The University of Chicago
Law Review

Volume 79 Summer 2012 Number 3

ARTICLES

Orwell's Armchair

Derek E. Bambauer†

America has begun to censor the Internet. Defying conventional scholarly wisdom that Supreme Court precedent bars Internet censorship, federal and state governments are increasingly using indirect methods to engage in "soft" blocking of online material. This Article assesses these methods and makes a controversial claim: hard censorship, such as the PROTECT IP and Stop Online Piracy Acts, are normatively preferable to indirect restrictions. It introduces a taxonomy of five censorship strategies: direct control, deputizing intermediaries, payment, pretext, and persuasion. It next makes three core claims. First, only one strategy—deputizing intermediaries—is limited significantly by current law. Government retains considerable freedom of action to employ the other methods and has begun to do so. Second, the Article employs a process-based methodology to argue that indirect censorship strategies are less legitimate than direct regulation. Lastly, it proposes using specialized legislation if the United States decides to conduct Internet censorship and sets out key components that a statute must include to be legitimate, with

† Associate Professor of Law, University of Arizona James E. Rogers College of Law. The author thanks Faisal Alam, Jelena Kristic, Brad Reid, Chris Vidiksis, and Eugene Weber for expert research assistance. Thanks for helpful suggestions and discussion are owed to Marvin Ammori, Miriam Baer, Katherine Barnes, Scott Boone, Annemarie Bridy, Ellen Bublick, Robin Effron, Kirsten Engel, Tom Folsom, James Grimmelmann, Rob Heverly, Dan Hunter, Margo Kaplan, Rebecca Kysar, Brian Lee, Lyrissa Lidsky, Sarah Light, Tom Lin, Gregg Macey, Irina Manta, David Marcus, Toni Massaro, Milton Mueller, Thinh Nguyen, Mark Noferi, Liam O'Melinn, Jim Park, David Post, Christopher Robertson, Simone Sepe, William Sjostrom, Roy Spece, Nic Suzor, Alan Trammell, Greg Vetter, Brent White, Mary Wong, Jane Yakowitz Bambauer, Peter Yu, Jonathan Zittrain, the participants in the IP Scholars Roundtable at Drake University School of Law, the participants in a workshop at Florida State University College of Law, and the participants in a workshop at the University of Arizona James E. Rogers College of Law. The author gratefully acknowledges the Dean's Summer Research Stipend Program, Dean Michael Gerber, and President Joan G. Wexler at Brooklyn Law School for financial support. The author welcomes comments at derekbambauer@email.arizona.edu.

the goal of aligning censorship with prior restraint doctrine. It concludes by assessing how soft Internet censorship affects current scholarly debates over the state's role in shaping information online, sounding a skeptical note about government's potential to balance communication.

> [T]he supreme power then extends its arm over the whole community. It covers the surface of society with a network of small complicated rules, minute and uniform, through which the most original minds and the most energetic characters cannot penetrate, to rise above the crowd. The will of man is not shattered, but softened, bent, and guided; men are seldom forced by it to act, but they are constantly restrained from acting.
>
> Alexis de Tocqueville[1]

INTRODUCTION

William Walsh was shocked to learn that he was a child pornographer.

On February 11, 2011, the IT administrator's personal blog at greyghost.mooo.com—containing information about his hobbies, computer product preferences, and family—was replaced by a page showing logos from the Department of Justice and the Department of Homeland Security over text stating that "[a]dvertisement, distribution, transportation, receipt, and possession of child pornography constitute federal crimes."[2] The page stated that the government had seized Walsh's domain name under the civil forfeiture provision of the federal anti–child pornography statute.[3] According to the government, Walsh's site was involved in the sordid international trade in child sexual abuse images.

However, Walsh and his site were innocent. So were Kent Frazier,[4] Moon's Garage,[5] and Seppo Kiuru,[6] though their sites were also labeled as child pornography. Theirs were among the eighty-four thousand websites swept up in a law enforcement effort to interdict ten sites accused of distributing child pornography.[7] As part of Operation Protect Our Children, the Departments of Justice and Home-

---

1 Alexis de Tocqueville, 2 *Democracy in America* 319 (Knopf 1945) (Henry Reeve, trans).

2 Ernesto Van Der Sar, *U.S. Government Shuts Down 84,000 Websites, 'by Mistake'* (TorrentFreak Feb 16, 2011), online at http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216 (visited Sept 20, 2012). See William R. Walsh, *From the Blithering Idiots Department. . .* (Feb 12, 2011), online at http://stop-error.xanga.com/741136585/from-the-blithering-idiots-department (visited Sept 20, 2012); *May I Have a Moment of Your Time?* (Apr 17, 2012), online at http://greyghost.mooo.com (visited Sept 20, 2012).

3 18 USC § 2254.

4 Frazier's site, once located at http://kfrazier.mooo.com, was treated like Walsh's site.

5 See http://moon.mooo.com (visited Sept 20, 2012).

6 See http://www.kiuru.mooo.com (visited Sept 20, 2012).

7 See Thomas Claburn, *ICE Confirms Inadvertent Web Site Seizures* (InformationWeek Feb 18, 2011), online at http://www.informationweek.com/news/security/vulnerabilities/229218959 (visited Sept 20, 2012).

land Security took control over ten domain names believed to host child pornography.[8] One of those domain names, mooo.com, was used by a service provider named FreeDNS to offer domain name hosting at no charge.[9] Thus, Walsh could have the FreeDNS service resolve requests for his site's domain name, greyghost.mooo.com, to his computer's IP address. Over eighty-four thousand other sites used FreeDNS for the same purpose.[10] All were labeled as child pornography when the government seized the top-level domain name mooo.com rather than targeting the specific subdomains believed to host illicit content.

Facing a storm of protest, the government rescinded its seizure of mooo.com three days later.[11] FreeDNS maintained that it had "never allowed this type of abuse of its DNS service."[12] However, the forfeiture provision allowed the government to seize mooo.com after an ex parte hearing, without notifying or involving FreeDNS.[13] This effectively forced FreeDNS and the site owners to prove their innocence in order to continue to publish online.

America has begun to censor the Internet. In addition to Walsh's blog, the federal government has blocked other law-abiding sites without notice, from pages about Cuban music[14] to soccer broadcasts[15] to WikiLeaks.[16] In the past year, it seized 125 domain

---

[8] See Department of Homeland Security, *Joint DHS-DOJ "Operation Protect Our Children" Seizes Website Domains Involved in Advertising and Distributing Child Pornography* (Feb 15, 2011), online at http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm (visited Sept 20, 2012).

[9] See FreeDNS, *News!* (Feb 12, 2011), online at http://freedns.afraid.org/news (visited Sept 20, 2012) (noting, for February 12, 2011, that "mooo.com (the most popular shared domain at afraid.org) was suspended at the registrar level").

[10] See Jamie Zoch, *When Mooo.com Was Seized by ICE, 80K Subdomains Affected* (DotWeekly Feb 15, 2011), online at http://www.dotweekly.com/when-mooo-com-was-seized-by-ice-80k-subdomains-affected (visited Sept 20, 2012).

[11] See Matt Liebowitz and Paul Wagenseil, *Oops! Child-Porn Seizure Shuts Down 84,000 Innocent Sites* (MSNBC Mar 30, 2011), online at http://www.msnbc.msn.com/id/41649634 (visited Sept 20, 2012).

[12] FreeDNS, *News!* (cited in note 9).

[13] See 18 USC § 2254; 18 USC § 983(a)(1)(A)(ii). See also Derek Bambauer, *U.S. Gets in on Censorship Action* (Info/Law Dec 2, 2010), online at http://blogs.law.harvard.edu/infolaw/2010/12/02/u-s-gets-in-on-censorship-action (visited Sept 20, 2012); Dan Goodin, *Unprecedented Domain Seizure Shutters 84,000 Sites* (The Register Feb 18, 2011), online at http://www.theregister.co.uk/2011/02/18/fed_domain_seizure_slammed (visited Sept 20, 2012).

[14] See Adam Liptak, *A Wave of the Watch List, and Speech Disappears*, NY Times A16 (Mar 4, 2008) (reporting the blacklisting of Cuban history and culture websites by the Treasury Department due to its suspicion that the owner was facilitating transit to Cuba, despite the fact that the websites themselves were unrelated to such facilitation).

[15] See Memorandum of Points and Authorities in Support of Puerto 80's Petition for Release of Seized Property and in Support of Request for Expedited Briefing and Hearing of Same, *Puerto 80 Projects S.L.U. v United States*, No 11-cv-03983, *2–3, 9, 15–20 (SDNY filed Jun 13, 2011) ("Rojadirecta Memorandum") (arguing that a website that provided a forum for

names[17] as part of a new strategic plan for intellectual-property enforcement, 10 for alleged child-pornography distribution,[18] and 24 based on involvement in a botnet.[19] This online censorship defies conventional scholarly wisdom,[20] which holds that the end of history[21] for American Internet filtering occurred in 2004, after the Supreme Court decisions that invalidated the Communications Decency Act of 1996[22] (CDA) and its progeny, the Child Online Protection Act[23] (COPA).

The reality, though, is not so simple. Hard censorship, where the government exerts control directly over Internet infrastructure or forces intermediaries to do so through law, is still largely blocked by architectural and constitutional constraints. However, this Article argues that government retains powerful tools to prevent access to disfavored Internet content through soft censorship: employing unrelated laws as a pretext to block material, paying for filtered access, or persuading intermediaries to restrict content.[24] While these methods are more indirect than a straightforward statutory prohibition, they are formidable precisely because they are less visible and less obviously a prior restraint. Moreover, they have not yet been thoroughly

users to post links to video streams of sporting events was not violating copyright law and should be released from seizure pending trial).

16 See Order Granting Permanent Injunction, *Bank Julius Baer & Co v WikiLeaks*, No C 08-00824 JSW, *1–2 (ND Cal filed Feb 14, 2008).

17 See US Intellectual Property Enforcement Coordinator, *2011 U.S. Intellectual Property Enforcement Coordinator Joint Strategic Plan: One Year Anniversary* 5 (June 2011), online at http://www.whitehouse.gov/sites/default/files/ipec_anniversary_report.pdf (visited Sept 23, 2012).

18 See Department of Justice, *Federal Courts Order Seizure of Website Domains Involved in Advertising and Distributing Child Pornography* (Feb 15, 2011), online at http://www.justice.gov/opa/pr/2011/February/11-crm-189.html (visited Sept 20, 2012).

19 See Public Interest Registry, *2011 Takedown Notices* (Apr 12, 2011), online at http://pir.org/why/takedowns2011 (visited Sept 20, 2012). A botnet is a collection of computers that are connected to the Internet and compromised by an attacker.

20 See, for example, John Copeland Nagle, *Pornography as Pollution*, 70 Md L Rev 939, 952 (2011); Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech*, in Saul Levmore and Martha C. Nussbaum, eds, *The Offensive Internet: Privacy, Speech, and Reputation* 155, 155 (Harvard 2010); Martha McCarthy, *The Continuing Saga of Internet Censorship: The Child Online Protection Act*, 2005 BYU Educ & L J 83, 87–94 (Issue 2); Susan Hanley Kosse, *Try, Try Again: Will Congress Ever Get It Right? A Summary of Internet Pornography Laws Protecting Children and Possible Solutions*, 38 U Richmond L Rev 721, 728–38 (2004).

21 Consider Francis Fukuyama, *The End of History and the Last Man* xii (Free Press 1992).

22 Pub L No 104-104, 110 Stat 133, codified at 47 USC §§ 223, 230, 303, 560–61, 609. See *Reno v ACLU*, 521 US 844, 874 (1997).

23 Pub L No 105-277, 112 Stat 2681 (1998), codified at 47 USC § 231. See *Ashcroft v ACLU*, 542 US 656, 666 (2004).

24 Polk Wagner makes a similar distinction between direct and indirect censorship. See R. Polk Wagner, *Filters and the First Amendment*, 83 Minn L Rev 755, 771–72, 777–78 (1999).

analyzed by scholars or courts, leaving the state with considerable freedom of action. The Article argues that soft censorship is less legitimate than hard censorship—its methods are not as transparent, open, narrow, or accountable as statutory schemes that specifically address online content control. It is thus worrisome that the government's power to censor the Internet is strongest where it is least legitimate.

This Article is the first to offer a theoretical account of seemingly unrelated measures as a coherent government effort to control Internet content. Previous scholarship has only explored individual aspects of soft censorship, without recognizing their larger implications for an American system of online restraints. For example, Seth Kreimer discusses state efforts to enlist intermediaries to engage in censorship by proxy.[25] Ronald Mann and Seth Belzley set out a framework for when deputizing intermediaries is sensible,[26] as do Douglas Lichtman and Eric Posner.[27] Candice Spurlin and Patrick Garry empirically assess the effects of the inducement provided by the Children's Internet Protection Act[28] (CIPA) for filtering on library patrons' access to information.[29] Tim Wu writes a defense of agencies' use of threats in place of formal rulemaking or enforcement through adjudication.[30] Annemarie Bridy discusses the market changes pushing Internet Service Providers (ISPs) and content providers into a willingness to engage in copyright enforcement via private ordering, particularly through filtering and user disconnection.[31] This Article argues these methods form a set of tools that the state can, and does, employ to block disfavored information with minimal constraint.

The Article next advances a controversial proposition: if hard censorship is more legitimate than soft, and society determines that

---

[25] See Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U Pa L Rev 11, 22–33 (2006).

[26] See Ronald J. Mann and Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 Wm & Mary L Rev 239, 265–75 (2005) (arguing for a gatekeeper regime under which no-fault liability is imposed on Internet intermediaries as least cost avoiders).

[27] See Douglas Lichtman and Eric Posner, *Holding Internet Service Providers Accountable*, 14 S Ct Econ Rev 221, 233–40 (2006).

[28] Pub L No 106-554, 114 Stat 2763, 2763A-335 (2000), codified at 20 USC §§ 6801, 6777, 9134 and 47 USC § 254.

[29] See Candice J. Spurlin and Patrick M. Garry, *Does Filtering Stop the Flow of Valuable Information?: A Case Study of the Children's Internet Protection Act (CIPA) in South Dakota*, 54 SD L Rev 89, 92–96 (2009).

[30] See Tim Wu, *Agency Threats*, 60 Duke L J 1841, 1848–52 (2011).

[31] See Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 Or L Rev 81, 102–03, 105, 120, 124–25 (2010).

government should prevent access to certain materials, then the federal government should pass and implement a statutory scheme for online censorship. The Article outlines key elements that would make such a statute legitimate.[32] It is not clear that censorship *should* occur. Rather, it is clear that it *is* occurring. If America decides to block access to pieces of the Net, this Article contends that it should do so in a way that is open, transparent, narrowly targeted, and protective of key normative commitments such as open communication, equal treatment under the law, and due process.

Finally, the Article also engages a larger scholarly debate about the proper role of government in shaping a profoundly important public space for communication—the Internet—that is primarily owned by private actors. The debate over the proper regulatory role of the state regarding information on the Net is a contentious one. In particular, scholars disagree vehemently over the merits and lawfulness of net neutrality rules and of government efforts to shape online content. Susan Crawford contends that communications policy should optimize the transmission of online communications rather than focusing on particular Internet layers or infrastructure providers, as a means of achieving "[t]he greatest possible diversity of new ideas."[33] In opposition, Daniel Lyons asserts that net neutrality obligations would take ISPs' property without compensation, effecting an unconstitutional taking.[34] Marvin Ammori argues for diminished scrutiny when government seeks to promote democratic content.[35] Hannibal Travis wants the Federal Communications Commission (FCC) to employ structural rules to ensure informational diversity.[36] This Article argues that the creativity of the American government's censorship efforts supports stringent review of state regulation of online information. Soft censorship has much to teach about the

---

[32] Previously, I developed a process-based methodology to assess censorship's legitimacy. See Derek E. Bambauer, *Cybersieves*, 59 Duke L J 377, 390–410 (2009) (proposing that censorship practices be evaluated along metrics of "openness, transparency, narrowness, and accountability").

[33] Susan P. Crawford, *The Internet and the Project of Communications Law*, 55 UCLA L Rev 359, 365, 375–90 (2007).

[34] See Daniel A. Lyons, *Virtual Takings: The Coming Fifth Amendment Challenge to Net Neutrality Regulation*, 86 Notre Dame L Rev 65, 92–114 (2011).

[35] See Marvin Ammori, *Beyond Content Neutrality: Understanding Content-Based Promotion of Democratic Speech*, 61 Fed Comm L J 273, 303–19 (2009).

[36] See Hannibal Travis, *The FCC's New Theory of the First Amendment*, 51 Santa Clara L Rev 417, 431–43 (2011) (substantiating a narrative in which the repeal of media neutrality regulation in the late 1980s precipitated a "'dark age' of deregulation and conglomerate control" that has severely constrained the heterogeneity of individual media consumption).

legitimacy of governmental actions that seek to shape Internet discourse.

The Article proceeds in five parts. First, it catalogues the censor's toolkit, providing an account of the methods by which state and federal governments can interdict content of which they disapprove. In the process, it distinguishes between hard and soft methods of censorship. Second, it subjects these methods to searching, process-based analysis of their legitimacy. Third, it evaluates the constraints upon these indirect tools, recasting the New Chicago School model of regulatory modalities as a means of *resisting* regulation.[37] Fourth, it makes a controversial and likely unpopular proposal: hard censorship is normatively preferable to soft censorship. A properly crafted statute allowing the government to block certain unlawful content would be legitimate, although not necessarily sensible. It would align Internet censorship with precedent on prior restraint in other media. Lastly, this Article explores how soft Internet censorship offers lessons for how American legal doctrine and scholarship should evaluate the state's role in shaping public discourse in the private medium of the Internet. This Article is concerned not with Orwell's Room 101, with its overt control over communication, but instead with Orwell's Armchair, where the state eases people into a censored environment through softer, more indirect means.[38]

I. THE CENSOR'S TOOLKIT

A nation-state that wants to censor the Internet has five options: direct control, deputizing intermediaries, pretext, payment, and persuasion. These methods range from pure government action and responsibility to almost completely private action. This Article classifies the two techniques with the greatest governmental role—direct control and deputizing intermediaries—as hard censorship. Here, the state imposes its content preferences directly, either by implementation through computer code[39] or by force of law.[40] The other three methods—pretext-based censorship via orthogonally related laws, paying for filtered access, and persuasion through pressure—are classified as soft censorship. There, the state's intervention is far less visible and direct, and might be formally easier to evade—though, as the Arti-

[37] See generally Lawrence Lessig, *The New Chicago School*, 27 J Legal Stud 661 (1998).

[38] George Orwell, *Nineteen Eighty-Four* 184 (Harcourt 1949).

[39] Lawrence Lessig, *Code Version 2.0* 4–8 (Perseus 2006) (suggesting that "the software and hardware . . . that make cyberspace what it is also regulate cyberspace as it is").

[40] See Robert M. Cover, *Violence and the Word*, 95 Yale L J 1601, 1613 (1986).

cle demonstrates, less so in practice. This Part first defines censorship in the Internet context and then explores each option.

A. Censorship as Prior Restraint

For this Article, censorship occurs when a government prevents communication between a willing speaker and a willing listener through interdiction rather than through post-communication sanctions. Filtering is a specific type of censorship, where the state uses technological methods to identify and block prohibited content. This usage of "censorship" is normatively neutral: the state censors equally when it seizes child pornography shipped via the postal service[41] and when it employs software to block access to a labor union's website on a Wi-Fi network.[42] Censorship is thus one means of increasing the cost of disfavored information. There are others: criminal sanctions for producing or consuming material,[43] taxes upon it,[44] or campaigns to drive social disapprobation for it.[45] Importantly, censorship is not binary, where information is either completely blocked or freely available: a state can succeed by raising the effective price of contraband information sufficiently. Indeed, even hard censorship cannot filter perfectly. China's system of Internet censorship, popularly known as the Great Firewall, can be breached by users with sufficient technical skill and yet is highly effective in controlling the information available to most Chinese citizens.[46] Thus, censorship (as used in this Article) describes a process where a state uses ex ante measures to make information more difficult or expensive to access, with the goal of preventing its consumption or distribution.

Ordinarily, the term "censorship" carries a pejorative connotation. It is particularly loaded in American scholarly and political discourse, where censorship is seen as anathema to deeply held beliefs

---

41 See, for example, *United States v Rabe*, 848 F2d 994, 996–97 (9th Cir 1988).

42 See, for example, *Pro-union Website Blocked in Wisconsin Capitol* (CNN Feb 22, 2011), online at http://articles.cnn.com/2011-02-22/us/wisconsin.budget_1_website-unions-access (visited Sept 20, 2012).

