars to devote greater attention to the importance of procedure. *See* Nathenson, *Civil Procedures*, *supra* note 86, at 914 (noting need for more scholarship addressing the procedures used to filter speech).

[564] *See* Nathenson, *Civil Procedures*, *supra* note 86; *see generally* Lawrence B. Solum, *Procedural Justice*, 78 S. CAL. L. REV. 181 (2004).

[565] *See* Nathenson, *Civil Procedures*, *supra* note 86, at 945-56.

[566] *See id.* at 947-56.

Figure 1: Super-Intermediaries and Digital Due Process



It should be noted that no principle is primary; instead, the presence or lack of each can feed back on the others, either boosting or reducing the overall level of Digital Due Process.[567] For example, a lack of intermediary *transparency* regarding what is taken down may tend to reduce the extent of public *participation* in criticizing such decisions. In turn, a lack of public criticism and commentary may cause the intermediary to become lax, reducing the *accuracy* of future removal decisions when considered against the backdrop of either law or the intermediary's own community guidelines. Thus, the principles of Digital Due Process act as *correlatives*, "intertwined principles that can easily reinforce or undermine one another."[568]

2. The Guiding-Process Principles of Digital Due Process

In the subsections below, the principles of Digital Due Process are further explored in the context of the Super-Intermediaries discussed in this article. The discussion is at a more detailed level than mere statements of "accuracy, transparency, and participation." However, even a set of detailed guidelines would not provide meaningful guidance for every type of intermediary in every type of situation.[569] Anything too detailed is likely to be a poor fit for intermedi-

[567] *See id.* at 948.

[568] *See id.*

[569] *See* MACKINNON, *supra* note 14, at 174 (noting that "one-size-fits-all" approaches such as the abortive "Global Online Freedom Act" are likely to be impossible).

aries that offer varied services, or serve different constituencies.[570] Too much detail might similarly fail to anticipate future developments in expression and technology, or even worse, reduce flexibility and lead to the "over-bureaucratization" of oversight.[571] Thus, these principles are not intended to be enacted into positive law. Instead, they are intended to provide guidance. Such guidance may eventually lead to Best Practices, industry standards, and eventually perhaps even to law.[572]

It should be noted, however, that the *specifics* of the principles as discussed below are written in mind of the *type* and *power* of the intermediaries discussed in this article: regarding the type, those hosting user content or providing search tools to find such content, and regarding the power, Super-Intermediaries. Although the general principles of accuracy, participation, and transparency should be heeded by any type of actor or intermediary that touches on freedom of expression, privacy, or other human rights, the specifics of the principles discussed below are crafted for the intermediaries discussed herein.[573] Finally, it should be noted that although this article concludes that Super-Intermediaries ought to pay especial heed to the

---

[570] *See* Bambauer, *Middlemen*, *supra* note 29, at 3 ("Legal scholars have not yet concentrated with sufficient attention on the extraordinary range and diversity of functions that intermediaries play.").

[571] *Cf.* Wiessner, *supra* note 18, at 310 (noting such concerns regarding NGOs).

[572] *See* Mueller et al., *supra* note 133, at 242 (looking to regime theory and international institutions, and concluding that principles are foundational, leading to norms, and then "agreement on rules and decisionmaking procedures") (citing Steven D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES (Steven D. Krasner ed., 1983)).

[573] There are myriad other actors that impact what can be found on the internet: providers of payment services such as credit-card companies; manufacturers of equipment used by other actors, such as routers and packet-switching equipment; governmental actors that install hardware or software at key points in the network; and creators of applications, operating systems, and protocols used by others. Considering accuracy, participation, and transparency may be important when examining each actor; however, how one might balance such principles, and the specifics of implementation will surely vary depending on the type of actor. Such matters provide an important area for future scholarly work.

guiding process principles, Digital Due Process is something that should be respected by any intermediary of any size.

a. Accuracy

In the context of legal proceedings, "accuracy" can refer to the finding of facts, the articulation of legal principles, and the application of facts to those principles. Consistency in law and its application helps to foster the legitimacy of a system of justice. Similarly, it is important for intermediaries, and particularly Super-Intermediaries, to strive for accuracy. For example, Rebecca MacKinnon states that Facebook's "hate and harassment" team "play[s] the roles of lawmakers, judge, jury, and police all at the same time."[574] She also notes that Facebook's governance system had not been "enforced consistently or uniformly."[575]

Rather than focus on any one intermediary, the discussion below will speak in general terms. First, intermediaries should try to make their content guidelines as clear as possible, to provide guidance to subscribers, users, and to the intermediary's own screeners. Specific examples of what is permissible or barred are particularly helpful. Second, where guidelines cannot be stated clearly, intermediaries should be forthright about the "squishiness" of such guidelines, still providing examples of the easier cases of prohibited content. Third, if a guideline is subject to considerable intermediary discretion, then the guidelines should so state. Fourth, intermediaries should take care that employees who screen or remove content are properly trained in order to foster consistent results, to reduce bias, to minimize capriciousness, and to ensure that screeners have respect and empathy for cultures and values that they may not personally share. In other words, when human intermediary screeners exercise discretion, they should not *abuse* their discretion. Likely, many of these four things are done by many intermediaries, although such

---

[574] MACKINNON, *supra* note 14, at 154.