43 See, for example, 18 USC § 1466A(a) (criminalizing the production, distribution, receipt, and possession of child sexual abuse images); 18 USC § 1832(a) (criminalizing the trafficking in trade secrets); 18 USC § 793 (criminalizing the same for national defense information).

44 See, for example, *Arkansas Writers' Project, Inc v Ragland*, 481 US 221, 227 (1987).

45 See, for example, Department of Health and Human Services, *Cyberbullying* (Mar 8, 2012), online at http://www.stopbullying.gov/topics/cyberbullying (visited Sept 20, 2012).

46 See James Fallows, *"The Connection Has Been Reset,"* The Atlantic 64, 69 (Mar 2008).

about the importance of unfettered discourse and free expression.[47] Yet America's normative commitment to open communication contains exceptions. Even the Supreme Court has permitted a state government to censor by seizing material in advance of a judicial determination as to whether it was unlawful.[48] The Court emphasized, rightly, the procedural safeguards included in the scheme rather than treating seizures as per se impermissible.[49] America, like every other country, views some material as sufficiently harmful to warrant blocking. And like most countries, America prefers not to describe such blocking as censorship. Each state balances freedom of expression against other values differently, leading to incommensurable definitions of what constitutes censorship.[50] For Americans, filtering file-sharing sites does not qualify as censorship,[51] but filtering politically oriented[52] or pornographic sites[53] does. For South Korean citizens, though, filtering pornographic sites or politically oriented material that praises North Korea does not count as censorship,[54] but blocking file-sharing sites does.[55] Norms vary. Every country assumes that its own views on content restrictions are not only defensible, but natural.

---

47 See, for example, *Sorrell v IMS Health Inc*, 131 S Ct 2653, 2664 (2011) (holding "[l]awmakers may no more silence unwanted speech by burdening its utterance than by censoring its content"); *Bantam Books, Inc v Sullivan*, 372 US 58, 70 (1963) (stating that "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity"). See also John Fee, *The Pornographic Secondary Effects Doctrine*, 60 Ala L Rev 291, 302 (2009) (writing that "[c]lassifying some kinds of speech as 'low value' for constitutional purposes is a dangerous exercise, for it risks the suppression of speech that the majority of society does not appreciate").

48 See *Kingsley Books, Inc v Brown*, 354 US 436, 438–39, 441 (1957).

49 Id at 441–44.

50 See Thomas S. Kuhn, *The Structure of Scientific Revolutions* 148 (Chicago 3d ed 1996) (defining incommensurability as a term used to describe the circumstance where disputants "disagree about the list of problems that any candidate for paradigm must solve").

51 See, for example, Mitch Bainwol, *Support for PROTECT IP Piles Up*, Music Notes Blog (RIAA May 26, 2011), online at http://www.riaa.com/blog.php?content_selector=riaa-news-blog&blog_selector=Support-For-PROTECT-IP (visited Sept 20, 2012); *Floyd Abrams: PROTECT IP Act Does Not Violate First Amendment* (American Federation of Television and Radio Artists May 24, 2011), online at http://aftra.org/69A98E28C25B42DCA66AED619E4D2084.htm (visited Sept 20, 2012).

52 See, for example, *Pro-union Website Blocked in Wisconsin Capitol* (cited in note 42).

53 See *Ashcroft v ACLU*, 542 US 656, 666 (2004) (affirming a preliminary injunction barring enforcement of COPA, a law aimed at curtailing minors' access to pornography).

54 Freedom House, *Freedom on the Net 2011: South Korea* *303–04 (2011), online at http://www.freedomhouse.org/sites/default/files/inline_images/South%20Korea_FOTN2011.pdf (visited Sept 20, 2012).

55 See Mike Masnick, *Kicking People off the Internet Not Enough in South Korea, Copyright Lobbyists Demand More* (Techdirt Nov 19, 2009), online at http://www.techdirt.com/articles/20091117/1154046972.shtml (visited Sept 20, 2012).

The virtue of this Article's more technical definition of censorship is that it concentrates upon the *method* a government uses to control information and defers analysis of the *legitimacy* of such measures to a separate step. The alternative is to be drawn into absurdity, such as classifying the removal of sites that facilitate intellectual property (IP) infringement as mere enforcement of property rights but removal of sites that report on human rights as censorship.[56] Censorship thus becomes a descriptive term; normative conclusions require rigorous analysis of each particular censorship regime.

I have previously argued that the legitimacy of censorship is best judged by the processes through which a state arrives at blocking decisions.[57] In particular, legitimacy depends on four factors: whether blocking is openly described, transparent in what content it targets, narrow and effective in what it actually filters, and accountable via formal or informal processes to the users it purports to protect.[58] 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.

An implicit consequence of using this process-based methodology to evaluate Internet censorship is that some filtering regimes will be judged legitimate. I have argued that the provisions of the Digital Millennium Copyright Act[59] (DMCA) that press intermediaries to censor in return for immunity from copyright liability should be viewed as justified under this framework.[60] This conclusion and the concomitant result that Internet censorship can be legitimate are controversial and have been criticized by scholars such as Milton Mueller.[61] However, it is helpful simply to note that this Article does not consider the efforts to restrict content that it describes as automatically suspect. It seeks to identify whether there are problems with how government engages in censorship rather than rejecting information control altogether.

---

[56] See Bambauer, 59 Duke L J at 384–86 (cited in note 32) (documenting the "scant agreement on what material ought to be off-limits" and concluding that "[c]omparing nations' online censorship from one normative perspective is unhelpful").

[57] See id.

[58] See id at 386–87.

[59] Pub L No 105-304, 112 Stat 2860 (2000), codified at 17 USC §§ 512, 1201–05.

[60] See Bambauer, 59 Duke L J at 401 (cited in note 32).

[61] Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* 206–08 (MIT 2010).

In many cases, censorship is surprisingly acceptable to people.[62] Users do not automatically flee, or oppose, censored communication platforms. Indeed, consumers are surprisingly comfortable with filtered information environments. Apple's iPhone, for example, holds 25 to 30 percent of the smartphone market in the United States[63] despite the fact that the company carefully censors which applications are available on its phones. Similarly, Apple removed an app named "ThirdIntifada" from its App Store because it was "offensive to large groups of people"[64] and infamously banned Pulitzer Prize-winning cartoonist Mark Fiore's app because it "ridicule[d] public figures."[65]

Other popular Internet platforms similarly exclude disfavored information. By default, Google employs its SafeSearch technology, which excludes sexually explicit images and videos from search results.[66] While users can easily alter the SafeSearch settings—making them either stricter or more lenient—behavioral economics scholarship demonstrates the power of default settings.[67] Bing, Microsoft's search engine, similarly sets a default of using SafeSearch at its moderate setting.[68] YouTube removes videos that involve sexually explicit content, graphic violence, hate speech, animal abuse, and drug abuse.[69] Most e-mail service providers block spam.[70]

---

[62] See, for example, Craig A. Depken II, *Who Supports Internet Censorship?* (First Monday Sept 4, 2006), online at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1390/1308 (visited Sept 20, 2012) (analyzing the results of an online survey on Internet censorship in which more than 46 percent of respondents agreed with such censorship in principle).

[63] See Philip Elmer-DeWitt, *Needham: Android's Market Share Peaked in March*, Apple 2.0 (CNNMoney Jun 21, 2011), online at http://tech.fortune.cnn.com/2011/06/21/needham-androids-market-share-peaked-in-march (visited Sept 20, 2012) (citing a Needham & Co estimate of 29.5 percent market share for the first quarter of 2011); Henry Blodget, *Android Is Destroying Everyone, Especially RIM—iPhone Dead in Water* (Bus Insider Apr 2, 2011), online at http://www.businessinsider.com/android-iphone-market-share-2011-4 (visited Sept 20, 2012) (citing a Comscore estimate of 25.2 percent for the same period).

[64] *Apple Removes Anti-Israel 'ThirdIntifada' App from App Store* (Huffington Post June 22, 2011), online at http://www.huffingtonpost.com/2011/06/23/apple-removes-anti-israel-thirdintifada-app_n_882857.html (visited Sept 20, 2012).

[65] Laura McGann, *Mark Fiore Can Win a Pulitzer Prize, but He Can't Get His iPhone Cartoon App Past Apple's Satire Police*, Nieman Journalism Lab (Nieman Foundation Apr 5, 2010), online at http://www.niemanlab.org/2010/04/mark-fiore-can-win-a-pulitzer-prize-but-he-cant-get-his-iphone-cartoon-app-past-apples-satire-police (visited Sept 20, 2012).

[66] See Google Help, *SafeSearch: Filter Objectionable Content*, online at http://support.google.com/websearch/bin/answer.py?hl=en&answer=510&topic=1678515&ctx=topic (visited Sept 20, 2012).

[67] See id. See also Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* 85–87 (Yale 2008) (discussing default settings).

[68] See Bing Help, *Block Explicit Websites*, online at http://onlinehelp.microsoft.com/en-US/bing/ff808441.aspx (visited Sept 20, 2012).

[69] See *YouTube Community Guidelines*, online at http://www.youtube.com/t/community_guidelines (visited Sept 20, 2012).

The prevalence of bowdlerized information platforms has important consequences for soft censorship. America's shared belief in free expression suggests that users would doggedly resist the imposition of filtering. Yet the evidence predicts a much more muted response. Americans love the iPhone and use Google with such regularity that the search engine's name has become a verb.[71] Censorship that is sufficiently subtle is likely to be accepted, even if only grudgingly.

Having defined its use of censorship, the Article now explores each modality in detail.

B. Direct Control

Chesterfield, Virginia, is a county south of Richmond that offers residents and visitors the Metro Richmond Zoo, a NASCAR speedway, Virginia State University, and free wireless Internet access.[72] Anyone can surf the Web using Chesterfield's Citizen Wi-Fi, provided they do not want pornography.[73] The county does not provide access to the entire Internet from Citizen Wi-Fi: Chesterfield employs the Websense Internet-filtering software to block access to "graphic pornography," as defined by Websense's "adult material" content category.[74] Websense's "Adult Material" category includes not only graphic pornography but also material on sex education, lingerie, swimsuits, and sexuality.[75] Chesterfield offers Internet users a choice: access the Internet for free, at the cost of being blocked from speech that the county government dislikes or pay for unfiltered access.[76]

---

[70] See, for example, *Holomaxx Technologies Corp v Microsoft Corp*, 2011 WL 3740813, *4 (ND Cal).

[71] See, for example, *Merriam-Webster* (Merriam-Webster 2012), online at http://www.merriam-webster.com/dictionary/google (visited Sept 20, 2012).

[72] See Chesterfield County, *Tourism and Leisure: Tourism and Leisure—Visit Chesterfield*, online at http://www.chesterfield.gov/visitors.aspx?id=3019 (visited Sept 20, 2012) (detailing the pleasures of Chesterfield); Chesterfield County, *Connected Government: Citizen Wi-Fi—Frequently Asked Questions*, online at http://www.chesterfield.gov/connectedgovernment.aspx?id=2086 (visited Sept 20, 2012).

[73] See Chesterfield County, *Connected Government: Citizen Wi-Fi—Access to Free, Wireless Internet Is as Easy as Opening a Laptop!*, online at http://www.chesterfield.gov/connectedgovernment.aspx?id=2083 (visited Sept 20, 2012).

[74] *Acceptable-Use Policy*, online at http://www.chesterfield.gov/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=10156 (visited Sept 20, 2012).

[75] Websense, *URL Categories: Accurate, Current, and Comprehensive*, online at http://www.websense.com/content/URLCategories.aspx (visited Sept 20, 2012). Chesterfield blocks the Sex subcategory but not Lingerie and Swimsuit, Nudity, or Sex Education. See E-mail from Barry Condrey, Chief Information Officer of Chesterfield County (June 29, 2011) (on file with author).

[76] Chesterfield seeks to "eliminate access 'to materials that constitute obscenity or child pornography, materials harmful to juveniles, or materials that create a sexually harassing envi-

Chesterfield's direct provision of censored Internet access is increasingly common. Culver City in California—home to three movie studios—provides free Wi-Fi that blocks peer-to-peer (P2P) file-sharing applications.[77] Utah Transit Authority's express buses offer wireless access to commuters but filter "offensive sites."[78] Houston's municipal Wi-Fi network blocks both adults and minors from reaching material that is obscene, constitutes child pornography, or is harmful to minors.[79] Boston filtered its public wireless network until funding problems forced it offline.[80]

Direct control is a potent form of hard censorship. Its success, though, depends on the architecture of a country's networks, which can result either from deliberate design decisions or from path dependency. History matters. Saudi Arabia and China exemplify the capabilities of hard censorship through direct control. In Saudi Arabia, all Internet traffic passes through a single point—a group of proxy servers—that acts as the locus for censorship.[81] A government agency, the Communications and Information Technology Commission, holds responsibility for blocking content, and the Saudi Telecom Company, which is owned by the state, is the primary access and network provider.[82] Similarly, China performs its Internet filtering using routers at the backbone of the network, which is state owned.[83] With direct control, governmental responsibility for censorship is immediate, obvious, and singular. The state imposes content deci-

ronment,' which are illegal or inappropriate." Chesterfield County, *Acceptable-Use Policy* (cited in note 74).

[77] See Karl Bode, *LA Muni-Fi Filters Smut, P2P: Audible Magic Gear at the MPAA's Request* . . . (Broadband Reports Aug 23, 2006), online at http://www.broadbandreports.com/shownews/77538 (visited Sept 20, 2012).

[78] Utah Transit Authority, *Frequently Asked Questions*, online at http://www.rideuta.com/mc/?page=RidingUTA-Amenities-WirelessInternet-FAQs (visited Sept 20, 2012).

[79] Houston Public Library, City of Houston, and WeCAN Houston, *Digital Inclusion Initiative Frequently Asked Questions* 10 (May 21, 2008), online at http://www.uh.edu/hcpp/DigitalInclusionInitiativeFAQ.pdf (visited Sept 20, 2012).

[80] See Danny Weitzner, *City of Boston Censoring Municipal WiFi* (Apr 24, 2007), online at http://dig.csail.mit.edu/breadcrumbs/node/188 (visited Sept 20, 2012); Ionut Arghire, *After Municipal Wi-Fi Network Fail, Boston Settles for Hotspot Patchwork* (Softpedia Apr 19, 2008), online at http://news.softpedia.com/news/After-Municipal-Wi-Fi-Network-Fail-Boston-Settles-For-Hotspot-Patchwork-83845.shtml (visited Sept 20, 2012).

[81] Ronald Deibert, et al, eds, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* 561–70 (MIT 2010).

[82] See generally OpenNet Initiative, *Internet Filtering in Saudi Arabia* (Aug 6, 2009), online at http://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf (visited Sept 20, 2012).

[83] See OpenNet Initiative, *Internet Filtering in China in 2004–2005: A Country Study* 3–4 (Apr 14, 2005), online at http://opennet.net/sites/opennet.net/files/ONI_China_Country_Study.pdf (visited Sept 20, 2012).

sions by creating a choke point for access that it controls and then implementing filtering at that point.

In the United States, significant direct control by state actors is unlikely for architectural reasons. Most of the relevant Internet infrastructure in America, such as the network backbone, routers, and access points, is privately owned and operated. During the Internet's early development, the primary infrastructure—first the Advanced Research Projects Agency Network, and then the National Science Foundation Network—was owned by the federal government, but the administration of President Bill Clinton made a deliberate decision to privatize the network backbone in 1995.[84] Internet access to homes and residences is provided almost exclusively by private firms offering Internet service via digital subscriber line (DSL), cable modem, satellite, or wireless telephone services.[85] Thus, while federal and state governments provide some publicly available access points, most users obtain Internet access over privately held networks.

However, the emergence of publicly provided Internet access—typically hailed as a boon that can close America's digital divide[86]—ironically poses risks to open Internet communication. Government has nearly free rein in deciding what content to permit or deny when it supplies the medium.[87] This power is profound: there is no difference in principle between censoring speech on topics of political debate such as abortion and censoring political speech directly. A government that can forbid counseling on abortion in state-funded clinics,[88] and forbid access to material "harmful to minors" on its Internet services,[89] can just as readily block content related to foreign policy choices.[90] It is not clear that there are constitutional constraints on the government's ability to filter publicly provided Internet access, only political ones. For example, while there have been lawsuits

---

84 See Manuel Castells, *The Rise of the Network Society* 46 (Wiley-Blackwell 2d ed 2010).

85 Industry Analysis and Technology Division, Wireline Competition Bureau, FCC, *Internet Access Services: Status as of June 30, 2010* (Mar 2011), online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-305296A1.pdf (visited Sept 20, 2012).

86 See, for example, Jan Chipchase, *Is Internet Access a Human Right?*, CNN.com Blogs (CNN July 14, 2011), online at http://globalpublicsquare.blogs.cnn.com/2011/07/14/is-internet-access-a-human-right (visited Sept 20, 2012).

87 See Part III.B.

88 See *Rust v Sullivan*, 500 US 173, 192–200 (1991).

89 20 USC § 9134(f)(1)(A)(i) (forbidding the grant of funds to any library that does not have in place a policy of "technology protection" for Internet-enabled computers that protects against access to visual depictions that are "harmful to minors"). See *United States v American Library Association, Inc*, 539 US 194, 203–09 (2003).

90 See Liptak, *A Wave of the Watch List*, NY Times at A16 (cited in note 14) (reporting on allegations that a travel site was banned for facilitating tourism in Cuba).

against schools that block material based on its viewpoint, such as support for gay and lesbian students, none has resulted in a decision on the merits.[91] While this may demonstrate a consensus that such discrimination is unlawful, it more likely results from school districts' unwillingness to devote scarce funds to litigation or to endure scrutiny over alleged bias against a group of their students. Similarly, politically based funding that restricts information has been found constitutional. Such restrictions include Title X grants prohibiting abortion counseling,[92] arts funding requiring respect for "general standards of decency,"[93] and international HIV funding banning promotion of abortion.[94] Direct provision of Internet access by government comes at a cost: one may be able to reach only speech of which the state approves.

Thus, while history prevents America from using direct control, a form of hard censorship, to filter the majority of Internet access, it remains a potent tool where available.

C. Deputizing Intermediaries

Alaska decided to replay history. The state's legislature passed a bill that banned the distribution of indecent material to minors, and Governor Sean Parnell signed it into law.[95] ISPs, among others, would have faced liability under the law.[96] The statute was strikingly similar not only to the provisions of two federal laws invalidated by the Supreme Court[97] but also to a series of state laws struck down as violations of the First Amendment.[98] And, as in each prior case, a federal court permanently enjoined Alaska's law from being enforced. The district court in Alaska noted that it was unclear whether

---

91 Consider Complaint for Injunctive Relief, Declaratory Judgment, and Nominal Damages, *Parents, Families, and Friends of Lesbians and Gays, Inc v Camdenton R-III School District*, No 2:11-cv-04212, *1 (WD Mo filed Aug 15, 2011), online at http://www.aclu.org/files/assets/pflagcomplaint.pdf (visited Sept 20, 2012).

92 See *Rust*, 500 US at 178–81.

93 20 USC § 954(d)(1). See *National Endowment for the Arts v Finley*, 524 US 569, 590 (1998).

94 *Center for Reproductive Law and Policy v Bush*, 304 F3d 183, 186 (2d Cir 2002).

95 See Alaska Stat Ann § 11.61.128(a) (criminalizing the knowing distribution of certain material harmful to minors if the recipient was under 16 years of age); Chris Klint, *Federal Judge Blocks State Anti–Child-Porn Law* (KTUU July 1, 2011), online at http://www.ktuu.com/news/ktuu-federal-judge-blocks-state-anti-child-porn-law-070111,0,472573.story (visited Sept 20, 2012) (tracing the bill's history).

96 See Alaska Stat Ann § 11.61.125(d).

97 See *Ashcroft*, 542 US at 666; *Reno v ACLU*, 521 US 844, 874, 885 (1997).

98 See *American Booksellers Foundation for Free Expression v Sullivan*, 799 F Supp 2d 1078, 1080–81 (D Alaska 2011) (listing cases).

the law required knowledge that a recipient was underage but that even if it did, there are "no reasonable technological means that enable a speaker on the Internet to ascertain the actual age of persons who access their communications."[99] Thus, the statute created a risk that adult Internet users would limit their expression only to what was suitable for minors, a harm deemed constitutionally impermissible by the Supreme Court under similar circumstances.[100]

The outcome of the suit against Alaska's statute appeared obvious: the law was quite similar to § 223 of the CDA, which was invalidated by the Supreme Court in 1997.[101] Nonetheless, Alaska enacted the statute, and defended it, in a seemingly (and ultimately) fruitless effort. Yet Alaska is in good company: six other states have had similar laws invalidated since the Court ruled on the CDA.[102] Both state and federal governments have remained eager to mandate that intermediaries carry out filtering of disfavored content, on pain of civil or criminal sanctions despite the consistently skeptical attitude of reviewing courts.[103]

The second method of censorship is where government deputizes key intermediaries to perform filtering via public law regulation. This step—also a form of hard censorship—has been the most obvious and popular regulatory response in the US to perceived problems of harmful content online. The federal government twice enacted legislation that would have compelled ISPs and other intermediaries to block material deemed harmful to minors, once as the CDA[104] and once as COPA.[105] In each case, the ACLU challenged the

---

99 Id at 1081–82.

100 See id, citing *Reno*, 521 US at 876.

101 See *Reno*, 521 US at 860, 885 (overturning then-current 47 USC § 223(d)). Section 223(d) criminalized using an interactive computer service, such as the Internet, to display patently offensive material concerning sex or excretion in a manner available to people under the age of eighteen. Alaska's law criminalized knowing distribution, including on the Internet, of material harmful to minors if the recipient was under the age of sixteen. The statute is also similar to § 231 of COPA, which criminalized knowingly posting, for commercial purposes, Web material that was harmful to minors. See *Ashcroft*, 542 US at 661–62, 666 (overturning then-current 47 USC § 231(a)(1)).

102 *Sullivan*, 799 F Supp 2d at 1080–81 (listing cases). See also *American Libraries Association v Pataki*, 969 F Supp 160, 183–84 (SDNY 1997) (striking down a similar New York statute on Commerce Clause grounds in the same year that *Reno* was decided).

103 The only state statute to survive scrutiny is that of Ohio and then only because the state narrowed its interpretation of the law to cover only "personally directed communication between an adult and a person that the adult knows or should know is a minor." *American Booksellers Foundation for Free Expression v Strickland*, 601 F3d 622, 628 (6th Cir 2010) (upholding Ohio Rev Code § 2907.31(D) against First Amendment and Commerce Clause challenges). Generally available Internet content, such as a web page, would not run afoul of the Ohio statute.

104 See 47 USC § 223 (1996), abrogated by *Reno*, 521 US at 885.

law on constitutional grounds and succeeded—once because the law was deemed overbroad[106] and once because the Supreme Court viewed end-user filtering technology as a less restrictive alternative.[107] While these decisions would seem to foreclose legally mandated filtering, bills that require Internet censorship are hardy congressional perennials. For example, in the 111th Congress, Senator Patrick Leahy proposed legislation entitled Combating Online Infringement and Counterfeits Act,[108] which passed the Judiciary Committee but not the Senate itself. Representative Paul Kanjorski introduced a bill that would have required ISPs to filter material related to brokerage fraud.[109] Similarly, in the 112th Congress, Senator Leahy and nine other senators introduced the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011[110] (PROTECT IP Act), which unanimously passed the Senate Judiciary Committee.[111]

State governments have also attempted to mandate filtering. In 2009, Minnesota sought to require ISPs to prevent customers from accessing gambling sites. The state reversed course after a gambling interest group challenged the regulations in court as violations of the First Amendment and the Commerce Clause.[112] In 2002, Pennsylvania required ISPs to block sites designated by the state attorney general as offering child pornography.[113] The result—blocking over 1.1 million sites to prevent access to roughly 400 with unlawful material—was found to be unconstitutional by a federal court as a violation of both the First Amendment and the Dormant Commerce Clause.[114] Alaska, Michigan, New Mexico, New York, South Caroli-

105 See 47 USC § 231 (1996 & Supp 1998), abrogated by *Ashcroft*, 542 US at 666.

106 See *Reno*, 521 US at 885.

107 See *Ashcroft*, 542 US at 666.

108 S 3804, 111th Cong, 2d Sess, in 156 Cong Rec S 7207 (Sept 20, 2010).

109 Investor Protection Act of 2009, HR 3817, 111th Cong, 1st Sess, in 155 Cong Rec H 11456 (Oct 15, 2009).

110 S 968, 112th Cong, 1st Sess, in 157 Cong Rec S 2936 (May 12, 2011).

111 Greg Sandoval, *Senate Panel OKs Controversial Antipiracy Bill* (CNET May 26, 2011), online at http://news.cnet.com/8301-31001_3-20066456-261.html (visited Sept 20, 2012).

112 See Complaint and Demand for Declaratory and Injunctive Relief, *Interactive Media Entertainment & Gaming Association v Willems*, No 0:09CV01065, *16, 18–19 (D Minn filed May 6, 2009) (available on Westlaw at 2009 WL 456360) ("Willems Complaint"). Poker Players Alliance, *Poker Players Alliance Declares Victory in Minnesota* (June 4, 2009), online at http://theppa.org/press-releases/2009/06/04/mn-poker-players-alliance-declares-victory-in-minnesota-060409 (visited Sept 20, 2012) (celebrating Minnesota's decision to reverse course on Internet gambling).

113 See *Center for Democracy & Technology v Pappert*, 337 F Supp 2d 606, 619–21 (ED Pa 2004).

114 See id at 655, 658, 660, 662.

na, Vermont, and Virginia all promulgated legislation similar to the CDA or COPA, and all had their laws blocked by similar First Amendment challenges.[115] Lawmakers are persistent. Thus, US states that attempt to impose filtering mandates on Internet intermediaries face not only First Amendment challenges but also limits based on the effects of such laws on interstate commerce, a zone constitutionally reserved to Congress.[116]

The key check on governmental attempts to use legal regulation to bind intermediaries, such as ISPs, to perform censorship has been the protection for free speech under the First Amendment. Filtering laws face at least two First Amendment hurdles: describing prohibited content with sufficient precision[117] and showing that censorship—disfavored prior restraint—is the best-tailored method of achieving the state's goals.[118] These barriers are formidable and greatly foreclose governmental attempts to formally devolve responsibility for censorship onto intermediaries for the foreseeable future.[119]

However, legislators can refine filtering laws to make them more likely to withstand scrutiny. The first adjustment is to target only content that is plainly unlawful. Both the CDA and COPA faltered here; the CDA banned both "indecent" and "patently offensive" communications,[120] and COPA aimed at material that was "patently offensive with respect to minors" and lacked "serious literary, artistic, political, or scientific value for minors."[121] In both cases, the Supreme Court found the bans overbroad because they trod up-

115 See *Sullivan*, 799 F Supp 2d at 1080–81.

116 Consider *Hunt v Washington State Apple Advertising Commission*, 432 US 333, 348–54 (1977).

117 See *Reno*, 521 US at 874.

118 See, for example, *ACLU v Mukasey*, 534 F3d 181, 190 (3d Cir 2008).

119 As a practical matter, the current Supreme Court appears to be highly speech protective. Countervailing considerations such as protecting minors from video game violence, reducing prescription drug costs, preventing emotional harm to the families of American soldiers killed in combat, or improving access to media by less well-funded political candidates were held insufficient to justify speech restrictions in the October Term 2010 alone. See *Arizona Free Enterprise Club's Freedom Club PAC v Bennett*, 131 S Ct 2806, 2824, 2828–29 (2011) (holding that an Arizona statute providing for public election financing pegged to private election financing imposes an unconstitutional burden on the speech of private candidates and their financers); *Brown v Entertainment Merchants Association*, 131 S Ct 2729, 2742 (2011) (holding that a California law restricting minors' access to violent video games is unconstitutional under the First Amendment); *Sorrell*, 131 S Ct at 2659, 267 (holding the same for a Vermont statute prohibiting the sale, disclosure, and use of pharmacy records revealing doctors' prescribing practices); *Snyder v Phelps*, 131 S Ct 1207, 1220 (2011) (holding that a protest near the funeral of a soldier was entitled to protection under the First Amendment from tort liability). This trend likely decreases further the chance that federal filtering legislation would survive judicial scrutiny.

120 See *Reno*, 521 US at 859–61.

121 See *Ashcroft*, 542 US at 661–62, quoting 47 USC § 231(e)(6).

on speech that was lawful for adults. Reducing the scope of prohibited content will be unpalatable for legislators, who frequently prefer to target pornography,[122] content "harmful to minors,"[123] or material supporting terrorist groups.[124] But, focusing only on content that is clearly unlawful—such as child pornography, obscenity, or intellectual property infringement—has constitutional benefits that can help a statute survive. These categories of material do not count as speech for First Amendment analysis, and hence the government need not satisfy strict scrutiny in attacking them.[125] Recent bills seem to show that legislators have learned this lesson—the PROTECT IP Act, for example, targets only those websites with "no significant use other than engaging in, enabling, or facilitating" IP infringement.[126] Banning only unprotected material could move censorial legislation past overbreadth objections.

Additionally, censorship laws would need to show that they do not sweep too much protected speech into the cybersieves along with unprotected information. When Pennsylvania required ISPs in the state to prevent access to child pornography sites, for example, the ISPs blocked traffic to those sites' IP addresses. The providers claimed that retrofitting their networks to engage in more finely tuned filtering methods, such as URL-based blocking, would be prohibitively expensive.[127] The consequence of targeting IP addresses was that roughly 1.1 million unrelated sites were filtered along with about 400 that allegedly hosted child porn—or, approximately 2,700 lawful sites blocked for each unlawful one. Unsurprisingly, a federal district court found this massive overblocking burdened "substantial-

---

122 See, for example, Michael O'Brien, *Bachmann, Santorum Sign onto Social Conservative Pledge*, The Hill's Blog Briefing Room (The Hill July 8, 2011), online at http://thehill.com/blogs/blog-briefing-room/news/170471-bachmann-santorum-sign-onto-social-conservative-pledge (visited Sept 20, 2012).

123 *Sullivan*, 799 F Supp 2d at 1079, quoting Alaska Stat Ann § 11.61.128.

124 See, for example, Elizabeth M. Renieris, Note, *Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and United Kingdom and the Need for an International Solution*, 11 Vand J Enter & Tech L 673, 682–85 (2009); Thomas Claburn, *Senator Lieberman Wants Terrorist Videos Removed from YouTube* (InformationWeek May 20, 2008), online at http://www.informationweek.com/news/internet/google/207801148 (visited Sept 20, 2012).

125 See, for example, *Harper & Row Publishers, Inc v Nation Enterprises*, 471 US 539, 555–60 (1985) (suggesting that copyright infringement can overshadow First Amendment rights); *New York v Ferber*, 458 US 747, 765 (1982) (holding that a New York law covering child pornography "describes a category of material the production and distribution of which is not entitled to First Amendment protection"); *Miller v California*, 413 US 15, 23 (1973) (reaffirming that material classified as obscenity is "unprotected by the First Amendment").

126 PROTECT IP Act § 2, in 157 Cong Rec at S 2937 (cited in note 110).

127 See *Pappert*, 337 F Supp 2d at 630.

ly more protected material than [was] essential" to the government's goal of interdicting child pornography.[128]

Technology, though, has progressed significantly since Pennsylvania's statute was struck down in 2004. ISPs increasingly use sophisticated monitoring techniques, such as deep-packet inspection, to calibrate network performance, monitor for malware, and differentiate among types of content to implement quality of service.[129] Providers can distinguish BitTorrent content from Web content, and from VoIP phone calls. As ISPs increasingly deploy cheaper and more sophisticated network equipment, courts may look more favorably upon legal rules that require them to use their new tools to filter unlawful material.[130] The costs of filtering have fallen, and its effectiveness—ISPs' ability to block prohibited material, and only that material—has risen. Overblocking will likely be less of a hurdle for future filtering legislation, both in constitutional and technological terms.

In short, while First Amendment precedent limits significantly the state's ability to compel intermediaries to censor, technological progress and legislative restraint could enable government to deputize intermediaries.

D. Pretext

Blame the Kentucky Derby.

In September 2008, the Commonwealth of Kentucky sought to have 141 domain names for gambling sites, such as AbsolutePoker.com and PokerStars.com, transferred to the state's control. The sites operate, and their domain names are registered, outside Kentucky; indeed, most are outside the United States altogether. Defending the move, Governor Steve Beshear argued that "[u]nlicensed, unregulated, illegal Internet gambling poses a tremendous threat to the citizens of the Commonwealth," necessitating the seizure.[131] In reality, the state worried that online gambling would undercut revenue from horse rac-

---

128 Id at 655.

129 See Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U Ill L Rev 1417, 1432–36 (2009); Bridy, 89 Or L Rev at 102–05, 120–25 (cited in note 31).

130 See Bridy, 89 Or L Rev at 102–05, 120–25 (cited in note 31).

131 Commonwealth of Kentucky, Press Release, *Kentucky Seizes Domain Names of Illegal Internet Gambling Sites* (Sept 22, 2008), online at http://migration.kentucky.gov/newsroom/governor/20080922onlinegaming.htm (visited Sept 20, 2012).

ing and offline gambling;[132] gambling interests were major contributors to the Governor's political campaign.[133]

Kentucky cited its gambling regulations as legal authority for the move.[134] Under Kentucky law, any illegal gambling device can be forfeited to the state.[135] The statute defines gambling devices either as "[a]ny so-called slot machine or any other machine or mechanical device an essential part of which is a drum or reel with insignia thereon" or "[a]ny other machine or any mechanical or other device . . . designed and manufactured primarily for use in connection with gambling."[136] Domain names do not fit either definition. Nonetheless, the Commonwealth successfully convinced a trial court to issue the seizure notice, in a hearing that did not include the domain name owners.[137] While the legal contest over the seizure has been bogged down in procedural questions of standing, the larger issue remains open: Kentucky continues to assert authority over any website, and domain name, that operates in purported violation of its laws, anywhere in the world.[138]

It is unlikely that Kentucky's gambling law covers Internet domain names. The definitions for gambling devices are clearly aimed at mechanical devices such as roulette wheels, poker tables, and slot machines,[139] and domain names are not "designed and manufactured primarily for use in connection with gambling."[140] Moreover, Kentucky probably could not lawfully regulate domain names even if its statute clearly covered them.[141] Domain names, and the Internet more broad-

132 See id.

133 Mike Masnick, *Kentucky's Gambling Domain Name Grab Sets a Terrible Precedent* (Techdirt Oct 10, 2008), online at http://www.techdirt.com/articles/20081009/1142502506.shtml (visited Sept 20, 2012).

134 See Order of Seizure of Domain Names, *Commonwealth v 141 Internet Domain Names*, No 08-ci-1409, *1–2 (Franklin Cir Ct filed Sept 18, 2008) ("Kentucky Order of Seizure"), online at http://www.thedomains.com/wp-content/order-of-seizure-of-domain-names.pdf (visited Sept 20, 2012).

135 See Ky Rev Ann Stat § 528.100.

136 Ky Rev Ann Stat § 528.010(4).

137 Kentucky Order of Seizure at *3.

138 See *Commonwealth v Interactive Media Entertainment & Gaming Association, Inc*, 306 SW3d 32, 34–35 (Ky 2010).

139 See Ky Rev Stat § 528.010(4)(b).

140 Ky Rev Stat § 528.010(4)(b).

141 See, for example, Amicus Curiae Brief of the Electronic Frontier Foundation, the Center for Democracy and Technology, the ACLU of Kentucky, the Media Access Project, the United States Internet Industry Association, the Internet Commerce Coalition, and the Internet Commerce Association in Opposition to the Appeal of the Commonwealth of Kentucky, *Commonwealth v Interactive Media Entertainment & Gaming Association, Inc*, No 2008-ca-2036, *10–13 (Ky filed May 12, 2009) (available on Westlaw at 2009 WL 3291802).

ly, are modalities of interstate and international communication.[142] Regulation of such modalities is reserved to Congress by the Commerce Clause.[143] To the extent that Kentucky's law interfered with interstate or international commerce, it would be preempted by the Commerce Clause unless Congress had authorized such interference—which it expressly has not.[144] Kentucky's domain name grab constitutes a pretext-based effort to censor online gambling entities through a statute that is, at best, tangentially related to the Internet. This exemplifies the third method open to government censors: pretext. Pretext is also the first form of indirect, or soft, censorship analyzed by this Article.

Government censors are creative. They have employed a series of seemingly unrelated laws as a means of restricting Internet content. The US Department of the Treasury ordered an American domain name registrar to disable sites owned by a company that arranges travel to Cuba, in violation of American law, even though several of the sites were unrelated to travel.[145] A federal judge ordered a registrar to cease directing traffic to WikiLeaks when the site posted documents claiming that a Caymanian bank helped clients engage in tax fraud.[146] Like Kentucky, Minnesota sought to extend its regulations regarding offline gambling to the Internet, temporarily ordering ISPs to block access to poker websites.[147] The federal government has repeatedly used civil forfeiture laws designed to prevent the loss of property used for unlawful purposes to interdict access to websites offering allegedly counterfeit goods or content that infringes copyright.[148]

These methods represent censorship by pretext, which occurs when state officials use unrelated laws as means of blocking access to disfavored speech. Pretext, though, is generally permissible as a constitutional matter, unless the government manifests unlawful intent,[149] or the law itself is designed to discriminate among content

---

142 See *Pataki*, 969 F Supp at 181.

143 See US Const Art I, § 8, cl 3; *Mobile County v Kimball*, 102 US 691, 702 (1880).

144 See, for example, 31 USC §§ 5361(b), 5362(10)(D)(ii).

145 See Liptak, *A Wave of the Watch List*, NY Times at A16 (cited in note 14).

146 See *Whistle-Blower Site Taken Offline* (BBC News Feb 18, 2008), online at http://news.bbc.co.uk/2/hi/technology/7250916.stm (visited Sept 20, 2012); Derek E. Bambauer, *Consider the Censor*, 1 Wake Forest J L & Pol 31, 34–37 (2011).

147 See Willems Complaint at *16 (seeking declaratory judgment that an attempt by Minnesota to pressure Internet casinos is unconstitutional).

148 Margaret Grazzini, *Four Rounds of ICE Domain Name Seizures and Related Controversies and Opposition*, Berkeley Tech L J Bolt (Berkeley Feb 23, 2011), online at http://btlj.org/?p=917 (visited Sept 20, 2012).

149 See *Washington v Davis*, 426 US 229, 249–52 (1976) (rejecting a Title VII challenge to a police department's hiring test).

providers.[150] However, pretext is problematic when applied to information. Laws regulating speech necessarily include safeguards to prevent flaws such as vagueness, overbreadth, or content discrimination. Regulations unrelated to speech usually lack these protections and concomitantly confer greater power upon government censors and impose greater costs on society. Moreover, they present a heightened risk of arbitrary enforcement, since they are employed not to address the societal interest that is the laws' initial purpose but for an orthogonal one that empowers officials to reify their normative preferences regarding information through selective enforcement.[151]

With domain name seizures, for example, the federal government can prevent a website from communicating at a particular address on the Internet by obtaining, in an ex parte hearing, a warrant on the grounds that the domain name is involved in willful copyright infringement.[152] While the loss of a single domain name may be overcome relatively readily, given that domain names are inexpensive to register and rapidly indexed by search engines, the government must typically demonstrate greater justification for interfering with speech. Indeed, the standard for seizing a domain name is lower than that government must meet to prove the underlying offense of copyright infringement,[153] and yet it enables the state to censor a website unless its owner can show that the seizure creates substantial hardship.[154] Courts may well facilitate pretext-based seizures, either out of disapprobation for the challenged content or because they fail to recognize the importance of the First Amendment issues involved. For example, in the first challenge to a domain name seizure by the federal government, a federal judge dismissed the website owner's attempt to recapture the domain name in a five-page opinion that gave short shrift to the First Amendment problems inherent in the forfeiture statute.[155]

---

150 *Ragland*, 481 US at 227 (noting that a "discriminatory tax on the press burdens rights protected by the First Amendment").

151 Consider *Colorado v Bertine*, 479 US 367, 372, 376 (1987) (finding no Fourth Amendment violation in inventory search by police in part because there did not appear to be bad faith or pretextual use of the search).

152 See, for example, Order, *Puerto 80 Projects, S.L.U. v United States*, No 11-cv-04139-PAC, *1 (SDNY filed Aug 4, 2011) ("Puerto 80 Order"), online at https://www.eff.org/files/RojadirectaOrder.pdf (visited Sept 20, 2009).