[575] *Id.* at 155. She further notes that it was not until 2011 that Facebook created an "easy-to-use appeals process" for persons whose accounts had been deactivated. *Id.* at 159.

information does not appear to be widely available.[576]

Finally, "hard" cases may require additional layers of review. For example, some speech is likely considered to be universally offensive and legally impermissible.[577] Speech geared towards fraud might be an example of an "easy" removal case once the fraud is noticed. If a screener positively identifies online material as being attempted fraud, the removal decision is not particularly difficult. But other speech, such as defamation of religion as exemplified by *Innocence of Muslims*, presents a much harder removal case. Such speech might be considered to be generally offensive by the public, but still legally permissible in many regions of the world. This is an example of a hard speech case, one that requires especial care from the intermediary, perhaps requiring additional layers of internal review, and perhaps even external input.

b. Transparency

Many authors call for intermediaries to provide greater transparency.[578] For example, Professor Julie Cohen discusses "operational transparency," encompassing transparency about the: 1) "design and implementation of surveillance practices"; 2) "operation of the network's borders and flows"; and 3) "processes by which net-

---

[576] For a promising example, YouTube's Community Guidelines page tries to give at least some level of detail. *See* YouTube, *Community Guidelines*, *supra* note 439. For example, regarding the prohibition on shocking and disgusting content, YouTube states "including a clip from a slaughter house in a video on factory farming may be appropriate. However, stringing together unrelated and gruesome clips of animals being slaughtered in a video may be considered gratuitous if its purpose is to shock rather than illustrate." *Id.* However, YouTube's guidance regarding hate speech is much more vague. *See supra* text accompanying note 441 (discussing "fine line"). Detailed discussion of what YouTube and others do is beyond the scope of the present project. Regardless, the more intermediaries can provide guidance, the more notice the public will have.

[577] Again, thanks to Professor John Makdisi for making the observations that prompted the analysis above. *See supra* note 40.

[578] *See, e.g.*, Citron & Norton, *supra* note 8, at 1441; Pasquale, *supra* note 17, at 161-62 (calling for qualified transparency).

work standards are designed and adopted."[579] Rebecca MacKinnon suggests boosting corporate transparency, building an information environment that is more citizen-centric and citizen-driven, and building processes to engage with users, customers, and other stakeholders.[580] Additionally, Professor Molly Land points to ICCPR Article 19(2) as a basis for requiring intermediaries to provide heightened transparency and accountability, including a reference to a phrase of interest to this article, "digital due process standards."[581] In short, it is time to accept the fact that some Super-Intermediaries may have power that in some respects is quasi-governmental in nature.[582] This power encourages governments and others to enlist intermediaries "to act indirectly on their behalf," thus avoiding governmental accountability.[583]

Although this article raises a number of concerns regarding using international human rights law, Professor Land's point is well taken. Moreover, she makes valuable points regarding *why* technology companies are likely to participate in efforts to enhance online freedom: 1) many are deeply committed to online freedom; 2) many may welcome normative guidance; 3) the benefits of "political 'cover'"; and 4) public image.[584] She makes a strong case for considering how human rights can be better serviced through code and practices, but leaves full consideration of "human rights defaults" for later consideration by herself and others.[585] Perhaps this article serves as one response.

Notably, among the ongoing efforts to develop principles for internet governance, the Internet Rights & Principles Coalition is

---

[579] COHEN, *supra* note 406, at 235.

[580] MACKINNON, *supra* note 14, at 244-48.

[581] Land, *Law of Internet*, supra note 26, at 448.

[582] For instance, intermediaries make decisions regarding whether to remove speech, essentially limiting the need for legal process in most cases. Similarly, intermediaries can filter speech even before it comes online, essentially creating extra-judicial prior restraints.

[583] Bambauer, *Censorship v.3.1*, *supra* note 150, at 31.

[584] Land, *Law of Internet*, supra note 26, at 452-54.