153 See 17 USC § 506(a)(1)–(2).

154 See 18 USC § 983(f)(1)(D).

155 See Puerto 80 Order at *4 (holding that "the First Amendment considerations discussed here certainly do not establish the kind of substantial hardship required to prevail on this petition").

Pretext might be particularly problematic in a zone where American constitutional doctrine is especially lenient regarding speech protections: intellectual property. The Supreme Court has rejected heightened scrutiny of copyright legislation on First Amendment grounds, for example, because copyright law contains built-in safeguards such as fair use, the idea-expression dichotomy, the prohibition on copying facts, and various technical exemptions such as exemptions for libraries and archives.[156] Government efforts to prevent IP infringement thus receive greater judicial deference than other regulation of speech does.[157] This may be worrisome when, in fact, state enforcement of IP rights occurs at the direction of IP owners, as has occurred with the seizure of domain names that allegedly infringe copyright law.[158] Conferring enforcement decisions regarding speech on private parties with a vested interest raises concerns about arbitrary enforcement.

Government officials can employ laws that are formally neutral, and unrelated to Internet expression, to block access to information of which they disapprove. Reviewing courts may permit such actions because they agree with the underlying impulse toward censorship or because they fail to appreciate the expressive interests at stake.[159] Pretext-based efforts are a substantial focus of American online filtering today and represent a method of soft censorship with relatively few checks.

E. Payment

Students at the University of Dayton can use the school's network to watch YouTube videos, send e-mail, and browse the Web, but they can't share files using peer-to-peer software such as Bit-

---

156 See *Eldred v Ashcroft*, 537 US 186, 218–21 (2003).

157 See, for example, *San Francisco Arts & Athletics, Inc v United States Olympic Committee,* 483 US 522, 532–40 (1987) (upholding a federal law granting the United States Olympic Committee exclusive use of the word "Olympic"); *Zacchini v Scripps-Howard Broadcasting Co*, 433 US 562, 569–78 (1977) (holding that First Amendment did not protect a television news company from suit when it televised a "human cannonball act" without the permission of the actor); *Universal City Studios, Inc v Corley*, 273 F3d 429, 453–58 (2d Cir 2001) (rejecting a First Amendment challenge to the DMCA).

158 See, for example, Simon Vozick-Levinson, *Why Is the Department of Homeland Security Shutting Down Popular Rap Sites? An Official Explains Why They're Targeting Bloggers*, Music Mix (Entertainment Weekly Nov 30, 2010), online at http://music-mix.ew.com/2010/11/30/homeland-security-rap-blog (visited Sept 20, 2012).

159 Puerto 80 Order at *4. See also *Universal City Studios*, 273 F3d at 455–58 (permitting an injunction against hyperlinking by a website).

Torrent.[160] Administrators at the private university prevent P2P data from transiting Dayton's network. Blocking P2P software prevents some infringing activity—most BitTorrent traffic consists of unauthorized downloads of copyrighted materials[161]—but it also prevents Dayton students from updating their copies of World of Warcraft or Starcraft II.[162] Blizzard, the company that produces these games, uses P2P technology to distribute patches for the games more efficiently.[163] While gamers are hardly a priority for university IT administrators, why would the University of Dayton target a specific application for filtering given these side effects?

The answer, in a word, is money. While the university notes that P2P traffic can cause network congestion and reveal private files inadvertently, its primary reason for filtering is to ensure that the school remains eligible for federal student aid.[164] The Higher Education Opportunity Act[165] (HEOA) requires schools that want to remain eligible for such aid to implement at least one "technology-based deterrent[]" as a means of impeding unlawful distribution of copyrighted material.[166] Filtering software that blocks file sharing is explicitly listed as a canonical technology-based deterrent,[167] and the University of Dayton believes "blocking P2P traffic is our 'safest harbor' in meeting" HEOA requirements.[168] Federal aid is critical to

---

160 See University of Dayton, *P2P File Sharing* (2010), online at http://www.udayton.edu/udit/accounts_access/p2p.php (visited Sept 20, 2012); Procera Networks, *Taking Full Control of Network Resources at the University of Dayton* *1, online at http://www.proceranetworks.com/images/documents-2011-04-14/CS-Dayton-2011-4-14.pdf (visited Sept 20, 2012).

161 A January 2010 study by Princeton computer science professor Ed Felten and his student, Sauhard Sahi, sampled 1,021 BitTorrent files available via the trackerless Mainline DHT variant. They estimated that only 1 percent of the files were noninfringing. See Ed Felten, *Census of Files Available via BitTorrent*, Freedom to Tinker Blog (CITP Jan 29, 2010), online at https://freedom-to-tinker.com/blog/felten/census-files-available-bittorrent (visited Sept 20, 2012) (providing a breakdown of the various file types observed).

162 See University of Dayton, *P2P File Sharing* (cited in note 160).

163 See id; *Blizzard Downloader Common Errors and Issues* (Battle.Net June 21, 2012), online at https://us.battle.net/support/en/article/blizzard-downloader-common-errors-and-issues (visited Sept 20, 2012); Peter Smith, *Rogers Communication Throttling World of Warcraft Players* (ITworld Mar 28, 2011), online at http://www.itworld.com/internet/141632/rogers-communications-throttling-world-warcraft-players (visited Sept 20, 2011).

164 See University of Dayton, *P2P File Sharing* (cited in note 160).

165 Pub L No 110-315, 122 Stat 3078 (2008), codified in various sections of Title 20.

166 HEOA § 493, 122 Stat at 3309; 34 CFR § 668.14(b)(30).

167 The Manager's Report accompanying the HEOA listed four technology-based deterrents: "bandwidth shaping, traffic monitoring to identify the largest bandwidth users, a vigorous program of accepting and responding to [DMCA] notices, and a variety of commercial products designed to reduce or block illegal file sharing." *Higher Education Opportunity Act: Conference Report to Accompany H.R. 4137*, HR Conf Rep 110-803, 110th Cong, 2d Sess 548 (2008).

168 See University of Dayton, *P2P File Sharing* (cited in note 160).

many students' ability to finance higher education.[169] Losing aid eligibility would be a severe blow for a school. Thus, the federal government can use its funding power to induce schools such as Dayton to filter content and applications that they would otherwise permit. In short, payment is a potent tool to prod intermediaries to filter.

Using the power of the public fisc to induce censorship is particularly potent for entities that both provide Internet access and depend upon governmental grants or largesse. Universities, for example, not only receive grants to support research expenditures[170] but also depend upon federally subsidized loans to their students to help make higher education affordable. Funding, though, often comes at the price of unfettered speech decisions. For example, Congress mandates that institutions of higher education provide military recruiters with access to their students equal to that granted other recruiters[171] and that such schools not discriminate on the basis of sex,[172] regardless of the schools' views on these topics. Schools that decline to meet either condition forfeit access to certain federal funding.[173] Similarly, under the administration of Presidents Ronald Reagan and George H.W. Bush, federal funding for family-planning services required that recipient organizations refrain from discussing pregnancy termination with patients.[174] The relevant regulations passed constitutional scrutiny, as Congress was permitted to fund only the speech that it intended to support.[175]

Congress has used its power of the purse to press censorship on schools. Under CIPA, primary and secondary schools must install filters that prevent access to materials that are obscene, that constitute child pornography, or that are harmful to minors to obtain discounted Internet access under the federal E-Rate program.[176] Under the HEOA, institutions of higher education must develop and implement plans to combat copyright infringement on their networks; these plans

---

169 In 2007–2008, 47 percent of postsecondary undergraduate students received federal student aid in some form, with an average total amount of $6,600. National Center for Education Statistics, *Fast Facts* (Department of Education 2011), online at http://nces.ed.gov/fastfacts/display.asp?id=31 (visited Sept 20, 2012).

170 See Philip Hamburger, *The New Censorship: Institutional Review Boards*, 2004 S Ct Rev 271, 321–24 (2004).

171 See 10 USC § 983(b); *Rumsfeld v Forum for Academic and Institutional Rights, Inc*, 547 US 47, 70 (2006).

172 See 20 USC § 1681(a); *Grove City College v Bell*, 465 US 555, 574 (1984).

173 See *Grove City College*, 465 US at 575.

174 See *Rust*, 500 US at 179–81.

175 Id at 192–201.

176 47 USC § 254(h)(5).

must include at least one technology-based deterrent.[177] While the implementing regulations leave it to a school's discretion to determine what constitutes a "technology-based deterrent,"[178] a number of institutions moved to employ content filtering to satisfy this requirement.[179] Indeed, filtering that blocks file sharing is singled out as one of the four mechanisms that satisfies HEOA's requirements.[180] Similarly, at least six states have promulgated laws that condition funding for schools or libraries on those institutions engaging in Internet filtering.[181]

Paying key intermediaries to filter requires the government to allocate fiscal resources, which are always sharply contended for, to the goal of censoring Internet content. However, despite its costs, payment is an attractive option for at least two reasons, as demonstrated by CIPA and related state laws. First, engaging in content restrictions via the spending power, rather than by direct legislative command, generally enables this type of soft censorship to survive First Amendment scrutiny. The state's scope of action may be even greater when censoring through payment. Not only can the government command that intermediaries filter certain content in exchange for funding, it can arguably require them to block based on viewpoint as well. The Supreme Court's controversial decision upholding limits on abortion counseling by medical providers who received Medicaid family planning funds validated limits based on viewpoint, despite the Court's attempts to disguise them as content-neutral provisions.[182] The line between content-based and viewpoint-based restrictions is a malleable one that depends in large measure on how the limit is framed. A mandate that schools and libraries block material with nudity would likely survive scrutiny as a justifiable content-

---

177 HEOA § 493, 122 Stat at 3309; 34 CFR § 668.14(b)(30). See also 20 USC § 1094(a)(29).

178 34 CFR § 668.14(b)(30)(i).

179 *Bowling Green State University, Digital Copyright Safeguards Program—Response*, online at http://www.bgsu.edu/infosec/responsesafeguards.html (visited Sept 20, 2012); Texas State University–San Marcos, *Copyright Infringement Deterrence Plan* (July 2, 2010), online at http://security.vpit.txstate.edu/awareness/digital_copyright_p2p_filesharing/copyright_infringement_deterrence.html (visited Sept 20, 2012); Illinois State University, *Peer-to-Peer (P2P) File Sharing is Blocked on Campus* (Nov 29, 2011), online at http://helpdesk.illinoisstate.edu/kb/index.phtml?kbid=1432 (visited Sept 20, 2012); Southern Connecticut State University, *Copyright and P2P File Sharing*, online at http://www.southernct.edu/oit/securityandpolicy/p2p (visited Sept 20, 2012).

180 HR Conf Rep No 110-803 at 237, 548–49 (cited in note 167).

181 The states are California, Colorado, Georgia, Iowa, Ohio, and Utah. See National Conference of State Legislatures, *Laws Relating to Filtering, Blocking, and Usage Policies in Schools and Libraries* (Feb 13, 2012), online at http://www.ncsl.org/default.aspx?tabid=13491 (visited Sept 20, 2012). A number of other states simply mandate that schools and libraries filter without funding as enticement. See id.

182 See *Rust*, 500 US at 192–94.

based restriction,[183] but it could just as readily be framed as limiting pro-nudity websites.[184]

Additionally, the government may have greater leverage with payment: it can implement censorship with only partial funding of Internet access. With direct control, by contrast, the government bears the full cost of supplying access. Philip Hamburger notes that universities must monitor all research projects involving human subjects through institutional review boards (IRBs) to remain eligible for federal funding from agencies that have adopted the Common Rule as a condition of eligibility, including projects with no public funds involved.[185] Thus, the government imposes a review procedure on all research conducted on human subjects by paying for a portion of it. Similarly, universities risked losing federal research funding if any of their constituent institutions failed to grant access to military representatives on equal terms with other recruiters—even if those institutions did not themselves receive such monies.[186] While entities are free to decline government funding, doing so makes them less competitive relative to peers who accept such funding, as they must either accept the greater costs of unfiltered provision, or pass those costs through to users in the form of increased fees. This accomplishes the state's goal: access to prohibited material becomes more expensive. Payment may be attractive to government because it is cost efficient: the state can control behavior for an entire institution by funding a small part of it.[187]

Payment is a popular form of soft censorship, cabined only by governmental willingness (and, perhaps, capacity) to spend public funds on Net access measures.

F. Persuasion and Pressure

WikiLeaks faced a cascade. The whistleblowing site had published a series of sensitive American diplomatic and military docu-

---

183 See *American Library Association*, 539 US at 203–05 (upholding a law requiring public libraries to filter information that is "harmful to minors," including obscene material, even though such a law is based on content).

184 *Rust*, 500 US at 209–11 (Blackmun dissenting) (interpreting a regulation preventing abortion counseling as a viewpoint-based restriction of all advocacy of abortion as family planning). Sites opposing nudity would hardly include nude images.

185 See Hamburger, 2004 S Ct Rev at 301–06 (cited in note 170).

186 See *Forum for Academic and Institutional Rights*, 547 US at 70.

187 Consider *FCC v League of Women Voters of California*, 468 US 364, 400 (1984) (noting that the anti-editorializing condition on Corporation for Public Broadcasting (CPB) funding would apply to all content on stations receiving only 1 percent of their funding from the CPB).

ments related to the conflict in Afghanistan in July 2010, the conflict in Iraq in October 2010, and the State Department in November 2010.[188] Reaction from the American government was swift, and harsh.[189] In addition to contemplating formal legal charges against WikiLeaks contributors such as Julian Assange, government officials sought to convince private firms involved with the site to censor it.[190] First, Senator Joseph Lieberman had his staff contact Amazon.com, which hosted WikiLeaks on its cloud computing service EC2.[191] Within twenty-four hours, Amazon terminated its relationship with WikiLeaks, citing unspecified violations of the company's Terms of Service.[192] Lieberman promised continued scrutiny, saying he would ask "what [Amazon] and other web service providers will do in the future to ensure that their services are not used to distribute stolen, classified information."[193]

Next, payment service provider PayPal ceased processing donations to WikiLeaks, citing a letter sent by State Department legal adviser Harold Koh to WikiLeaks.[194] MasterCard quickly followed suit,[195] as did Visa[196] and Discover.[197] Banks stopped processing transactions for the site.[198] US pressure sought to choke off donations to WikiLeaks, or at least to make them difficult and costly.

---

188 Yochai Benkler, *A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate*, 46 Harv CR–CL L Rev 311, 321–27 (2011).

189 Id at 330–39.

190 Id at 339–40. See also Bambauer, 1 Wake Forest J L & Pol at 33 (cited in note 146).

191 Ewen MacAskill, *WikiLeaks Website Pulled by Amazon after US Political Pressure*, Guardian (London) 11 (Dec 2, 2010). See Charles Arthur, *WikiLeaks Evades Hackers with Shift to Amazon*, (Guardian Nov 29, 2010), online at http://www.guardian.co.uk/technology/2010/nov/29/wikileaks-amazon-ec2-ddos (visited Sept 20, 2012).

192 Hal Roberts, *Amazon's Terms of Service and WikiLeaks' Censorship* (Guardian Dec 3, 2010), online at http://www.guardian.co.uk/commentisfree/cifamerica/2010/dec/03/wikileaks-amazon-takedown-censorship (visited Sept 20, 2012).

193 Joe Lieberman, *Amazon Severs Ties with WikiLeaks* (Dec 1, 2010), online at http://lieberman.senate.gov/index.cfm/news-events/news/2010/12/amazon-severs-ties-with-wikileaks (visited Sept 20, 2012).

194 Alexia Tsotsis, *PayPal VP on Blocking WikiLeaks: State Department Said It Was Illegal* (TechCrunch Dec 8, 2010), online at http://techcrunch.com/2010/12/08/paypal-wikileaks (visited Sept 20, 2012).

195 Declan McCullagh, *MasterCard Pulls Plug on WikiLeaks Payments* (CNET Dec 6, 2010), online at http://news.cnet.com/8301-31921_3-20024776-281.html (visited Sept 20, 2012).

196 Aoife White, *Visa Europe Blocks WikiLeaks Donations through Payment Site* (Bloomberg July 8, 2011), online at http://www.bloomberg.com/news/2011-07-08/visa-europe-will-block-wikileaks-donations-through-payment-site.html (visited Sept 20, 2012).

197 *Visa Blocks WikiLeaks Donations Again* (RT July 8, 2011), online at http://rt.com/usa/news/visa-wikileaks-donations-thursday (visited Feb 25, 2012); Samuel Richter, *The U.S. Government Blocked Diners Club from Accepting WikiLeaks Payments* (Benzinga Nov 2, 2011), online at http://www.benzinga.com/news/11/11/2087446/the-u-s-government-blocked-diners-club-from-accepting-wikileaks-payments (visited Sept 20, 2012).

198 Benkler, 46 Harv CR–CL L Rev at 342 (cited in note 188).

The United States continued to apply pressure on intermediaries to cease service to WikiLeaks. After the site's US-based Domain Name Server (DNS) provider, EveryDNS, dropped WikiLeaks as a client (in the face of denial-of-service attacks on its servers), WikiLeaks moved to Switch, a Swiss DNS provider.[199] The US government pushed Switch to stop working with WikiLeaks, but the company refused.[200] By contrast, the American data visualization company Tableau Software removed graphics analyzing the content of the WikiLeaks documents in response to Senator Lieberman's public statement.[201] Relatedly, the State Department sought to discourage college students from reading the leaked cables by suggesting it could lead to denial of a security clearance and thus federal government career opportunities.[202]

WikiLeaks survives. But the coordinated pressure campaign by various US government actors reduced access to the site, increased its costs, and sent a clear signal of American willingness to use informal means as well as formal legal mechanisms to interdict content perceived as threatening. Political figures portrayed the organization as anti-American; Vice President Joe Biden called WikiLeaks founder Assange a "hi[gh]-tech terrorist,"[203] Secretary of State Hillary Clinton accused the site of "an attack on the international community . . . that safeguard[s] global security,"[204] and Representative Peter King sought to have the site declared a terrorist organization.[205] The pressure on US companies was significant—government officials strongly suggested that companies doing business with the site were at least fellow travelers, if not complicit in WikiLeaks's actions.[206]

---

[199] Charles Arthur and Josh Halliday, *WikiLeaks Fights to Stay Online after US Company Withdraws Domain Name* (Guardian Dec 3, 2010), online at http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns (visited Aug 6, 2012).

[200] Josh Halliday, *WikiLeaks Site's Swiss Registry Dismisses Pressure to Take It Offline* (Guardian Dec 4, 2010), online at http://www.guardian.co.uk/media/2010/dec/04/wikileaks-site-swiss-host-switch (visited Sept 20, 2012).

[201] Charles Arthur, *WikiLeaks Cables Visualization Pulled after Pressure from Joe Lieberman* (Guardian Dec 2, 2010), online at http://www.guardian.co.uk/world/blog/2010/dec/03/wikileaks-tableau-visualisation-joe-lieberman (visited Sept 20, 2012).

[202] See *Some Columbia U. Students Warned about WikiLeaks* (FoxNews Dec 4, 2010), online at http://www.foxnews.com/us/2010/12/04/columbia-u-students-warned-wikileaks (visited Sept 20, 2012).

[203] Ewen MacAskill, *Julian Assange Like a Hi-tech Terrorist, Says Joe Biden*, Guardian (London) 11 (Dec 20, 2010).

[204] *WikiLeaks Diplomatic Cables Release 'Attack on World'* (BBC Nov 29, 2010), online at http://www.bbc.co.uk/news/world-us-canada-11868838 (visited Sept 20, 2012).

[205] Helen Kennedy, *WikiLeaks Should Be Designated a 'Foreign Terrorist Organization,' Rep. Pete King Fumes*, NY Daily News 4 (Nov 28, 2010), online at http://articles.nydailynews.com/2010-11-28/news/27082693_1_air-strikes-arab-leaders-wikileaks (visited Sept 20, 2012).

[206] See Benkler, 46 Harv CR–CL L Rev at 339–42 (cited in note 188).

It is doubtful that the government could have obtained a court order commanding Amazon.com to sever ties with WikiLeaks, or MasterCard to cease accepting donations for the site.[207] Yet, informal government pressures on key intermediaries accomplished what formal legal action likely could not. The clash between WikiLeaks and the American government illustrates the last method of censorship: persuasion and pressure. Persuasion involves a range of tactics that employs various combinations of norms-based pressures, market incentives, and laws. Persuasion also involves a gradient of pressure, from moves that simply expand options to those that regulate through "raised eyebrow"[208] and the threat of creating new public law if firms fail to act.[209] Formally, though, persuasion is voluntary: no one is required to censor, and no one is provided remuneration to do so.

Persuasion demonstrates the creativity that censors adopt when more direct regulation is foreclosed. Utah, for example, considered a proposal by law professor and censorship advocate Cheryl Preston to designate as "community conscious" those ISPs who refuse to publish obscene content, remove it upon notification, and comply with court orders that mandate removal.[210] Five states try to persuade individuals to engage in end-user content filtering by requiring ISPs either to provide filtered Internet access[211] or to provide links to freely available software to perform this task.[212] These laws permit the ISP to charge for the filtering product or service.[213] The Pennsylvania state police pressed the ISP Sparklit.com to shut down a website critical of Scranton city officials, allegedly by falsely stating that

---

207 See, for example, id at 363–65. See also Bambauer, 1 Wake Forest J L & Pol at 35–36 (cited in note 146).

208 See Aurele Danoff, Comment, *"Raised Eyebrows" over Satellite Radio: Has* Pacifica *Met Its Match?*, 34 Pepperdine L Rev 743, 744–75 (2007).

209 See Matthew Lasar, *Big Content, ISPs Nearing Agreement on Piracy Crackdown System* (Ars Technica June 23, 2011), online at http://arstechnica.com/tech-policy/news/2011/06/big-content-isps-nearing-agreement-on-piracy-crackdown-system.ars (visited Sept 20, 2012).

210 Bob Bernick Jr, *Ways to Cut Access to Porn Studied*, Deseret Morning News A1 (Apr 19, 2007); see Cheryl B. Preston, *Making a Family-Friendly Internet a Reality: The Internet Community Ports Act*, 2007 BYU L Rev 1471, 1475–83.

211 La Rev Stat Ann § 51:1426; Md Comm Law Code Ann § 14-3704; Nev Rev Stat § 603.160; Utah Code Ann § 76-10-1231. See National Conference of State Legislatures, *Laws Relating to Filtering, Blocking, and Usage Policies in Schools and Libraries* (cited in note 181).

212 Tex Bus and Comm Code Ann § 323.002.

213 See La Rev Stat Ann § 51:1426(D)(2); Md Comm Law Code Ann § 14-3704(c); Nev Rev Stat § 603.160(3)(b); Utah Code Ann § 76-10-1231(3)(b).

the site was under investigation for criminal harassment.[214] The FBI had an ISP remove a private investigator's website that sought information on an informant who allegedly helped entrap a New York lawyer in a money laundering scheme.[215]

Governmental persuasion comes with different levels of pressure. Free censorware expands parental options, but with little coercion to employ them.[216] Governments can notify Web hosts that their servers contain potentially objectionable content. For example, the FBI informed Burst.net that its blogging service Blogetery was hosting material related to the terrorist group al Qaeda, including instructions on building bombs.[217] Burst.net elected to temporarily shut down the service. The FBI instructed Burst.net that it could terminate the offending site but did not mandate that it do so.

At an intermediate level, government officials seek to change corporate behavior through reputational sanctions. Senator Lieberman pushed Amazon.com to drop WikiLeaks as a client. Recently, Senator Dan Coats of Indiana demanded that the television network NBC provide him with a written account of why the network edited its airing of the Pledge of Allegiance to exclude the words "under God, indivisible."[218] Coats also pressed the company to detail "what actions NBC intends to take to prevent such inappropriate edits from occurring in the future."[219] The "community conscious" ISP designation overtly seeks to shame providers into restricting content; Preston intended it to single out an "ISP that's chosen to (be) helpful in eliminating pornography. If you choose not to do that, great. But the citizens in Utah will be made aware."[220] ISPs would thus choose between

---

214 Amended Complaint, *Pilchesky v Miller*, No 3:05-cv-2074, *8 (MD Pa filed Dec 21 2005), online at http://www.aclupa.org/downloads/PilcheskyComplaint.pdf (visited Sept 20, 2012). See also Kreimer, 155 U Pa L Rev at 26–27 (cited in note 25).

215 Evan Ratliff, *The Mark*, New Yorker 56, 62 (May 2, 2011).

216 Australia's NetAlert program provided free filtering software to parents, but only 29,000 copies were downloaded and used (as against a target of 1.4 million). See Andrew Colley, *Costs and Lack of Enthusiasm Threaten Free Net Nasty Blocking Plan*, Australian 29 (Feb 26, 2008).

217 See Greg Sandoval, *Bomb-Making Tips, Hit List behind Blogetery Closure* (CNET July 19, 2010), online at http://news.cnet.com/8301-31001_3-20010923-261.html (visited Sept 20, 2012).

218 Dan Coats, *Coats Asks NBC for Explanation of Why "Under God" Omitted from Pledge during U.S. Open Broadcast* (June 21, 2011), online at http://coats.senate.gov/newsroom/press/release/coats-asks-nbc-for-explanation-of-why-under-god-omitted-from-pledge-during-us-open-broadcast (visited Sept 20, 2012).

219 Id.

220 Bernick, *Ways to Cut Access to Porn Studied*, Deseret Morning News at A1 (cited in note 210) (alteration in original) (quoting BYU law professor Cheryl Preston).

complying with filtering criteria or forfeiting a governmental moniker of approval.

More forcefully, President Barack Obama's administration reportedly threatened ISPs with legislation that would mandate termination of the accounts of users accused of intellectual property infringement[221] and also blocking of infringing content itself,[222] as a cudgel to press providers to agree to implement these measures voluntarily. The resulting agreement between ISPs and content providers was negotiated,[223] if not in the shadow of the law, then in the threat of such shadow.[224] The government has employed similar tactics to pressure ISPs to adopt voluntary data retention measures to aid law enforcement;[225] ISP resistance led to the introduction of legislation mandating an eighteen-month retention period.[226] State pressure becomes increasingly problematic and likely illegitimate, as its forcefulness mounts. Entities such as ISPs face a painful choice: accede to governmental demands they dislike or face mandatory measures that are even more objectionable.

Persuasive efforts that result in private agreements to censor information become more problematic as they include a larger share of the relevant actors and as the homogeneity or standardization of the content restrictions increases. When then–New York Attorney General Andrew Cuomo pressed ISPs to prevent access to Usenet news

---

221 Vice President Biden supported both termination and filtering at a press conference introducing the administration's strategy to protect intellectual property. See Greg Sandoval, *Biden to File Sharers: 'Piracy is Theft'* (CNET June 22, 2010), online at http://news.cnet.com/8301-31001_3-20008432-261.html (visited Sept 20, 2012). The US government attempted to include user termination and filtering provisions in the Anti-Counterfeiting Trade Agreement (ACTA) (May 2011), online at http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf (visited Sept 20, 2012), that would bind signatory countries to implement these measures. Eric Pfanner, *Quietly, Nations Grapple with Steps to Quash Fake Goods*, NY Times B6 (Feb 16, 2010) (describing reports that the secret agreement includes measures to "sever copyright violators' Internet connections").

222 Pfanner, *Nations Grapple*, NY Times at B6 (cited in note 221).

223 See RIAA, MPAA, and Participating ISPs, *Memorandum of Understanding* 4–14 (July 6, 2011), online at http://info.publicintelligence.net/CCI-MOU.pdf (visited Sept 20, 2012).

224 See Jason Mick, *Obama Conscripts ISPs as "Copyright Cops," Unveils "Six Strikes" Plan* (DailyTech July 8, 2011), online at http://www.dailytech.com/Obama+Conscripts+ISPs+as+Copyright+Cops+Unveils+Six+Strikes+Plan/article22107.htm (visited Sept 20, 2012).

225 See Declan McCullagh, *DOJ Wants Mandatory Data Retention*, CBS's Tech Talk (CBS Jan 25, 2011), online at http://www.cbsnews.com/8301-501465_162-20029440-501465.html (visited Sept 20, 2012); Declan McCullagh, *Gonzales Pressures ISPs on Data Retention* (CNET May 26, 2006), online at http://news.cnet.com/2100-1028_3-6077654.html (visited Sept 20, 2012).

226 See Protecting Children from Internet Pornographers Act of 2011 § 4(a), HR 1981, 112th Cong, 1st Sess, in 157 Cong Rec H 3644 (May 25, 2011), online at http://www.gpo.gov/fdsys/pkg/BILLS-112hr1981rh/pdf/BILLS-112hr1981rh.pdf (visited Sept 20, 2012).

groups, claiming that they were a source of child pornography, all of New York's major ISPs responded in the same fashion: by dropping Usenet.[227] Meaningful market choice may be precluded by a standardized set of responses from access providers, driven in each case by pressure from state actors. Measures that are voluntary for intermediaries become effectively mandatory for users.

Governmental suasion, followed by private action, appears the least objectionable of the censorship tools. Companies that filter the Net have done so voluntarily, at least formally, and are presumably free to revisit their decisions. However, persuasion and pressure can be troubling for at least four reasons. First, the government may push intermediaries to censor speech that it could not lawfully block itself, as with WikiLeaks or the Scranton protest site. While this method may be less effective at times—the Swiss provider Switch ignored US efforts—it also insulates state efforts from constitutional challenge, since private parties formally make the decisions regarding content.[228] Private actors such as ISPs may be particularly vulnerable to governmental pressure, since they must interact with state regulators such as the FCC and Department of Justice in other contexts.[229]

Second, the move to silence WikiLeaks raises the specter of unequal enforcement—the government made no such attempt to dissuade or prevent publication of the cables by mainstream outlets such as the *New York Times* or the *Guardian*.[230] Informal government pressure may be selectively deployed against critics, whistleblowers, or political opposition, where formal moves would be cabined by statutory or constitutional constraints.

Third, trying to force WikiLeaks off the Internet complicates American efforts—including by Secretary of State Clinton, a

---

[227] See, for example, Declan McCullagh, *N.Y. Attorney General Forces ISPs to Curb Usenet Access* (CNET June 10, 2008), online at http://news.cnet.com/8301-13578_3-9964895-38.html (visited Sept 20, 2012).

[228] See *Denver Area Educational Telecommunications Consortium, Inc v FCC*, 518 US 727, 737 (1996).

[229] The FCC has substantial authority in other industries that ISPs are involved in, such as cable television. See, for example, John Eggerton, *Enforcement Bureau Recommends Denying Comcast Request to Stay Tennis Channel Decision* (Multichannel News Feb 8, 2012), online at http://www.multichannel.com/content/enforcement-bureau-recommends-denying-comcast-request-stay-tennis-channel-decision (visited Sept 20, 2012).

[230] See Benkler, 46 Harv CR–CL L Rev at 326–27 (cited in note 188). I have argued elsewhere that there are important distinctions between mainstream media outlets and WikiLeaks—in particular, the more rigorous ethical framework used by journalists working for mainstream media and their accountability as American companies to American citizens. See Bambauer, 1 Wake Forest J L & Pol at 40–41 (cited in note 146).

WikiLeaks critic—to advocate for online free expression.[231] Internet freedom is a significant component of the State Department's policies, both rhetorically[232] and technologically.[233] However, China too can claim that online material critical of its government is unlawful—banned by the country's national security laws.[234] Similarly, China praised British Prime Minister David Cameron's suggestion that social media be censored to prevent violence.[235] While the equivalence between China's censorship and America's attempts to interdict WikiLeaks is a false one, it has rhetorical appeal.[236]

Lastly, the clash of interests that characterizes the legislative process often produces rules that involve protection for countervailing interests such as freedom of expression, due process, and edge-based innovation.[237] In private negotiations, though, such interests are unrepresented and are incorporated only insofar as either the state or the affected firms care to consider them.[238]

This circumvention of limits on state power via enlisting private cooperation is increasingly apparent in other contexts, such as data gathering by the government. For example, Robert O'Harrow documents the close working relationship between data aggregators and law enforcement that emerged after the terrorist attacks of September 11, 2001.[239] Law enforcement requests for information about an

---

231 See, for example, Rebecca MacKinnon, *'Internet Freedom' in the Age of Assange* (Foreign Policy Feb 17, 2011), online at http://www.foreignpolicy.com/articles/2011/02/17/internet_freedom_in_the_age_of_assange?page=full (visited Sept 20, 2012).

232 See Hillary Rodham Clinton, *Remarks on Internet Freedom* (US Department of State Jan 21, 2010), online at http://www.state.gov/secretary/rm/2010/01/135519.htm (visited Sept 20, 2012).

233 See James Glanz and John Markoff, *U.S. Underwrites Internet Detour around Censors*, NY Times A1 (June 12, 2011).

234 Deibert, et al, eds, *Access Controlled* at 456–59 (cited in note 81).

235 See *Riots Lead to Rethink of Internet Freedom* (Global Times Aug 13, 2011), online at http://www.globaltimes.cn/NEWS/tabid/99/articleType/ArticleView/articleId/670718/Riots-lead-to-rethink-of-Internet-freedom.aspx (visited Sept 20, 2012) (praising Prime Minister David Cameron's suggestion to prevent rioters from using Twitter as "bold").

236 See, for example, *China Report Criticizes U.S. Human Rights Record* (Fox News Apr 11, 2011), online at http://www.foxnews.com/world/2011/04/11/china-issues-report-criticizing-human-rights (visited Sept 20, 2012).

237 See, for example, Jessica Litman, *Digital Copyright* 135–45 (Prometheus 2001) (describing legislative negotiations over the DMCA).

238 Bargaining between firms in different industries might produce arrangements that protect countervailing interests as a byproduct. For example, the new memorandum of understanding between ISPs and content owners includes an appeals process for users, a review of measures to disrupt IP infringement by an independent expert, and grace periods between multiple notifications of claimed infringement. See *Memorandum of Understanding* at *5, 7, 14 (cited in note 223). These safeguards might represent solicitude for users' interests but more likely derive from ISP concerns about losing customers.

239 Robert O'Harrow, *No Place to Hide* 2–6 (Free Press 2005).

individual might require a warrant if made directly to that person, but under the third-party doctrine's exception to the Fourth Amendment, investigators can obtain data from data-mining firms simply upon request.[240] Government can evade statutory limits on data gathering as well as constitutional ones through similar means. Geolocation data held by mobile wireless providers can be had without a warrant,[241] as can IP address records held by ISPs[242]—a critical reason for the Department of Justice's effort to force data retention requirements upon them. In short, governmental efforts to persuade, or pressure, private parties to act where the state itself might encounter difficulties in achieving regulatory ends are on the rise.

Persuasion seems like the paradigmatic example of permissible soft censorship. The government, too, is permitted to speak and to advocate for controversial positions.[243] Yet there are concerns when persuasion slides into pressure. When the government can indirectly threaten or compel private actors to fall in line with its preferences, there is a threat to the constitutionally protected liberty to exchange information that is checked poorly, if at all, by standard First Amendment doctrine. Persuasion, then, should be viewed not with leniency, but with considerable skepticism.

This Part has introduced a taxonomy based on the level of state involvement in content restrictions, ranging from hard censorship via direct control of infrastructure or legal mandates to intermediaries, through soft censorship by employing tangentially related regulation through pretext, paying entities to filter, or persuading and pressuring key actors. The next Part assesses the legitimacy of soft censorship tactics.

II. LEGITIMACY

Legitimate censorship has four virtues: it is openly described, transparent about what it restricts, narrow in the material to which it

---

240 See *United States v Miller*, 425 US 435, 443–44 (1976) (holding that the "Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities"); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L Rev 561, 563 (2009) (describing the doctrine wherein, "[b]y disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed").

241 See Stephanie K. Pell and Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 Berkeley Tech L J 117, 133–56 (2012).

242 See 18 USC § 2703(d).

243 See Robert C. Post, *Subsidized Speech*, 106 Yale L J 151, 158 (1996).

applies, and accountable to the people it seeks to protect.[244] In previous work, I have elucidated a framework to apply these four factors to assess whether a particular regime of Internet filtering is legitimate.[245] American censorship normally scores well on the accountability criterion, since it emerges from a democratic government that must regularly defend its decisions to the voters it purports to protect.[246] American filtering, though, may encounter problems with countermajoritarian concerns that are a component of accountability analysis, such as when public schools block sites with a positive view of homosexuality but leave ones with a negative view available.[247] Courts, however, provide a check upon majoritarian decision making,[248] and advocates for minority interests, such as gay and lesbian groups, have recourse to them when appeals to the political branches fail.[249]

Analysis of filtering rules in the United States, then, turns on the other three factors: openness, transparency, and narrowness. Concrete conclusions depend upon the details of each statute or rule, requiring greater length than is possible in this Article.[250] It is possible, though, to sketch rough yet helpful relative conclusions about the soft censorship methods outlined above. This Part briefly assesses the merits of the methods on each criterion.

A. Openness

To date, each soft censorship method except persuasion has performed well regarding openness. For example, most government-funded Internet access that is filtered discloses its restrictions via

---

244 See Bambauer, 59 Duke L J at 386–87 (cited in note 32).

245 See id at 390–410.

246 Citizens can thus participate in filtering decisions. See id at 401–04.

247 See, for example, Jonathan Oosting, *ACLU to Rochester High: Stop Filtering Lesbian, Gay, Bisexual and Transgender Resource Sites* (MLive Mar 28, 2011), online at http://www.mlive.com/news/detroit/index.ssf/2011/03/aclu_urges_rochester_high_stop.html (visited Sept 20, 2012); Tom Jackman, *Access to Gay Web Sites at Schools?*, Wash Post B2 (Apr 14, 2011).

248 But see Amanda Frost and Stefanie A. Lindquist, *Countering the Majoritarian Difficulty*, 96 Va L Rev 719, 728–40 (2010) (describing majoritarian pressures on elected judges).

249 See, for example, Suzanne Ito, *ACLU Sues Missouri School District for Illegally Censoring LGBT Websites*, Blog of Rights (ACLU Aug 15, 2011), online at http://www.aclu.org/blog/free-speech-lgbt-rights/aclu-sues-missouri-school-district-illegally-censoring-lgbt-websites (visited Sept 20, 2012) (describing suit over school filtering after appeal to school administrators failed).

250 For an example of the detailed analysis required to reach a conclusion, see Derek E. Bambauer, *Filtering in Oz: Australia's Foray into Internet Censorship*, 31 U Pa J Intl L 493, 516–29 (2009) (applying a four-part legitimacy framework to Australia's proposed Internet censorship regime).

terms of use that describe blocking or similar methods.[251] When the Department of Homeland Security seized domain names for allegedly assisting in copyright infringement, the government redirected users seeking those sites to a block page disclosing the seizure and providing information on the statutes involved.[252] Payment and pretext are not inherently open, but thus far the United States has been relatively straightforward in its implementation of content blocking with these tactics.

Persuasive efforts, by contrast, have not been open. The openness problem with persuasion is twofold. First, the state's role in content blocking is obscured, perhaps even deliberately, by the putatively private arrangement.[253] Thus, while the Obama administration and New York Governor Andrew Cuomo played key roles in the agreement between content companies and ISPs to police online infringement, details on their efforts and goals are elusive.[254] The risk is that governmental goals may be disguised as objectives of private firms, driven by financial or competitive motives. Second, private entities may not disclose that they censor content.[255] Comcast did not alert users that it throttled BitTorrent traffic,[256] and ISPs have been reluctant to disclose their network management practices to consumers.[257] If filtering is even marginally unpopular, ISPs may not be candid about imposing it, or they may avoid disclosure to minimize circumvention efforts.

It is possible for government to be open about its role in pressing content blocking on private parties. Cuomo, for example, openly pressured ISPs operating in New York to censor Usenet newsgroups

---

[251] See notes 73–81 and accompanying text.

[252] See Steven Musil, *U.S. Seizes Sites Linked to Copyright Infringement* (CNET Nov 26, 2010), online at http://news.cnet.com/8301-1023_3-20023918-93.html (visited Sept 20, 2012).

[253] See, for example, Timothy B. Lee, *ISP Flip-Flops: Why Do They Now Support "Six Strikes" Plan?* (Ars Technica July 6, 2011), online at http://arstechnica.com/telecom/news/2011/07/why-did-telcos-flip-flop-and-support-six-strikes-plan.ars (visited Sept 20, 2012).

[254] See id. See also Kevin Parrish, *Obama Admin Backing New Six Strikes ISP Policy* (Tom's Guide July 8, 2011), online at http://www.tomsguide.com/us/Comcast-Verizon-throttle-six-strikes-Obama,news-11799.html (visited Sept 20, 2012).

[255] See FCC, *In the Matter of Preserving the Open Internet Broadband Industry Practices*, 25 FCCR 17905, 17925–27 (2010), online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf (visited Sept 20, 2012) ("Preserving the Open Internet").