[585] *Id.* at 456.

drafting a Charter of Human Rights and Principles for the Internet.[586] A summary of "ten core principles" includes matters such as universality and equality, rights and social justice, accessibility, expression and association, network equality (including freedom from filtering), and more.[587] Of additional interest is the governance provision, which states that the internet should be governed against a foundation of human rights and social justice, which should happen in "a *transparent* and multilateral manner, based on principles of *openness*, inclusive *participation* and *accountability*."[588]

So how might Super-Intermediaries better foster transparency in their operations regarding content? The subsections below consider aspects of intermediary transparency, specifically, the topics for which transparency ought to be provided, the form and context of transparency information, and the problem of governmental secrecy, which can frustrate intermediary efforts at providing transparency.

i. Subject Matter of Transparency

This subsection addresses the types of information that ought to be provided, whereas the subsection following considers the form that such information might take. As a preliminary comment, I do not mean to suggest that every bit of information below must always be provided. Although the details of what should be publicized may vary, one guideline may be in favor of a presumption of transparency, with heightened levels of transparency in cases where the speech is not considered to be universally offensive and impermissible. In other words, the "harder" the case, the likelier the need for heightened transparency. Easier cases may merit lesser transparency when the burdens of transparency substantially outweigh the benefits.

---

[586] *See* Internet Rights & Principles Coalition, *The IRP Charter Website*, http://internetrightsandprinciples.org/wpcharter/ (last visited Aug. 26, 2013); *see also* MACKINNON, *supra* note 14, at 240 (discussing the Charter and the core principles).

[587] *See* Internet Rights & Principles Coalition, *10 Internet Rights and Principles*, http://internetrightsandprinciples.org/images/IRPflyer.pdf (last visited Aug. 26, 2013).

[588] *Id.* (emphasis added).

What should be disclosed? First, as stated in the prior subsection, intermediaries should be as clear as possible about their *content guidelines*. Thus, Professors Citron and Norton note that although intermediaries expend significant resources addressing complaints of abuse, their practices remain unclear.[589] They therefore suggest a commitment to transparency that would include explaining the *grounds* of certain decisions, providing *definitions* of banned speech, and giving *examples* of the harms forestalled by removal.[590]

Second, intermediaries should also be as clear as possible about *removal and reinstatement procedures*. Such guidelines are of particular importance to users whose content is removed, because such stakeholders typically lack the resources of copyright owners and governmental actors who may demand content removal.

Third and crucially, intermediaries should *publicize demands* for removal, blockage, and the like. They should clearly and publicly catalogue requests and name the requesting party.[591] Additionally, copies of demands should generally be provided. Further, such information should generally be made available *regardless* of whether the intermediary complies with any such demand.[592] Providing such information may be crucial to induce shaming and accountability, and to encourage future restraint by such actors.

Fourth, intermediaries should *reveal any action taken* in response to a demand. Even when hosted user content is removed for good cause, it is important to publicly acknowledge the deletion.[593]

---

[589] Citron & Norton, *supra* note 8, at 1477.

[590] *Id.*

[591] When a YouTube video is blocked by Content ID or taken down due to a cease-and-desist demand, YouTube displays a notice on the video's former page saying who initiated the removal. *See, e.g.*, Alex Pasternack, *NASA's Mars Rover Crashed Into a DMCA Takedown*, http://motherboard.vice.com/blog/nasa-s-mars-rover-crashed-into-a-dmca-takedown, MOTHERBOARD (last visited Sept. 29, 2013) (showing image of notice on YouTube).

[592] Such information ought to include public information on Content ID rules, such as when a company has claimed that its copyrights permit it to block, track, or monetize a particular video.

[593] Citron & Norton, *supra* note 8, at 1471. For copyright claims, YouTube will name the requesting party, but does not appear to provide detailed information

Thus, whether faced with a governmental or private demand, providers should generally publish the content of the demand, the outcome—i.e., any action taken or not taken in response—as well as an explanation appropriate to the type of content and context.[594] Moreover, intermediaries also ought to err in favor of publicizing *internal* decisions taken that affect speech or access, regardless of whether those decisions were made unilaterally by the intermediary, in response to external pressures, or as a result of explicit negotiations with governmental or private parties. Such transparency is essential because an ISP might make a speech-related removal or blockage decision after negotiations with the government; in such cases the intermediary's action might have been taken "if not in the shadow of the law, then in the threat of such shadow."[595]

Fifth, intermediaries ought to provide relevant information about *other actors*, so that stakeholders understand what is likely to be blocked or filtered. Thus, as Google currently does, intermediaries ought to provide information regarding known third-party interferences with content.[596] Examples might be a video intermediary deciding to publicize information regarding *other* ISPs that throttle or filter the video site's content. Other examples would include identifying governmental activity in blocking the video site's content through techniques such as IP address filtering, domain-name filtering, filtering of specific URLs, or the use of deep packet inspection to block content. Although the intermediary may be unable to prevent such interference with its content, the act of making such information public may shed light and help to end or limit such conduct. Super-Intermediaries should commit themselves to fostering meaningful transparency that promotes accountability and public debate.

---

on the video's page on the specifics. Regarding removals under its Community Guidelines, it would appear that YouTube merely says "This video has been removed because its content violated YouTube's Terms of Service." An example of such a video can be found at http://www.youtube.com/watch?v=cGYbl5aqsYA.

[594] Citron & Norton, *supra* note 8, at 1477 (noting importance of releasing grounds of decisions).