[256] Marguerite Reardon, *Comcast Denies Monkeying with BitTorrent Traffic* (CNET Aug 21, 2007), online at http://news.cnet.com/8301-10784_3-9763901-7.html (visited June 10, 2012).

[257] See *Preserving the Open Internet*, 25 FCCR at 17936–41 (cited in note 255).

after his staff found child pornography on a number of such groups.[258] To date, though, the level of openness for persuasion has been poor.

B. Transparency

Transparency measures whether a government describes adequately the content that it blocks online and the criteria that it uses to demarcate prohibited from permissible material.[259] Censorship can be open without being transparent, and vice versa.[260]

None of the soft censorship methods has been transparent to date. Pretext-based and persuasive methods have suffered similar transparency problems. The range of sites that could be targeted under civil forfeiture laws, or for warnings regarding potential IP infringement, is quite broad. Simply piecing together the statutory provisions involved in forfeiture is onerous.[261] Furthermore, all three soft approaches devolve decision making on what content to block from state actors to private ones. The Department of Homeland Security has relied heavily on input from the Motion Picture Association of America (MPAA) and Recording Industry Association of America (RIAA) in selecting domain names for seizure.[262] Similarly, the copyright alert system set in place by the Memorandum of Understanding between ISPs and content owners places responsibility for defining alleged infringement with content owners.[263] While the meth-

---

[258] See Declan McCullagh, *Cuomo Strong-Arms Comcast over Usenet* (CNET July 22, 2008), online at http://news.cnet.com/8301-13578_3-9997051-38.html (visited Sept 20, 2012).

[259] Bambauer, 59 Duke L J at 392–96 (cited in note 32).

[260] For example, Kazakhstan admits to blocking web content but is vague about what material is off-limits, prohibiting "inappropriate" or "destructive" sites. See OpenNet Initiative, *Kazakhstan*, 187 (Dec 9, 2010), online at http://opennet.net/sites/opennet.net/files/ONI_Kazakhstan_2010.pdf (visited Sept 20, 2012); Freedom House, *Freedom on the Net 2011: Kazakhstan*, 217–18 (2011), online at http://freedomhouse.org/sites/default/files/inline_images/Kazakhstan_FOTN2011.pdf (visited Sept 20, 2012). In practice, Kazakhstan blocks political opposition material, media with political content, and circumvention tools. Id at 218. Blocking can also be transparent, but not open: some Chinese search engines reveal that they filter sites at governmental behest, although China is unwilling to admit to censorship. See Bambauer, 59 Duke L J at 394 (cited in note 32).

[261] See, for example, Bambauer, *U.S. Gets In on Censorship Action* (cited in note 13) (performing some "painful statutory lifting" in trying to read all the relevant statutory provisions consistently).

[262] See, for example, Andrew T. Reynolds, Application and Affidavit for Seizure Warrant, *In re Rapgodfathers.com*, Civ No 10-2822M, *16–19 (CD Cal filed Nov 17, 2010), online at http://documents.nytimes.com/request-to-seize-web-sites-for-piracy (visited Jun 10, 2012) (noting agent's "discussion with MPAA and RIAA representatives" regarding rapgodfathers.com domain name); Darlene Storm, *ICE Domain Seizures Relied on Twisted Evidence and MPAA Say So*, Computerworld's Security Is Sexy Blog (Computerworld Dec 22 2010), online at http://blogs.computerworld.com/17575/ice_domain_seizures_relied_on_twisted_evidence_and_mpaa_say_so (visited Sept 20, 2012).

[263] See *Memorandum of Understanding* at *4–5 (cited in note 223).

odologies employed for detecting infringement are subject to independent review, the independent experts can only recommend, not require, changes.[264] And payment-based approaches almost always result in the affected institution outsourcing content decisions to a third-party provider of filtering technology, such as Websense or Blue Coat.[265] Congress did transparently define what content must be blocked for a school or library to qualify for the E-Rate program in CIPA:[266] obscenity, child pornography, and material harmful to minors, where the last category is further defined similar to obscenity as outlined by the Supreme Court in *Miller v California*.[267] The challenge, from a transparency perspective, is that the government is not the entity that applies this standard. It is difficult for government to be transparent about what content it targets for blocking when a third party makes those decisions on its behalf.

To date, soft censorship has not been transparent about what content is targeted for filtering or how decisions regarding classification are made.

C. Narrowness

Content filtering via soft censorship has been limited, in that relatively few sites have been blocked, but it has not been narrow. Narrowness has two components: overinclusivness and underinclusiveness.[268] All three forms of soft censorship have been both overinclusive and underinclusive to date.

Pretext-based blocking has been strongly underinclusive. Indeed, the federal government itself has argued that owners of seized domain names are not suffering substantial hardship because their sites continue to operate at other domains.[269] Similarly, Kentucky has not contended that its efforts to censor gambling-related content by seizing 141 domain names will suppress all such allegedly unlawful online activity available to the state's residents. While there is no evidence yet that either Kentucky or the Department of Homeland Security is targeting these sites for any ulterior motive, the seizures ap-

---

264 See id at *5.

265 See, for example, ACLU, *ACLU "Don't Filter Me" Initiative Finds Schools in Four More States Unconstitutionally Censoring LGBT Websites*, Blog of Rights (Apr 11, 2011), online at http://www.aclu.org/lgbt-rights/aclu-dont-filter-me-initiative-finds-schools-four-more-states-unconstitutionally-censori (visited Sept 20, 2012).

266 See 47 USC § 254(h)(5)(B), (6)(B).

267 413 US 15 (1973). Compare 47 USC § 254(h)(7)(G) (asking whether a work appeals to a "prurient interest"), with *Miller*, 413 US at 24.

268 See Bambauer, 59 Duke L J at 396–400 (cited in note 32).

269 See Puerto 80 Order at *3–4.

pear arbitrary: there is no real effort to interdict even a significant share of the unlawful content.

Pretext-based censorship has also been overinclusive. When the Department of the Treasury seized domain names related to Cuban tourism, it blocked not only commercial tourism sites but also several sites related to the island's culture, history, and literature.[270] The regulations authorizing seizures have an exemption for informational materials, which appear to cover such sites.[271] As the mooo.com example at the beginning of this Article suggests, technical errors by censors have at times resulted in massive overblocking.

Payment-based blocking has been strongly overinclusive and might have been underinclusive. The overinclusion might result from deliberate decisions by local officials responsible for implementing filtering or from the devolution of content categorization to private firms whose criteria do not correspond to those of the state.[272] Thus, some public schools have blocked access to nonpornographic material on gay and lesbian issues, whether due to discomfort with the viewpoint espoused or because the filter employed does not distinguish between such material that is harmful to minors, and that which is not.[273] Some advocates argue that filtering under CIPA is underinclusive by permitting adults to view pornography—material harmful to minors—on request.[274] For example, two New York City council members introduced legislation to prevent adults from viewing pornography in public libraries when a minor is nearby, arguing this would prevent taxpayers from subsidizing the consumption of content harmful to children.[275]

Persuasion-based blocking depends greatly on the private agreement at issue. Little is known, for example, about how the new copyright alert system negotiated between ISPs and content owners, at the behest of the Obama and Cuomo administrations, will operate

---

270 See Liptak, *A Wave of the Watch List*, NY Times at A16 (cited in note 14).

271 See 31 CFR § 515.545(a) (authorizing "[t]ransactions relating to the dissemination of informational materials"); 31 CFR § 515.332(a)(1) (defining "informational materials").

272 Consider ACLU, *"Don't Filter Me"* (cited in note 265); Jackman, *Access to Gay Web Sites at Schools?*, Wash Post at B2 (cited in note 247).

273 See ACLU, *"Don't Filter Me"* (cited in note 265) (observing, upon bringing the filtering to their attention, that some school districts immediately unblocked LGBT sites while others were more reluctant).

274 See, for example, *Library Bill Aims to Keep Porn Away from Children* (Times Newsweekly May 26, 2011), online at http://www.timesnewsweekly.com/news/2011-05-26/Local_News/Library_Bill_Aims_To_Keep_Porn_Away_From_Children.html (visited Sept 20, 2012).

275 Id.

in practice.[276] Yet, there have been persuasive campaigns that have resulted in extraordinary overblocking. Cuomo's effort to push ISPs to censor Usenet news groups resulted in the providers simply dropping Usenet altogether, forfeiting a wide breadth of innocent content. That approach was also underinclusive—despite early reports, Cuomo did not demand that ISPs filter websites, or other methods by which child pornography is exchanged, meaning that most of the illegal content was unaffected.[277] ISPs have incentives to underblock, which generates less work and is less likely to antagonize customers. Content owners have incentives to overblock, since they do not bear the costs of treating lawful use as infringement. In short, persuasive blocking is at risk based on narrowness.

Thus, soft censorship often fares poorly on narrowness analysis.

D. (Il)legitimate

The methods of soft censorship outlined in Part I do not look legitimate under a process-based analytical framework. Pretext-based and payment-based filtering can be open about censorship, but persuasion-based regimes are often hopelessly opaque. All three methods lack transparency. Lastly, they tend to result in overblocking and underblocking, whether due to erroneous decisions, technical errors, or normative divergence between private content classifications and public goals. Soft censorship is deeply problematic from the perspective of the process-oriented legitimacy methodology.

III. LIMITS

Contrary to conventional scholarly wisdom, American federal and state governments are not precluded from Internet censorship. Rather, they are constrained in the methods that they can employ to prevent access to material online. Thus far, constitutional limitations based on First Amendment protections have blocked the state from deputizing intermediaries as censors.[278] However, this removes but one arrow from government's quiver. The other four tools—direct control over infrastructure, payment, pretext, and persuasion under pressure—remain viable options.

---

[276] The author represents computer security researcher Christopher Soghoian in a Freedom of Information Act suit against the Office of Management and Budget that seeks to compel release of documents related to the copyright alert system. *Soghoian v Office of Management and Budget*, No 1:11-cv-02203-ABJ (DDC 2012).

[277] See Danny Hakim, *Net Providers to Block Sites with Child Sex*, NY Times A1 (June 10, 2008).

[278] See Part I.C.

This Part explores the limits upon each of these four methods. It concludes with a paradox: the techniques permitted for government use have greater practical constraints, such as resource limitations, but far fewer of the procedural and structural checks on state power that are at the heart of American constitutionalism, particularly for core normative commitments such as free expression.

Limits come in multiple forms. Robust, easy to use tools that bypass censorship can be as effective a check upon governmental suppression of content as legal constraint.[279] Lawrence Lessig's New Chicago School model proposes four forces by which human behavior can be shaped.[280] Lessig notes that law is not the only way to constrain our actions; architecture (including software code), market forces, and social norms also play a role. A generation of Internet scholars has sought to apply Lessig's New Chicago School modalities to regulatory problems.[281] Yet, scholars have not acknowledged that these four forces are not merely ways of regulating—they also describe ways to *limit* regulation. Indeed, the New Chicago School taxonomy is best seen as not merely defining regulatory options but instead as a set of interfaces between government and individuals, and between individual citizens. This Part employs the New Chicago School modalities to catalog the constraints on soft censorship in the United States.

A. Code

Code appears capable of acting as a powerful brake on filtering. Determined users can bypass even complete network shutdowns. Egypt's citizens used international dial-up modem connections,[282] sat-

[279] See The Citizen Lab, *Everyone's Guide to By-Passing Internet Censorship: For Citizens Worldwide*, 17–27 (Toronto 2007), online at http://www.nartv.org/mirror/circ_guide.pdf (visited Sept 20, 2012). See also *Ashcroft v ACLU*, 542 US 656, 666 (2004). But see Erica Naone, *Censorship Circumvention Tools Aren't Widely Used*, Technology Review (MIT Oct 18, 2010), online at http://www.technologyreview.com/web/26574 (visited Sept 20, 2012).

[280] See Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv L Rev 501, 507 (1999).

[281] See, for example, Nicolas Suzor, *The Role of the Rule of Law in Virtual Communities*, 25 Berkeley Tech L J 1817, 1828 (2010) (cautioning that the four modalities do not imply that cyberspace self-governance is ideal); Lilian Edwards, *Coding Privacy*, 84 Chi Kent L Rev 861, 862–63 (2010) (arguing that the modality of architecture trumps the modality of law in cyberspace); Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 Georgetown L J 1, 4 (2006).

[282] See Steven Hoffer, *Egypt Internet Ban: 5 Ways the Protesters Are Beating the Blackout* (AOL Feb 1, 2011), online at http://www.yalibnan.com/2011/02/01/egypt-5-ways-the-protesters-are-beating-the-internet-blackout (visited Sept 20, 2012).

ellite access,[283] and Google's "Speak to Tweet" service to communicate,[284] despite the state's effort to sever connections with the wider Internet.[285] A team at the think tank New America Foundation is developing Commotion Wireless, which links wireless devices to build an ad hoc, mesh network to provide Internet access in case of such a disruption.[286] Indeed, the federal government has historically sponsored methods of bypassing Internet censorship, from providing free anonymized Internet access to Iranians[287] to sponsoring circumvention software,[288] to developing an "Internet in a suitcase,"[289] designed to permit activists to set up alternative networks.

There are already code-based ripostes to US soft censorship.[290] Activists have developed programs, such as the MAFIAAFire Redirector add-on for the Firefox browser, which circumvent domain name seizures.[291] Engineers have provided guides to using offshore DNS servers,[292] created alternative DNS resolution methods via P2P software,[293] and explained how to use Tor to bypass filtering.[294] In ad-

283 See Jeremy Kirk, *With Wired Internet Locked, Egypt Looks to the Sky* (PCWorld Jan 28, 2011), online at http://www.pcworld.com/article/218064/with_wired_internet_locked_egypt_looks_to_the_sky.html (visited Sept 20, 2012).

284 See Dawn Kawamoto, *Can Google Help Protesters Bypass the Egyptian Internet Shutdown?*, Daily Finance (AOL Feb 1, 2011), online at http://www.dailyfinance.com/2011/02/01/google-twitter-saynow-egypt-protests (visited Sept 20, 2012).

285 See Ryan Singel, *Report: Egypt Shut Down Net with Big Switch, Not Phone Calls*, Threat Level (Wired Feb 10, 2011), online at http://www.wired.com/threatlevel/2011/02/egypt-off-switch (visited Sept 20, 2012).

286 Open Technology Initiative, *Commotion Wireless* (New America Foundation), online at http://oti.newamerica.net/commotion_wireless_0 (visited Sept 20, 2012).

287 See OpenNet Initiative, *Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran* (May 5, 2004), online at http://opennet.net/advisories/001 (visited Sept 20, 2012).

288 See Nicole Gaouette and Brendan Greeley, *U.S. Funds Help Democracy Activists Evade Internet Crackdowns* (Bloomberg Apr 19, 2011), online at http://www.bloomberg.com/news/2011-04-20/u-s-funds-help-democracy-activists-evade-internet-crackdowns.html (visited Sept 20, 2012).

289 See Glanz and Markoff, *U.S. Underwrites Internet Detour around Censors*, NY Times at A1 (cited in note 233).

290 See, for example, Drew Wilson, *8 Technical Methods That Make the PROTECT IP Act Useless* (ZeroPaid Aug 7 2011), online at http://www.zeropaid.com/news/95013/8-technical-methods-that-make-the-protect-ip-act-useless (visited Sept 20, 2012).

291 Mozilla, *Add-Ons: MAFIAAFire Redirector* (Feb 13, 2012), online at https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector (visited Sept 20, 2012).

292 See, for example, Alucard, *The Simplest Way to Bypass a DNS Block* (The Simplest July 10, 2011), http://www.thesimplest.net/pc/simplest-way-bypass-dns-block (visited Sept 23, 2012).

293 See, for example, Shelly, *BitTorrent-Based DNS to Thwart US Domain Seizures* (ByteStyle Nov 10, 2010), online at http://bytestyle.tv/content/bittorrent-based-dns-thwart-us-domain-seizures (visited Sept 20, 2012).

dition, technical efforts to overcome censorship by authoritarian countries could just as readily be deployed to bypass American filtering. Telex, for example, deploys deep-packet inspection to detect embedded, encrypted codes in requests for ordinary Web pages that, in fact, direct the system to retrieve blocked ones.[295] Telex could be operated by ISPs in countries that permit access to material blocked in the United States, and American users could obtain this content without being either interdicted or detected.[296] Circumvention cuts all censors equally.

Responses via code, though, already partially achieve the government's ends by raising the costs of communication. Circumvention tools are more challenging to use than standard Internet software.[297] People who are not technologically adept are unlikely to work to employ proxy hosts, alternative DNS servers, or anonymizers. Put simply, there are far more people comfortable using a Mac than using Linux—and circumvention technology is akin to Linux in its complexity.

In addition, law can limit circumvention. The Department of Homeland Security demanded that Mozilla, developer of the Firefox browser, remove the MAFIAAFire Redirector from its repository, alleging it circumvented their seizure order.[298] With the advent of digital content and high-speed networks, the music and movie industries feared the wholesale piracy of their works.[299] At their behest, Congress passed Title I of the DMCA, which banned—including on pain of criminal penalties—the use or distribution of technologies that bypass access controls.[300] This ban on circumvention for the purpose of protecting copyright could easily be replicated to safeguard filtering. While a ban could not be perfectly enforced, it would further augment the cost of sidestepping Internet censorship.

---

294 See Drew Wilson, *Guide: How to Defeat US DNS Censorship (Using Tor)* (ZeroPaid Aug 1, 2011), online at http://www.zeropaid.com/news/94838/guide-how-to-defeat-us-dns-censorship-using-tor (visited Sept 20, 2012).

295 See Eric Wustrow, et al, *Telex: Anticensorship in the Network Infrastructure,* 1–12 (Michigan and Waterloo Aug 2011), online at https://telex.cc/pub/telex-usenixsec11.pdf (visited Sept 20, 2012).

296 See J. Alex Halderman, *Anticensorship in the Internet's Infrastructure*, Freedom to Tinker Blog (CITP July 18, 2011), online at https://freedom-to-tinker.com/blog/jhalderm/anticensorship-internets-infrastructure (visited Sept 20, 2012).

297 See Naone, *Censorship Circumvention* (cited in note 279).

298 See Harvey J. Anderson, *Homeland Security Request to Take Down MAFIAAFire Add-on*, HJA's Blog (May 5, 2011), online at http://lockshot.wordpress.com/2011/05/05/homeland-security-request-to-take-down-mafiaafire-add-on (visited Sept 20, 2012).

299 Litman, *Digital Copyright* at 122–45 (cited in note 237).

300 See 17 USC §§ 1201–04.

Technical tools can pierce technical walls. Yet, empirical data on use of circumvention software in authoritarian countries such as China strongly suggests that these measures are but a minor problem for censors.[301] Users are relatively easily kept within the bounds of censored platforms. The Internet is an environment of near-zero transaction costs.[302] Ironically, this disempowers code as a constraint: users have become accustomed to frictionless information environments and might be intolerant of the additional steps or slower speeds necessary to reach prohibited materials. Code, in short, has considerable theoretical promise to constrain censorship, and determined users will generally be able to reach blocked information. However, filtering raises the costs of content, making it highly effective for the majority of users and weakening code's constraint.

B. Law

Law checks censorship far less than expected.

Statutes and regulations, for example, often leave space for filtering. The DMCA immunizes service providers who block material on copyright grounds. Section 230(c)(2) of the Telecommunications Act of 1996[303] immunizes providers and users of interactive computer services for filtering content.[304] Even net neutrality rules, commonly hailed as a countermeasure to online blocking, permit filtering. The FCC's proposed net neutrality regulations, for example, protect only *lawful* content and permit network operators to engage in "reasonable network management."[305]

The US Constitution offers a second potential form of legal constraint. Yet, the Constitution might also empower filtering. ISPs are likely to object to net neutrality, for example, as unlawful interference with their right to make editorial decisions and, hence, to speak.[306] While this argument proves too much—it would mean, for example, that common carrier regulation of telephone companies is constitutionally prohibited[307] and that this defect has gone unnoticed for decades—it carries considerable rhetorical force after the Su-

301 See Naone, *Censorship Circumvention* (cited in note 279).

302 For a discussion of transaction costs, see generally R.H. Coase, *The Problem of Social Cost*, 3 J L & Econ 1 (1960).

303 Pub L No 104-104, 110 Stat 56, 138, codified at 47 USC § 230(c)(2).

304 See 47 USC § 230(c)(2).

305 *Preserving the Open Internet*, 25 FCCR at 17951–58 (cited in note 255).