[595] Bambauer, *Orwell*, *supra* note 39, at 896.

[596] *See* Google, *Transparency Report: Current Disruptions of Traffic to Google Products and Services*, http://www.google.com/transparencyreport/traffic/#expand=SD (last visited Sept. 29, 2013).

ii. Form and Context of Transparency

The next matter is to consider the forms that public intermediary transparency can take, as well as the contexts in which it is provided. For example, it should be noted that internet intermediaries have the unique opportunity to use *code* as a way of integrating transparency directly into their services. Indeed, Professor Edward Felten notes that software can be transparent, "making code, issue tracking, and design discussions public," regardless of whether the code is open-source or not.[597]

Thus, transparency can be, and often is, an integral part of an intermediary's interface. First, intermediaries can provide *notices or "block" pages*. For example, when Google censors results from its search engine, it "usually places some sort of explanation in the search results to explain and justify the policy."[598] Similarly, when content is removed from YouTube, the site still shows a page, generally indicating that content was taken down or blocked.[599] Block pages inform the public that information was blocked or disabled. Ideally, block pages should provide—in the context of the page where the information was once found—an explanation of the reasoning for the removal, the identity of the party seeking removal, and links to any demand or request for removal.[600]

Second, intermediaries should create or use *repositories of demands*. Currently, the *Chilling Effects Clearinghouse* operates a repository of cease-and-desist letters, takedown notices, and other materials.[601] Although some intermediaries (such as Google and

---

[597] Ed Felten, *Software Transparency*, FREEDOM TO TINKER (Sept. 16, 2013), https://freedom-to-tinker.com/blog/felten/software-transparency/.

[598] VAIDHYANATHAN, *supra* note 5, at 15 (noting Google engaging in rare self-censorship where search results "are troublesome or politically controversial" or reflect a website trying to rig the system).

[599] *See supra* note 591 (noting that YouTube discloses source of removal and blockage requests).

[600] Bambauer, *Orwell*, *supra* note 39, at 934. Google and Twitter forward copies of demands to *Chilling Effects.* Additionally, Google's Transparency Report provides links to takedown notices hosted on *Chilling Effects*.

[601] *See* Chilling Effects Clearinghouse, *supra* note 90.

Twitter) transmit demands to *Chilling Effects*, transparency would be fostered if all Super-Intermediaries shared demands with *Chilling Effects*. Alternatively, the Global Network Initiative might be enlisted to provide a central repository. In either case, it would be helpful if intermediaries would collaborate on industry standards for the immediate and public posting of removal requests.

Third, demands should generally be publicized *even when materials are not removed*. For example, if materials are available in one country but not another, then that information should be included on the live page or block page.[602] Additionally, if content is tracked or monetized as it can be under a program like Content ID, then such information ought to be publicly acknowledged on the video's page.

Fourth, intermediaries should continue providing and enhancing their *transparency reports*. As of this writing, a number of Super-Intermediaries provide transparency reports, including Google, Facebook, Microsoft, Twitter, and Yahoo.[603] Super-Intermediaries that do not currently provide such reports should do so.[604] Google in particular should be commended for the serious effort it puts into its transparency report. Not only does it provide information on requests to take down content from governments and copyright owners, but it also provides information on user data requests, and information on disruptions to its products and services.[605] Interested parties can also download spreadsheets of the underlying data.

Intermediaries should follow Google's lead in providing detailed transparency reports; further, all intermediaries should innovate to find ways to make their transparency reports better and more useful. A block page might include a link that directs a user back to

---

[602] If YouTube content is *blocked* in one country, YouTube appears to acknowledge this on the block page. However, assuming that this information is not provided in countries where the video is *not blocked* (which appears to be the case with *Innocence of Muslims*), this article would suggest that blockage information should be indicated anyway. Thus, for videos that are not available everywhere, the general public ought to be informed as to where it is blocked and why.

[603] *See supra* sources collected in note 426.

[604] It should also be noted that the recommendations in this article may apply to smaller intermediaries as well.

[605] Google, *Google Transparency Report*, *supra* note 426.

further details in an online transparency report, as well as a link to a takedown notice.[606] Also, intermediary code should be crafted to provide ongoing transparency updates. Rather than providing periodic updates, it would be more helpful for all Super-Intermediary Transparency Reports to be updated automatically.[607] Thus, this article envisions an intertwining scheme of transparency, one that places information in context, and which becomes an integral part of a Super-Intermediary's architecture. Transparency reports might eventually transform into continually updated databases, better serving the goals of transparency while disputes are live, rather than months later when matters may have been resolved.

iii. The Problem of Governmental Secrecy

Finally, we must remember that intermediaries are not the only relevant actors. Governmental actors need to be more transparent as well and provide central indexes of governmental demands for content removal. Unfortunately, sometimes laws or governmental orders, such as national security orders under the Foreign Intelligence Surveillance Act (FISA) or via National Security Letters, may prohibit intermediaries from releasing details on governmental demands.[608] Even when the U.S. government grudgingly permitted intermediaries to release information on national security requests, the information was in the aggregate, lacked detail, and was lumped

---

[606] Admirably, Google's Transparency Report provides *Chilling Effects* links for individual copyright takedown notices. All intermediaries should follow Google's lead and continue innovating, such as by including such links directly on the affected page so that greater takedown information is provided in context.

[607] Google provides daily updates of copyright removal requests. *See* Fred Von Lohmann, *More Data about Copyright Removals in Transparency Report*, GOOGLE POLICY BY THE NUMBERS (Dec. 11. 2012), http://policybythenumbers.blogspot.com/2012/12/more-data-about-copyright-removals-in.html.

[608] *See* Brad Smith, Gen'l Counsel & Exec. V.P., Legal & Corp. Affairs, *Standing Together For Greater Transparency*, MICROSOFT ON THE ISSUES (Aug. 30, 2013), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx (noting that Google and Microsoft sued the U.S. government in June 2013 for the right to publish more information on FISA orders).

together with other information, such as criminal matters.[609] Google objected, stating that "[l]umping the two categories together would be a step back for users," and requested the ability to publish national security requests separately.[610] Legal constraints such as these reduce the public's trust in the government, in intermediaries, and frustrate the goals of Digital Due Process.

c. Participation

The third guiding process principle underlying Digital Due Process is participation. This principle considers *who* might be a relevant stakeholder and *how* they might participate.

i. Stakeholder Participants

Participants may include a myriad of stakeholders. The first category might be stakeholders who are interested in *maintenance or removal* of content. Subscribers of intermediaries who post content have an obvious interest in preventing removal of their content. Also relevant are the users who seek to access that content. Governmental actors also have a stake in any intermediary process, as do private parties who seek removal of content, such as copyright infringement.

---

[609] *See, e.g.*, Apple, *Apple's Commitment to Customer Privacy* (June 16, 2013), https://www.apple.com/apples-commitment-to-customer-privacy (reporting 4,000-5,000 requests in six-month period); Ted Ullyot, Facebook General Counsel, *Facebook Releases Data, Including All National Security Requests* (June 14, 2013), http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests (reporting 9,000-10,000 requests in six-month period); Marissa Mayer, CEO, & Ron Bell, General Counsel, *Our Commitment to Our Users' Privacy* (June 17, 2013), http://yahoo.tumblr.com/post/53243441454/our-commitment-to-our-users-privacy (reporting 12,000-13,000 requests in six-month period).

[610] Google, Posting to Google+ (June 15, 2013), https://plus.google.com/+google/posts/huN19gnPq5n; *see also* Claire Cain Miller, *Google Calls U.S. Data Request Disclosures a Step Backward for Users*, N.Y. TIMES BITS BLOG (June 15, 2013), http://bits.blogs.nytimes.com/2013/06/15/google-calls-u-s-data-request-disclosures-a-step-backward-for-users/.

A more diffuse interest may be represented by members of the public: a significant example of a diffuse but powerful stakeholder group would be citizens of Islamic nations who felt outraged over *Innocence of Muslims*. Even though the disputed content did not violate a "Western" proprietary right, one cannot doubt that many Muslims felt strongly about the matter.

A second category of stakeholders are those directly or indirectly involved in an *intermediary's decision-making process*. Examples include human decision-makers at an intermediary who screen content, persons in an intermediary's legal department, and the officers and directors of such companies. Speaking more broadly, stakeholders also include other intermediaries; indeed, the existence of the Global Network Initiative provides a stellar example of the fact that powerful intermediaries are becoming increasingly interested in having a voice in decisions made by other intermediaries.

ii. Nature and Quality of Participation

The nature and quality of stakeholder participation is also critical to maximizing Digital Due Process. The more participation, the more incentive intermediaries have to satisfy their users, and the less tempted governments and private actors may be to overreach. First, stakeholders might participate in removal/blockage decisions by formal *legal process*, although this appears to be relatively rare.[611]

More commonly used is a second mechanism, namely, *private adjudication processes* such as demand letters, DMCA takedown notices, and automated filtering.[612] For present purposes, it suffices to note that such private adjudication procedures tend to suffer from a number of procedural defects that tempt rights-holders

---

[611] *Compare* Table 2 (listing relatively small number of U.S. federal lawsuits), *with* Part IV.B.1.b.ii (detailing the number of private demands sent to intermediaries).

[612] *See supra* Part IV.B.1.b.ii (regarding cease-and-desist and takedowns); *see also* text accompanying notes 484-87 (regarding automated filtering).

to make overblown and even frivolous demands for removal.[613] As a result, it is crucial for intermediaries to maximize transparency in order to inform the public and to deter overreaching. Intermediaries should also make it as easy as possible for users to challenge such removal requests.