306 See Susan Crawford, *Reading* Brown v. Entertainment Merchants Assn (June 27, 2011), online at http://scrawford.net/blog/reading-brown-v-entertainment-merchants-assn/1445 (visited Sept 20, 2012).

307 See 47 USC § 202(a).

preme Court's First Amendment decisions regarding data collection and speech regulation during October Term 2010.[308] Moreover, relevant precedent suggests that the state has considerable freedom in employing soft censorship. This subsection examines three potential constitutional limits: the public forum doctrine, the unconstitutional conditions doctrine, and the concept of the right of access inherent in some First Amendment cases.

1. Public forum doctrine.

The public forum doctrine presents one potential constraint on censorship. However, if the doctrine constrains at all, it does so weakly for three reasons: public forum theory is badly confused, the analytical emphasis on state intent at forum creation encourages censorship, and the forum concept is poorly suited to platforms that transmit information rather than storing it.

Speech requires space. American constitutional jurisprudence recognizes that speakers need a place where they can reach an audience; the classic example is publicly owned property such as parks and sidewalks.[309] There, the state may not regulate speech, save for content-neutral rules, unless "the restriction is 'necessary to achieve a compelling state interest . . . and narrowly drawn to achieve that end.'"[310]

The government can prescribe how loud a speaker may be but not the subjects upon which the speaker might declaim.[311] Spaces dedicated to public discourse are public fora.[312] Hard cases, such as whether a university's meeting rooms[313] or a school's interoffice mailboxes[314] constitute public fora, led to the development of the "limited public forum" doctrine,[315] whereby the government can limit speech to a particular purpose or subject (though it may not discriminate based on viewpoint even then).[316] If government-owned space does not fall within any of the public forum categories, then the state

---

308 See note 119.

309 See *Hague v Committee for Industrial Organization,* 307 US 496, 515 (1939).

310 Lyrissa Lidsky, *Public Forum 2.0*, 91 BU L Rev 1975, 1982 (2011), quoting *Perry Education Association v Perry Local Educators' Association*, 460 US 37, 45 (1983).

311 See *Ward v Rock Against Racism*, 491 US 781, 803 (1989) (holding that a municipal noise regulation applying to parks was a content-neutral restriction of speech).

312 See *Southeastern Promotions, Ltd v Conrad*, 420 US 546, 555 (1975) (describing a designated public forum).

313 See *Widmar v Vincent*, 454 US 263, 265 (1981) (discussing a university regulation against providing rooms for purposes of "religious worship or religious teaching").

314 See *Perry Education Association v Perry Local Educators' Association*, 460 US at 46–47.

315 See *Christian Legal Society v Martinez*, 130 S Ct 2971, 2985 (2010).

316 *Perry*, 460 US at 46–49 (noting the prohibition on viewpoint discrimination even in a limited public forum).

may restrict speech within that space, subject only to rational basis scrutiny and the requirement not to discriminate based on viewpoint.[317]

The public forum doctrine constrains minimally because it is strikingly unclear—the case law evades categorization or organization.[318] It is difficult to determine what constitutes a forum—when government property is a proper location for speech, and when it is not.[319] And the dividing lines that separate the various types of fora are elusive. A sidewalk is a public forum,[320] but not if it is owned by the Postal Service.[321] Funding for student organizations by public universities qualifies as a public forum,[322] and a school may not exclude religious student groups, unless they insist on admitting only those who agree with their precepts.[323]

These difficulties multiply in cyberspace. This is partly because cyberspace is largely privately owned[324]—there are fewer candidates for inclusion in the forum doctrine—and partly because much turns on governmental actions and intent at the creation of the alleged forum.[325] When the government establishes a platform for communications, it may limit its ability to regulate information exchanged on that platform. The level of constraint depends on the government's intent in opening the forum and the restrictions it imposes initially. Content limits operate as a one-way ratchet:[326] the state may relax its rules for expression, but not increase them, unless it is prepared to close the forum entirely. This encourages the state to impose restrictions on communication from the inception of a new communications space.[327]

---

317 See id at 46.

318 Criticism of the doctrine is legion. See Lidsky, 91 BU L Rev at 1976 n 3 (cited in note 310) (collecting critiques).

319 See Aaron H. Caplan, *Invasion of the Public Forum Doctrine*, 46 Willamette L Rev 647, 652–54 (2010).

320 See *Police Department of Chicago v Mosley*, 408 US 92, 94 (1972).

321 See *United States v Kokinda*, 497 US 720, 727 (1990).

322 See *Rosenberger v Rectors and Visitors of University of Virginia*, 515 US 819, 830 (1995).

323 See *Christian Legal Society*, 130 S Ct at 2993.

324 See Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 Berkeley Tech L J 1115, 1117 (2005).

325 See *Cornelius v NAACP Legal Defense and Education Fund, Inc*, 473 US 788, 799–800 (1985).

326 See *Katzenbach v Morgan*, 384 US 641, 656–58 (1966) (holding that Congress may ratchet up civil rights beyond what the Court has recognized, but it may not ratchet down these recognized rights).

327 See, for example, Culver City, *WiFi Access*, online at http://www.culvercity.org/en/Government/IT/WiFi/WiFiAccess (visited Sept 20, 2012) (stating "[i]t is not the intent of the City or the Agency to allow unlimited access to the entire Internet. Nor is it the intent of the City or Agency to create a traditional or limited public forum (i.e., a free speech arena)").

Evidence from efforts to create new collaborative spaces online may act as a cautionary tale for government officials. For example, President Obama launched an initiative to engage citizens about policy ideas to bolster transparency, participation, and collaboration in government, known as the Open Government Dialogue. Users could submit ideas online, comment on others' suggestions, and vote for initiatives they favored. The Dialogue, though, quickly degenerated into a debate over demands by some participants that President Obama release his birth certificate to the public.[328] Moreover, after voting on over four thousand submitted ideas had finished, three of the five most popular ideas were related to legalizing recreational drugs.[329] Thus, the Obama administration faced a hard choice: filter content unrelated to the Dialogue's purpose and face charges of censorship[330] or risk losing interested participants put off by irrelevant posts.[331] The twin problems of online trolling[332] and the economics of attention[333] can create a need for the government to moderate Internet communication. For the state to engage in constitutionally acceptable content management, it must establish a given space as a limited or nonpublic forum. Thus, the doctrinal structure of the public forum pushes publicly funded communications platforms toward content restrictions.

Lastly, the public forum concept is a poor fit with Internet access provisioning. As with broadcast spectrum regulation, scarcity is implicitly at the heart of the public forum doctrine.[334] Public school-

328 *How the Open Government Dialogue Got Slimed* (Federal Computer Week June 4, 2009), online at http://fcw.com/Articles/2009/06/08/buzz-open-government-dialogue-birth-certificate.aspx (visited Sept 20, 2012).

329 See *Open Government Dialogue* (Natl Academy of Pub Admin June 26, 2009), online at http://opengov.ideascale.com (visited Sept 20, 2012) (collecting 4,221 submitted ideas).

330 See David Farrar, *It Seems Obama's "Open Government Dialogue" Has Been Done in by Transparency* (Next Right June 4, 2009), online at http://thenextright.com/davidfarrar/it-seems-obamas-open-government-dialogue-has-been-done-in-by-transparency (visited Sept 20, 2012).

331 John S. Monroe, *Conversation Turns Ugly at the Open Government Dialogue* (Federal Computer Week June 3, 2009), online at http://fcw.com/Blogs/Insider/2009/06/open-government-dialogue-complaints.aspx (visited Sept 20, 2012) (asking "[i]s it possible to conduct a national online dialogue without having it waylaid by unrelated political agendas?").

332 See Cory Doctorow, et al, *Essential Blogging* 15 (O'Reilly 2002) (describing a commenter who ruins discussions with "persistent bile" as a troll).

333 See, for example, Michael H. Goldhaber, *The Attention Economy and the Net* (First Monday Apr 7, 1997), online at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/519/440 (visited Sept 20, 2012).

334 See *Red Lion Broadcasting Co v FCC*, 395 US 367, 394 (1969) (calling "scarce" the radio frequencies administered by the FCC and suggesting that the scarcity of this good empowers the government to regulate it in the public's best interest). See also Timothy Zick, Summum*, the Vocality of Public Places, and the Public Forum*, 2010 BYU L Rev 2203, 2207

teachers' interoffice mailboxes,[335] funding for student organizations,[336] and high school newspapers[337] are all rivalrous resources: they are made ineffective by overuse. The state may always impose some rules to address scarcity (such as time, place, and manner restrictions),[338] but for limited public fora, it can go further and deal with scarcity problems purposively. Thus, government can allocate the resources of a limited public forum to achieve the ends for which it was initially created.[339]

Scarcity, though, is only minimally relevant to government-provisioned Internet access. First, while all resources are theoretically limited, broadband is far less rivalrous than mailboxes or newspaper column-inches and is less scarce even than space in public parks. Thousands of users can share an Internet connection without interfering with each other, in contrast to a sidewalk. Second, content limitations are an inapt means of addressing bandwidth scarcity. A child sexual abuse image may be small, and a lawfully purchased movie download may be large. File size or bandwidth use are rough proxies, at best, for the state's goals. Content limits cannot masquerade effectively as responses to scarcity. The public forum doctrine is partly a response to concerns about competition for scarce expressive resources. It is not well suited to contexts such as Internet access, where scarcity is minimally relevant to the government's underlying normative concerns.

The public forum doctrine is unlikely to constrain soft censorship.[340] Courts have been deferential to content regulation when the government makes plain its intent to filter when it creates a new public forum and abuse of online spaces will push officials to do so. Finally, the doctrine's implicit emphasis on the scarcity of communications resources fits poorly with Internet access.

(observing that monuments, unlike speakers, interfere permanently with scarce public space and therefore public forum analysis is not appropriate for monuments).

335 See *Perry*, 460 US at 46–47.

336 See *Rosenberger*, 515 US at 830.

337 See *Hazelwood School District v Kuhlmeier*, 484 US 260, 268–69 (1988).

338 See *Ward*, 491 US at 803.

339 See Lidsky, 91 BU L Rev at 1986 (cited in note 310) (noting that the Court accepted as reasonable the rationales advanced by the University of California in upholding its all-comers policy).

340 See Rebecca Tushnet, *Domain and Forum: Public Space, Public Freedom*, 30 Colum J L & Arts 597, 599 (2007) (stating that the public forum doctrine's "practical utility to speakers is largely committed to legislative discretion").

2. Unconstitutional conditions doctrine.

Two forms of soft censorship—direct provision and public funding—offer users an implicit bargain: surf the Net for free in exchange for accessing only part of its content. The state confers a benefit in exchange for users giving up their right to access otherwise lawful material. This type of bargain is policed by the unconstitutional conditions doctrine, which defines when government can ask citizens to surrender constitutionally protected rights in exchange for benefits.[341] While the doctrine could constrain provision or payment filtering, it is unlikely to do so for three reasons: First, the Supreme Court has already approved payment with schools and libraries, although adult bypass requirements may present an avenue to challenge soft censorship.[342] Second, the doctrine even permits viewpoint discrimination when the state funds speech exclusion of entire categories of content, such as pornography, that are unlikely to draw objection.[343] Lastly, unconstitutional conditions cases are a nearly impenetrable murk[344]—scholarly analysis struggles to reconcile conflicting precedent and tends to surrender descriptive analysis in favor of prescriptive recommendations for future development. In short, the unconstitutional conditions doctrine is unlikely to significantly constrain soft censorship.

The problem of unconstitutional conditions arose with the advent of the welfare state.[345] As the government began to fund activities from the public fisc, it increasingly began to condition its largesse on recipients behaving in certain ways. For example, states accepting federal highway funds must establish a minimum age of twenty-one for the lawful consumption of alcohol,[346] and welfare recipients must permit

341 See Kathleen M. Sullivan, *Unconstitutional Conditions*, 102 Harv L Rev 1413, 1421–28 (1989).

342 See *United States v American Library Association, Inc*, 539 US 194, 210–12 (2002).

343 See David Cole, *Beyond Unconstitutional Conditions: Charting Spheres of Neutrality in Government-Funded Speech*, 67 NYU L Rev 675, 688–94 (1992).

344 Scholarly articles treat the doctrine with a combination of resignation and rage. See, for example, Philip Hamburger, *Getting Permission*, 101 Nw U L Rev 405, 440 (2007); Daniel A. Farber, *Another View of the Quagmire: Unconstitutional Conditions and Contract Theory*, 33 Fla St U L Rev 913, 926–29 (2006); Sullivan, 102 Harv L Rev at 1416 (cited in note 341); Richard A. Epstein, *Unconstitutional Conditions, State Power, and the Limits of Consent*, 102 Harv L Rev 4, 11 (1988) (noting that scholars recognize the importance of the doctrine, but they "make[] far less sense" when attempting to describe what the doctrine is or how it arises); Seth F. Kreimer, *Allocational Sanctions: The Problem of Negative Rights in a Positive State*, 132 U Pa L Rev 1293, 1297 (1984) (observing that the "difficulties raised by the indirect constitutional infringements" of unconstitutional conditions evade a coherent framework).

345 See Kreimer, 132 U Pa L Rev at 1294–98 (cited in note 344).

346 See *South Dakota v Dole*, 483 US 203, 208–09 (1987).

investigators to enter their homes to verify eligibility.[347] The unconstitutional conditions doctrine asks when government may achieve indirectly what it may not do directly. For example, the federal government could not bar a nonprofit corporation from lobbying; such a ban would violate the First Amendment.[348] However, the state can condition the organization's tax-exempt status on abstention from lobbying.[349] The challenge for the doctrine is to explain why.

Since the government cannot criminalize posting material harmful to minors on the Internet, may it make funding for Internet access contingent upon filtering such content? Yes, at least for schools and libraries. In 2000, Congress passed legislation, CIPA, requiring schools and libraries to install filtering software that blocked obscenity, child pornography, and materials harmful to minors as a condition of obtaining discounted Internet access or being eligible for certain government grants.[350] The Supreme Court upheld the law because Congress can spend funds only for the purposes for which they were authorized, libraries traditionally did not stock pornographic materials, and the funding condition did not distort libraries' traditional role.[351]

The Court's opinion dismissed CIPA's potential effects on access by adult library patrons to lawful, but filtered, materials by assuming that patrons could have filters disabled upon request.[352] Justice Anthony Kennedy's concurrence made this assumption explicit: in his view, failure to allow an adult to bypass the filter would create an as-applied challenge to CIPA.[353] Yet, the Court's opinion does not go so far, and CIPA states only that disabling filters is permitted, not mandated.[354] It is unclear whether CIPA operates only as a default setting for Internet filtering. This matters for soft censorship because most government-provided Internet access does not offer a means for bypassing filters. Users can petition, in some cases, to have specific sites unblocked, but that is a question of classification, not of access to otherwise off-limits

347 See *Wyman v James*, 400 US 309, 326 (1971); *Sanchez v County of San Diego*, 464 F3d 916, 930–31 (9th Cir 2006).

348 See *Citizens United v Federal Election Commission*, 130 S Ct 876, 913 (2010).

349 See *Regan v Taxation With Representation of Washington*, 461 US 540, 545 (1983).

350 See CIPA § 3601, 114 Stat at 2763A-337, codified at 20 USC § 6777. See also *American Library Association*, 539 US at 199.

351 *American Library Association*, 539 US at 211–12.

352 Id at 208–09.

353 Id at 214–15 (Kennedy concurring).

354 See CIPA § 1721(b)(6)(D), 114 Stat at 2763A-347, codified at 47 USC § 254(h)(5)(D); CIPA § 1721(a)(5)(D), 114 Stat at 2763A-344, codified at 20 USC § 9134(f)(3).

material.[355] The bypass question offers a narrow path to challenge soft censorship.

Even if a challenge were to overcome the CIPA precedent, the unconstitutional conditions doctrine generally permits government, when funding speech, to dole out support only to positions with which it agrees. Viewpoint discrimination is forbidden as direct regulation.[356] However, the government can choose to fund speech about childbirth, while forbidding speech about abortion.[357] Despite the Supreme Court's insistence that "the Government has not discriminated on the basis of viewpoint; it has merely chosen to fund one activity to the exclusion of another,"[358] the regulations at issue plainly funded one perspective and suppressed another. Doctors could inveigh against, but not in favor of, abortion if they wanted to accept Title X funding. Similarly, the federal civil service can permit employees to engage in nonpartisan politics, but ban partisan activities.[359] Public employees can be terminated for engaging in "insubordinat[e]" speech without constitutional offense.[360] Similarly, viewpoint limits (prohibiting pro-abortion speech) can be readily disguised as content ones (prohibiting discussion of abortion at all, but permitting discussion of childbirth).

The existing doctrine suffers at least two additional flaws relevant to censorship. First, it creates status quo bias. When abortion is lawful, pro-abortion speakers have less need for expression than anti-abortion ones: inertia benefits them. A ban on one type of content—speech about abortion—affects speakers differently based on their viewpoint.[361] Second, content classifications are multifaceted and malleable. An image of a naked woman whose body shows scars from torture can be classified as related to nudity, human rights,

---

355 Compare Utah Transit Authority, *Frequently Asked Questions* (cited in note 78) (providing no method to request unblocking) and Culver City, *WiFi Access* (cited in note 327), with Chesterfield County, *Acceptable-Use Policy* at 3.B (cited in note 73) (specifying process to request blocking or unblocking).

356 See, for example, *Schacht v United States*, 398 US 58, 63 (1970) (holding unconstitutional a statute that, in the context of a theatrical production, permitted praise of the armed forces but forbade criticism).

357 See *Rust v Sullivan*, 500 US 173, 203 (1991).

358 Id at 193.

359 *United States Civil Service Commission v National Association of Letter Carriers*, 413 US 548, 556, 562 (1973). While this might seem to be a content-based restriction, the emphasis on partisan political activity reveals it to be viewpoint based. See id at 555–56, 562.

360 *Connick v Myers*, 461 US 138, 141 (1983) (noting that the condition would be not to speak in insubordinate fashion).

361 See Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 Wm & Mary L Rev 189, 197–200 (1983); Martin H. Redish, *The Content Distinction in First Amendment Analysis*, 34 Stan L Rev 113, 128–29 (1981).

women, torture, or a combination of these categories.[362] If the image is tagged as nudity, though, a decision to block nudity content will prevent access to non-erotic material with important social value.[363] This problem is profound for technological censorship, which often relies on arbitrary administrative decisions or software algorithms to decide what material to block.[364]

Finally, the logic of the unconstitutional conditions doctrine is utterly unclear. A condition on funding for legal assistance to indigent clients that prohibited efforts to amend or challenge existing welfare law was held unconstitutional.[365] A condition on funding for family planning that prohibited efforts to counsel on abortion was held constitutional.[366] Aligning the cases in a consistent, coherent fashion is a Herculean task. Scholars have sought to characterize the decisions as turning on whether a particular restriction is a threat or an offer,[367] or as establishing default rules for constitutional rights,[368] or as defining structural limits beyond which government may not operate.[369] The most likely answer to the tangle of seemingly contradictory opinions, though, is Philip Hamburger's statement that "the Court has been engaged in exploratory guesswork."[370] The sheer uncertainty of the doctrine makes it unlikely to constrain soft censorship.

3. Right of access.

A final possibility is that law could constrain censorship via a First Amendment right to access information. This option relies on an inchoate theory of audience-oriented interests present in First Amendment jurisprudence.[371]

---

362 See OpenNet Initiative, *Saudi Arabia* (cited in note 82).

363 See id.

364 See, for example, Marjorie Heins and Christina Cho, *Internet Filters: A Public Policy Report* 2–4 (Brennan Center for Justice 2001).

365 *Legal Services Corp v Velazquez*, 531 US 533, 543 (2001).

366 *Rust*, 500 US at 203.

367 See, for example, Kreimer, 132 U Pa L Rev at 1300–01 (cited in note 344) (observing that threats put the citizen in a worse position because of the exercise of a constitutional right while offers expand the citizen's range of options).

368 See, for example, Farber, 33 Fla St U L Rev at 931–40 (cited in note 344) (moving the inquiry from the rights themselves to flaws in the bargaining process between the government and the citizen).

369 See, for example, Philip Hamburger, *Unconstitutional Conditions: The Irrelevance of Consent*, 98 Va L Rev 479, 487 (2012) (arguing that the separation of powers acts equally as a constraint upon direct government action and unconstitutional conditions).