A third example of stakeholder participation is the use of *flagging systems*, which permit users to click on a button or link to notify an intermediary that content is potentially objectionable. Typically, flags lead to further internal review, and ultimately, to possible content removal.[614] Needless to say, one flag should rarely, and perhaps never, cause immediate removal. Moreover, when the flag identifies content that falls under a "hard" case of speech, it becomes all the more important that the matter is reviewed by a properly trained human, rather than relying solely on code.

Fourth and finally, intermediaries should err on the side of leaving breathing room for *circumvention* of blockage, at least in "hard" cases of speech, such as *Innocence of Muslims*. This is important because for these hard cases, there is nothing close to universal agreement on whether the materials are socially offensive or legally impermissible. Even in an Islamic country, there may be people who want to view such materials. There are a number of methods by which users could circumvent blockage. For example, if material is available on the dot-com version of a video site, but not on the Turkish site, the user could simply choose to visit the dot-com site. Unfortunately, at least some intermediaries use IP address geolocation to prevent this simple form of circumvention.[615] Another common method of circumvention is the use of proxy servers, which may defeat local blockage.[616] In fact, authors Schmidt and

---

[613] *See generally* Nathenson, *Civil Procedures*, *supra* note 86, at 922-45 (discussing, *inter alia*, problems caused by such enforcement techniques).

[614] *See supra* text accompanying notes 479-83 (discussing flags).

[615] *See supra* Part IV.B.2.b (explaining geolocation).

[616] *See* SCHMIDT & COHEN, *supra* note 19, at 84; Burnett, *supra* note 465, at 471-72 (explaining proxy servers). Schmidt and Cohen also note steps that companies took to help Egyptian activists, such as providing dial-up connections, as well as Google's tweet-by-phone service. *See* SCHMIDT & COHEN, *supra* note 19, at 140.

Cohen suggest that a balkanized internet may eventually create the need for "virtual asylum" where countries could create proxy and circumvention tools to permit dissidents to connect to the outside world.[617]

How should intermediaries deal with attempts to obtain content that is locally unavailable, such as *Innocence of Muslims*? One method an intermediary might use is providing circumvention tools on its site. As a practical matter, Super-Intermediaries may not wish to do this, because they may operate in countries where the content is banned. Another method might be for the intermediary to avoid taking steps to defeat common forms of circumvention such as when a proxy server is used to access content that is lawful in many parts of the world. Yet another intermediary response might be to take affirmative steps to defeat attempts at circumvention. Sometimes this step is entirely appropriate. Circumvention is not an all-purpose panacea: although circumvention may be lauded when it is used to bypass expression blocked by a repressive regime, it "cuts both ways" and can be used to do harm, such as by permitting the distribution of child pornography, malware, or viruses.[618] But when the content being sought is not widely condemned, intermediaries may need to leave breathing space for users in blocked areas to bypass such blockage.

3. Countervailing Concerns

The Digital Due Process framework discussed above must be considered in light of countervailing concerns, some more serious than others.

---

[617] *See* Eric Schmidt & Jared Cohen, *Web Censorship: The Net is Closing In*, THE GUARDIAN (Apr. 23, 2013), http://www.theguardian.com/technology/2013/apr/23/web-censorship-net-closing-in.

[618] Bambauer, *Cybersieves*, *supra* note 39, at 442.

a. Why Focus on Process?

Professor Milton Mueller rejects focusing solely on process because a reliance on process assumes that censorship can be done "fairly and appropriately," and that a process framework "legitimizes and encourages Internet censorship."[619] Discussing the work of Professor Bambauer, he argues that countries will censor openly, transparently, narrowly, and in an appropriately limited way *only* if such countries *first* respect the rights of individuals.[620] Mueller argues with some force that process alone is no guarantee of good results, and that if we assume that "citizens have a right to be *informed*" about governmental blocking of information, "then perhaps it is not too crazy to ask whether they also have a right to *get* that information without interference."[621]

Yet in making this argument, Mueller appears to concede crucial ground. For one thing, he cites in support of his position Article 19 of the UDHR, the First Amendment, and Article 10 of the European Convention.[622] But as previously discussed in this article, the International Bill of Human Rights embraces restrictions on speech, such as those contained in ICCPR Articles 19(3) and 20(2).[623] Moreover, the "First Amendment is not absolute."[624] Even Article 10 of the European Convention acknowledges the possibili-

---

[619] MUELLER, *supra* note 37, at 207.

[620] *Id.* at 208 (discussing Bambauer, *Cybersieves*, *supra* note 39). Notably, this article focuses not on governmental action, but rather on powerful internet intermediaries who tend to have international presences and therefore possess international, and oftentimes global concerns. Indeed, as Mueller acknowledges, content regulation of a global internet has led to private actors taking primary responsibility for monitoring speech and enforcing restrictions. *See id.* at 189.

[621] *Id.* at 208.

[622] *Id.* at 209. Along similar lines, Professor Molly Land argues that Article 19 "explicitly protects the technologies of connection and access to information." Land, *Law of Internet*, supra note 26, at 394.

[623] *See supra* Part III.B.

[624] *See* Brett M. Frischmann, *Speech, Spillovers, and the First Amendment*, 2008 U. CHI. LEGAL F. 301, 304 (2008); *see also* Pati, *supra* note 288, at 232 (noting "case-by-case jurisprudence that strikes a balance between individual rights and interests of the community").

ties of restrictions of expression.[625]

More fundamentally, he admits that there "is still a role for illegal content regulation," conceding that states can create "clear, explicit guidelines for what constitutes illegal content *in their territory*," including processes requiring companies to "take down such content *when it resides in their own jurisdiction.*"[626] Therein lies the rub: once one accepts the proposition that content may be socially and legally permissible in one area but not in another, internet balkanization appears to be the inevitable result. Once one concedes that different forms of internet censorship will occur in different parts of the world—a descriptive point made with equal force by Bambauer—one has effectively admitted that it is impossible to generate truly global norms for the substance of expression. It would appear to necessarily follow that where international agreement cannot be generated on substance, one must focus even more carefully on the *processes* by which such content decisions are made.

b. Transparency is Not a Panacea

Another potential objection is that the kinds of transparency discussed above would not foster Digital Due Process, but might frustrate it. Indeed, information overload is as likely to frustrate freedom as a lack of information.[627] Bald transparency is not a panacea, just as a pile of books do not constitute a library. However, this article argues for transparency that is provided in *context* and as an *integral* part of an intermediary's services.[628] Moreover, it is not necessary to provide full information on all types of blockage or removal actions. Factors for an intermediary to consider might include the extent to which the removed content is considered to be universally inappropriate. Thus, for content considered to be univer-

---

[625] *See supra* note 291.

[626] MUELLER, *supra* note 37, at 209 (emphasis added).

[627] Seventy-two hours of video are uploaded to YouTube every minute. YouTube, *Statistics*, http://www.youtube.com/yt/press/statistics.html (last visited July 14, 2013).

[628] *See supra* Part V.E.2.b.ii (regarding form and context of transparency).

sally offensive to social groups, as well as universally unlawful, content might be taken down and minimal information left online, with perhaps nothing more than an aggregate reference in a transparency report. But for content that is of varied acceptability around the globe—such as *Innocence of Muslims*—more information should be provided. For instance, it would be helpful for the video's page to provide a listing of the countries where it is blocked as well as information on official demands. Moreover, such information should be viewable in countries where the disputed content is available, as well as in countries where it is blocked.

c. Some Information Should Not Be Disclosed

An additional objection—and a powerful one—is that some information should not be disclosed. For example, an intermediary might not want to disclose information that might expose its trade secrets, such as certain internal operating procedures or its source code. Another objection might be that transparency might subject innocent third persons to embarrassment or harassment as a result of having their names dragged into a content dispute. Yet another might be that by providing information on blocked content for purposes of transparency, the intermediary might be defeating the purpose of blocking that content.

These are serious concerns. When legitimate issues arise regarding an intermediary's business information, its users' information, or other concerns, a number of limiting principles should be considered. First, information can be *redacted* in a form that still fosters transparency. For example, names and phone numbers can be redacted from published versions of cease-and-desist letters, as is done now by *Chilling Effects*. Equally so, search engines that remove listings might fairly provide partially redacted information sufficient for the public to know what was removed and why, but not enough to "spill the beans" on the deleted listing.

Second, transparency may sometimes have to be "*qualified*," as discussed by Professor Frank Pasquale in an article on search

engine ranking algorithms.[629] He says: "In response to actual and potential abuses of that power, rules that would limit carriers' and intermediaries' ability to discriminate . . . are becoming increasingly necessary. . . . [H]owever, *such transparency should be qualified* in order to protect important intellectual property interests of intermediaries."[630] Pasquale therefore recommends "formation of an Internet Intermediary Regulatory Council . . . . [to] follow up on complaints made by competitors, the public, or when it determines that a practice deserves investigation."[631]

Pasquale's recommendations carry force in the present context as well.[632] Whether oversight is provided by a governmental entity, quasi-governmental entity, or group like the Global Network Initiative, it is crucial that there be some form oversight to address overblown claims of secrecy. Additional guidance may be provided by analogy to privilege logs. A privilege log is provided during discovery in litigation, when the producing party wishes to withhold information on the basis of privilege or work-product protection. Although a privilege log does not contain the withheld documents, it must nevertheless contain sufficient information to "describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim."[633] Thus, even when an intermediary redacts or withholds information on the basis of trade secret, user privacy, or other basis, the norm should be for the intermediary to provide sufficient information for the public and monitoring bodies to challenge that assertion.

---

[629] *See* Pasquale, *supra* note 17, at 162.

[630] *Id.* at 160-61.

[631] *Id.* at 168-69.

[632] Professor Julie Cohen argues that such qualified transparency should also apply to other technologies, such as rights-management systems. *See* COHEN, *supra* note 406, at 237.

[633] FED. R. CIV. P. 26(b)(5)(A)(ii).

d. Cost

A final and substantial objection to the framework proposed in this article is that Digital Due Process and its underlying transparency may cost intermediaries significant amounts of money and time. Considering that Super-Intermediaries are private businesses, their main goal is to make profit and not merely to benefit the public.[634] Yet such concerns may prove too much. First, at the risk of sounding naive, there are things in life more important than money. Super-Intermediaries, as bearers of "great power," need to own up to the responsibilities implied by that power. Second, once transparency algorithms are built into an intermediary's architecture, the task of updating transparency reports, block pages, and the like might become a routine and automatic part of normal dispute processing.

Third, Digital Due Process may turn out to be smart business. Investing time and money to create computer and realspace processes that comply with Digital Due Process may ultimately reap great benefits for Super-Intermediaries, by increasing user trust, and encouraging more people to use the intermediaries' software and services. The importance of this point cannot be understated: the NSA scandal has seriously shaken the public's trust in powerful intermediaries, so much that the scandal may slow the adoption of cloud computing services, and deter foreigners from using American-based intermediaries.[635] It is time for Digital Due Process.

---

[634] "In most contexts, transparency is helpful, but, at the same time, it can also be quite costly." MOROZOV, *supra* note 23, at 239; *see also* COHEN, *supra* note 406, at 223 ("Some information-policy problems cannot be solved simply by prescribing greater 'openness' or more 'neutrality.'"); Lessig, *Against Transparency*, *supra* note 341.

[635] *See* Kashmir Hill, *How The NSA Revelations Are Hurting Businesses*, FORBES (Sept. 10, 2013), http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses (noting that "the NSA revelations may cost information technology companies $180 billion by 2016").

Conclusion

The beginning of this article recited clichés from *Spider-Man* and Google, variants on the mantra that power implies responsibility. Returning to those quotes, I take them to be earnest but somewhat empty moral truisms. To demand responsibility is to beg the question of responsibility to *whom* and for *what*. Thus, it is disconcerting that Google Chair Eric Schmidt, when asked what Google's unofficial *Don't Be Evil* slogan meant, once replied that evil "is what [Google co-founder Sergey Brin] says is evil."[636] Such a response, coming from a major force at a Super-Intermediary, is disconcerting: a leader who chooses to be the sole arbiter of good and evil risks becoming a tyrant. Put more mildly, even the best-intentioned leaders, and the best-minded Super-Intermediaries who wish to "do no evil" may find themselves in positions where their actions are simultaneously hailed and decried. As Siva Vaidhyanathan notes, however, the reality is somewhat more banal: "Google is not evil, but neither is it morally good."[637] It is instead *disruptive*,[638] and the power of Google and other Super-Intermediaries is growing so quickly that it is imperative for scholars to address just which responsibilities such power might imply.

Rebecca MacKinnon further reminds us that the power of global internet self-publishing does not guarantee a utopia of peace and democracy: "Life in the rain forest is just as likely to be nasty, brutish and short."[639] In other words, it is not enough to have a network, nor is it enough to have Super-Intermediaries that serve as

---

[636] Josh McHugh, *Google vs. Evil*, WIRED (Jan. 2003), http://www.wired.com/wired/archive/11.01/google.html; *see also* DAVID A. VISE & MARK MALSEED, THE GOOGLE STORY 211 (2005). Another author argues that "'Don't be evil' points to a moral center without coordinates," and that "Google is failing to recognize its position in a constellation of power structures." Natasha Lennard, *The Dangerous Ethics Behind Google's Transparency Claims*, SALON (June 11, 2013), http://www.salon.com/2013/06/11/the_dangerous_ethics_behind_googles_transparency_claims/.

[637] VAIDHYANATHAN, *supra* note 5, at 4.

[638] *Id.* (stating that Google "fractures and disrupts almost every market or activity it enters—usually for the better, but sometimes for the worse").

[639] MACKINNON, *supra* note 14, at 224.

the key nodes through which we congregate. We need a digital civilization, or if we choose to balkanize, digital civilizations.[640] In either case, such civilizations need Digital Due Process.

What should be the values that inform a digital world run in large part by Super-Intermediaries? Due to internal tensions and international disagreement, human rights law may not provide case-by-case guidance to Super-Intermediaries. However, it may nonetheless provide valuable touchstones for public discourse on matters of great public concern and controversy. To enable that discussion, Super-Intermediaries must therefore provide integrated, contextual transparency, and meaningful public participation, thus placing into the light themselves *as well as* those seeking to censor online content. The would-be "superheroes" of the internet should remove their "masks" so that the public can reach its own conclusion.

[640] *Id.*