370 Id at 488.

371 See, for example, *Stanley v Georgia*, 394 US 557, 564 (1969) (stating "the Constitution protects the right to receive information and ideas"); *Lamont v Postmaster General*, 381 US

Freedom of expression means more than simply a right to speak; it implies limits on government's ability to impede listeners who wish to hear that speech.[372] Audience-oriented reasoning can act as a proxy for speakers' interests, protect those of listeners, or both. Often, listener and speaker interests coincide, and the Court is able to invoke both without careful delineation. For example, the Court invalidated a law that mandated union organizers register with the government before seeking to enroll workers in the union, holding that both the organizers' right to speak and the workers' right to hear them had been violated.[373]

Difficulties arise when speech interests conflict: the listener does not want to receive information,[374] or the speaker does not wish to convey a message[375] or inform particular listeners,[376] or an intermediary objects to transmitting a particular speaker's information.[377] Speakers tend to win such conflicts.[378] Audience interests may help tip the balance when the Court must select among competing speakers' interests. For example, radio broadcasters have expressive interests at stake in selecting material to transmit, yet the Supreme Court upheld a requirement that they broadcast involuntarily the replies of people attacked during discussions of issues of public importance.[379] There, the Court held that

301, 307 (1965) (noting that, regarding a postal regulation of communist propaganda, "the addressee in order to receive his mail must request [it] . . . [which is] an unconstitutional abridgment of the addressee's First Amendment rights"); *Martin v City of Struthers*, 319 US 141, 143 (1943) (arguing "[t]he right of freedom of speech and press . . . necessarily protects the right to receive [literature]").

372 See, for example, *Reno v ACLU*, 521 US 844, 865–67 (1996); *Turner Broadcasting System, Inc v FCC*, 512 US 622, 641 (1994).

373 *Thomas v Collins*, 323 US 516, 534 (1945).

374 See, for example, *National Socialist Party of America v Village of Skokie*, 432 US 43, 43 (1977) (discussing an ordinance forbidding Nazis from marching through Skokie, Illinois); *Martin*, 319 US at 147–48.

375 See, for example, *Wooley v Maynard*, 430 US 705, 709–10 (1977) (examining a New Hampshire statute preventing drivers from obscuring the "Live Free or Die" motto on New Hampshire license places); *Speiser v Randall*, 357 US 513, 515–16 (1958) (describing a tax provision that required an oath of loyalty before tax exempt status was granted); *West Virginia State Board of Education v Barnette*, 319 US 624, 632–33 (1943) (discussing whether a school may compel students to salute the flag).

376 See, for example, *Richmond Newspapers, Inc v Virginia*, 448 US 555, 576 (1980) (holding that a criminal trial must be open to the public).

377 See, for example, *Turner*, 512 US at 630–32 (discussing "must-carry provisions" requiring carriage of local broadcast stations on cable systems); *Miami Herald Publishing Co v Tornillo*, 418 US 241, 244 (1974) (describing a newspaper's refusal to allow a politician to reply to its adversarial editorials in its own pages).

378 See *Texas v Johnson*, 491 US 397, 420 (1989) (holding that as between flag burners and those that do not want to see flags burned, the burners' right prevail); *Cantwell v Connecticut*, 310 US 296, 309–11 (1940) (holding that as between an offensive speaker and listeners on the street, the speaker's right prevails).

379 *Red Lion*, 395 US at 375.

the rights of the listeners and the disparaged speakers outweighed those of the broadcasters.[380] Generally, though, recipients' interests are either marginal or unexplored. The Supreme Court invalidated a similar right of reply for print media, holding that a newspaper's right to select what it expressed trumped a claimed right of access by a political candidate who had been criticized by the paper.[381] The Court focused on the competing speakers' interests; the newspaper's readers were kept in the background, relevant only insofar as they represented the ultimate beneficiaries of the First Amendment's safeguards.[382]

First Amendment intervention on behalf of information consumers typically requires special conditions, such as resource scarcity,[383] difficult-to-reach populations,[384] or quasi-state functioning by private actors who block access to speech.[385] Scarcity, as discussed in Part III.B.1, is not applicable to broadband access. In addition, scarcity is conceptually odd: government is allowed to intervene most where the opportunity to bypass state mandates is least. Second, most Internet consumers are not peculiarly difficult to reach. While they may have few options for broadband access, limitations from market structure alone rarely create cognizable First Amendment harm.[386] Lastly, despite attempts to classify actors such as Google as operating in near-governmental fashion, there is no real fear that the search engine or other Internet intermediaries operate like virtual governments.[387] Unlike company towns such as the one at issue in *Marsh v Alabama*,[388] Google cannot effectively cut off its users' access to information—Bing, Yahoo!, and Dogpile are but a few clicks away. The sharp decrease in transaction costs created by the Internet means that switching intermediaries is relatively easy.

The indirectness of soft censorship limits challenges based on a First Amendment right-of-access claim. Persuasion-based methods

---

380 Id at 390.

381 *Tornillo*, 418 US at 258.

382 See, for example, id at 248–50.

383 *Red Lion*, 395 US at 394 .

384 See *Turner*, 512 US at 663; *PruneYard Shopping Center v Robins*, 447 US 74, 78 (1980).

385 See *Marsh v Alabama*, 326 US 501, 502 (1946) (describing the efforts of a company town to prevent the distribution of pamphlets on its premises).

386 See, for example, *Tornillo*, 418 US at 248–54 (noting the dangers of media concentration but striking down a right-of-reply statute—which would have helped ensure balanced newspaper coverage—anyway).

387 See *KinderStart.com, LLC v Google, Inc*, 2007 WL 831811, *1 (ND Cal); *Search King, Inc v Google Technology, Inc*, 2003 WL 21464568, *2 (WD Okla).

388 326 US 501 (1946).

evade review because there is, formally, no state action[389]—censorship occurs through decisions by private firms. Right-of-access challenges are cognizable for payment-based censorship, but the Supreme Court's decision on CIPA resolves them in favor of the state. Direct governmental provision of Internet access is treated like payment. Attacks on pretext-based censorship have the greatest promise, but here they face judicial skepticism about the merits of the banned speech,[390] as well as procedural hurdles that make challenges costly and time consuming.[391] In short, while the First Amendment does protect a user's right to receive information, this particular safeguard functions only weakly as a constraint on soft censorship.

4. Law's limits.

Soft censorship seems like it would be limited by law. Yet law's grip on these methods of information control is oddly weak. Doctrinal confusion, lack of state action, and statutory lacunae for filtering all confer considerable freedom upon a government that seeks to censor indirectly.

C. Markets

In theory, market mechanisms could limit soft censorship. ISPs could reject government attempts to push them to censor,[392] or run alternative DNS servers to overcome domain name seizures,[393] or subsidize connections for eleemosynary institutions such as public schools and libraries.[394] Yet market constraints largely fail because American markets for Internet access offer but few choices to consumers. Not only does this reduce alternatives for market exit if one ISP filters but also it makes the government's job easier by decreasing the number of firms the government must coordinate to make soft censorship effective.

---

389 See *CBS v Democratic National Committee*, 412 US 94, 140–41 (1973) (finding no state action in the FCC refusal to require broadcasters to accept editorial advertising).

390 See Puerto 80 Order at *4.

391 See, for example, Terry Hart, *Rojadirecta: Barking Up the Wrong Tree?* (Copyhype Aug 9, 2011), online at http://www.copyhype.com/2011/08/rojadirecta-barking-up-the-wrong-tree (visited Sept 20, 2012) (describing the procedure to challenge domain-name seizure).

392 In Britain, a few ISPs have refused to adopt the Cleanfeed filtering system voluntarily. See Christopher Williams, *Small ISPs Reject Call to Filter Out Child Abuse Sites* (Register Feb 25, 2009), online at http://www.theregister.co.uk/2009/02/25/iwf_small_isps (visited Sept 20, 2012).

393 See Wilson, *8 Technical Methods* (cited in note 290).

394 See, for example, Nathan Olivarez-Giles, *Google Picks City for Fast Internet*, LA Times B2 (Mar 31, 2011) (describing Google's announcement to provide free broadband access to some Kansas City schools).

Pretext-based methods are the most difficult for market solutions to respond to. For example, imagine that the government seizes a domain name because its website contains content supportive of the communist regime in Cuba.[395] The domain name registrar, such as VeriSign (for .com domains), will redirect requests for that domain to a site of the government's choice.[396] Since VeriSign controls the .com registry, all DNS servers rapidly reflect the post-seizure change.[397] While an ISP could override VeriSign's change by editing its DNS records to reflect the pre-seizure mapping of the domain name, this involves incurring administrative overhead for, at most, minimal financial reward. Seth Kreimer has documented the incentive problems that occur when intermediaries must defend marginal speech interests,[398] and when these are compounded with the complications of maintaining nonstandard DNS information,[399] it is likely that access providers will not bother. Thus, a market for uncensored access is unlikely to occur when the government employs pretext-based moves, especially when the state uses the distributed DNS architecture to create transaction costs for resistance.

Market competition could also impede censorship efforts that rely on persuasion. For example, the federal government partnered with content owners to press ISPs such as Time Warner Cable to engage in technological efforts to impede copyright infringement; Time Warner customers might flee this arrangement by turning to alternative providers, such as CenturyLink, who are not part of the agreement.[400] Consumers could vote for freedom with their feet, moving from censored providers to uncensored ones—or, at least, demand-

---

395 See Liptak, *A Wave of the Watch List*, NY Times at A16 (cited in note 14).

396 See dL, *The Background Dope on DHS Recent Seizure of Domains* (Libérale et Libertaire Nov 28, 2010), online at http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains (visited Sept 20, 2012) (describing the technical details of domain-name seizures).

397 See Sean Michael Kerner, *VeriSign Accelerates DNS*, Enterprise Apps Today (IT Business Edge Sep 9, 2004), online at http://www.enterpriseappstoday.com/marketing/article.php/3406171/VeriSign-Accelerates-DNS.htm (visited Sept 20, 2012); Microsoft, *How DNS Works*, TechNet (Mar 28, 2003), online at http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx (visited Sept 20, 2012).

398 Kreimer, 155 U Pa L Rev at 27–29 (cited in note 25).

399 See Cricket Liu and Paul Albitz, *DNS and BIND* 136–39, 143–47 (O'Reilly 5th ed 2006).

400 For evidence of competition between CenturyLink and Time Warner, see Phillip Dampier, *CenturyLink Invests to Reinvent Themselves: Prism IPTV/25Mbps Service Arrives* (Stop the Cap! Feb 16, 2011), online at http://stopthecap.com/2011/02/16/centurylink-invests-to-reinvent-themselves-prism-iptv25mbps-service-arrives (visited Sept 20, 2012). For evidence that CenturyLink is not a party to the deal between ISPs and content owners, see *Memorandum of Understanding* at *21–23 (cited in note 223) (listing Time Warner Cable, but not CenturyLink, as a participant).

ing a discount for censored access. However, market competition has limited force in constraining persuasive soft censorship, for three reasons.

First, most consumers have, at best, two options for residential broadband service: the local cable operator and the local telephone company (via DSL). A recent FCC report on high-speed Internet access, which includes data through June 2010, found that 60 percent of residential broadband customers had only one provider who could offer 6 Mbps access, 22 percent had two providers, and 15 percent had none.[401] For slower broadband (3 Mbps downstream and 768 Kbps upstream), 23 percent of such customers had only one provider, 47 percent had two, and 3 percent had none.[402] Thus, for 6 Mbps broadband, 82 percent of consumers had two choices or fewer, and for slower broadband, 70 percent had at most two options.[403] This is not robust competition.

Second, consumers might have difficulty detecting filtering, particularly when it is implemented subtly. For example, Comcast slowed, but did not block, BitTorrent traffic on its network; many users assumed that network congestion or other technical problems were to blame.[404] Similarly, some ISPs covertly redirect users' search queries, so a consumer entering "Dell" into her browser's search bar would be sent to a site chosen by the ISP instead of receiving a page of Google search results.[405]

Lastly, ISPs might have incentives to filter that overcome any revenue loss from consumers who prefer uncensored access. Some providers, such as Comcast, also own content companies, such as the television and movie company NBCUniversal.[406] These companies internalize the benefits of blocking, such as filtering content that infringes on their IP rights. Others offer high-margin services, such as long-distance telephone calls, that are at risk of competition from online services such as Vonage.[407] Blocking competitors is profitable.

---

401 Industry Analysis and Technology Division, Wireline Competition Bureau, *Internet Access Services: Status as of June 30, 2010* 7 (FCC Mar 2011), online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-305296A1.pdf (visited Sept 20, 2012).

402 Id.

403 See id.

404 See Reardon, *Comcast Denies Monkeying* (cited in note 256).

405 See Jim Giles, *US Internet Providers Hijacking Users' Search Queries*, Tech (New Scientist Aug 10, 2011), online at http://www.newscientist.com/article/dn20768-us-internet-providers-hijacking-users-search-queries.html?full=true (visited Sept 20, 2012).

406 Columbia Journalism Review, *Who Owns What: Comcast* (July 23, 2011), online at http://www.cjr.org/resources/?c=comcast (visited Sept 20, 2012).

407 See, for example, Consent Decree, *In the Matter of Madison River Communications, LLC*, 20 FCCR 4295, 4297 (2005).

Moreover, as ISPs deploy technologies such as deep-packet inspection, they may be forced to negotiate arrangements with content providers that mandate filtering, as using deep-packet inspection may forfeit statutory safe harbors for copyright infringement.[408] Market competition will check censorship only if it is remunerative to do so. There are reasons to doubt that the rewards are currently sufficient.[409]

A final market alternative conceives of different governments creating unfiltered Internet access markets—payment as constraint, not censorship. For example, states could provide funds to schools and libraries that agreed not to censor or could provide unfiltered access directly. Some state-based entities, such as individual libraries, already choose this route. For example, libraries in Berkeley, California, do not filter the Internet,[410] relying on state funding as a consequence of forgoing federal E-Rate monies. In effect, California subsidizes the Berkeley libraries' decision not to censor.

There are at least four challenges with state-based open Internet access, though. First, state budgets are increasingly constrained by declining tax revenues during a recession and by growing pension obligations.[411] Internet access is not likely to be a significant priority. Second, diversity cuts both ways: some states will augment censorship rather than reduce it.[412] Third, open access at the local level will mean little if upstream access is filtered. The private bargains emerging between content providers and major ISPs do not appear to admit of override in the case of provision to public entities—government must buy access on the same terms as any other customer.[413] Lastly, the federal government maintains trump cards: its ability to override state decisions through contrary legislation, relying on

408 See Bridy, 89 Or L Rev at 103–07 (cited in note 31) (explaining that by taking an active role in monitoring and managing Internet traffic, ISPs risk losing the protection they were afforded on the basis that they operate as "dumb pipes").

409 See Kreimer, 155 U Pa L Rev at 35–40 (cited in note 25).

410 Berkeley Public Library, *Policies*, online at http://www.berkeleypubliclibrary.org/about_the_library/policies.php (visited Sept 20, 2012).

411 See generally Elizabeth McNichol, Phil Oliff, and Nicholas Johnson, *States Continue to Feel Recession's Impact* (Center on Budget and Policy Priorities May 24, 2012), http://www.cbpp.org/files/2-8-08sfp.pdf (visited Sept 20, 2012).

412 See, for example, Utah Code Ann § 9-7-215 to -216 (permitting libraries to restrict access to content in addition to obscenity, child pornography, and material harmful to minors).

413 See generally *Memorandum of Understanding* (cited in note 223).

the Supremacy Clause[414] and its capacity to buy adherence to its preferences through funding mandates.[415]

The combination of the limited set of broadband provider options generally available to American broadband consumers, the increasing incentives that providers have to filter, and the challenges of government-provided uncensored access means that market mechanisms constrain censorship weakly at best.

D. Norms

Norms, too, falter as a constraint on soft censorship. They are but a weak check for three reasons: framing problems, collective action problems, and heterogeneous preferences. First, norms depend critically upon framing. Limits on Internet content, though, begin at the thin edge of the wedge: there are few willing to lobby for access to material that infringes copyright, or to child pornography.[416] Opponents of filtering are at a perceptual disadvantage—they must oppose censorship on principle[417] while those who favor it will focus on the underlying content and the harms it generates.[418] In addition, censorship is rarely described as such. Instead, efforts to block access to information are described as enforcing property rights,[419] stopping piracy,[420] protecting public safety,[421] or safeguarding children.[422] Restricting access to disfavored content is framed to align with important social goals, and suggestions that blocking will expand are

414 See, for example, *Crosby v National Foreign Trade Council*, 530 US 363, 372–73 (2000).

415 See, for example, *Dole*, 483 US at 210.

416 See Rick Falkvinge, *The Copyright Lobby Absolutely Loves Child Pornography* (TorrentFreak July 9, 2011), online at http://torrentfreak.com/the-copyright-lobby-absolutely-loves-child-pornography-110709 (visited Sept 20, 2012).

417 See, for example, Nicole A. Ozer, *No Such Thing as "Free" Internet: Safeguarding Privacy and Free Speech in Municipal Wireless Systems*, 11 NYU J Legis & Pub Pol 519, 551–54 (2008).

418 See, for example, Preston, 2007 BYU L Rev at 1471–75 (cited in note 210) (describing in detail the amount of pornography available to children on the Internet).

419 See, for example, Chris Dodd, *MPAA Welcomes World Leaders' Commitment to Protecting Creative Content from Theft*, MPAA Blog (May 27, 2011), online at http://blog.mpaa.org/BlogOS/2011/05/default.aspx (visited Sept 20, 2012).

420 Victoria Espinel, *Working Together to Stop Internet Piracy*, The White House Blog (July 7, 2011), http://www.whitehouse.gov/blog/2011/07/07/working-together-stop-internet-piracy (visited Aug 6, 2012).

421 Brian Shields, *BART Says Riders Have No Right to Free Speech Inside Fare Gate as Officials Prepare for Planned Afternoon Protests* (KRON 4 News Aug 15, 2011), online at http://www.kron4.com/Article.aspx?ArticleID=1731 (visited Sept 20, 2012) (citing the "[c]onstitutional right to safety" in defending filtering).

422 See, for example, CP80, *Medical & Social Impacts*, online at http://www.cp80.org/impacts/medical_social (visited Sept 20, 2012).

generally dismissed as slippery slope concerns that will not materialize in practice.[423]

Next, a collective action problem hampers the effectiveness of norms as a constraint on soft censorship. Even if censorship is widely disliked, few people feel strongly enough, or have a sufficient stake in content filtering, to act. Inaction multiplies: opponents may feel that their views are idiosyncratic since few others take action on the issue.[424] While opponents may coalesce into small blocs of revolutionaries, such as the "hacktivist" groups Anonymous or Lulzsec, their influence is likely to be scant.[425]

Lastly, norms regarding the material blocked by filtering are variegated. IP infringement, such as the unlawful downloading and sharing of copyrighted music and movies, is widespread.[426] The music and movie industries frequently bemoan the lack of social sanctions for such conduct and have engaged in a series of educational campaigns designed to shift views, particularly among younger users.[427] Similarly, indecent and obscene content—particularly pornography—is widely consumed, although it is also the target of social disapprobation in some quarters.[428] Attitudes are mixed, if not contra-

---

[423] But see *Twentieth Century Fox Film Corp v British Telecommunications PLC*, [2011] EWHC 1981 (Ch) *3–4 at ¶¶1–4, *67 at ¶ 204 (holding, in the High Court of England and Wales Chancery Division, that British Telecom must block a file-sharing site using Cleanfeed technology initially deployed to filter child pornography).

[424] For the collective action problems involved in organizing large or hidden groups, see Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* 165–67 (Harvard 1965).

[425] See, for example, Paul McDougall, *Amazon Cloud Withstands WikiLeaks Attack*, Security (InformationWeek Dec 9, 2010), online at http://www.informationweek.com/news/security/attacks/228800075 (visited Sept 20, 2012).

[426] The International Federation of the Phonographic Industry (IFPI) claims that 95 percent of music downloads are unlawful. IFPI, *IFPI Digital Music Report 2009: Key Statistics* *2, online at http://www.ifpi.org/content/library/DMR2009-key-statistics.pdf (visited Sept 20, 2012). The research firm Envisional (commissioned by NBCUniversal) estimated that nearly one quarter of global Internet traffic is comprised of material that infringes IP rights. Envisional, *Technical Report: An Estimate of Infringing Use of the Internet* 2 (Jan 2011), online at http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf (visited Sept 20, 2012).

[427] See, for example, *CampusDownloading Video*, online at http://www.campusdownloading.com/dvd.htm (visited Sept 20, 2012); MPAA, *Governments around the World Take a Stand for Creators, Consumers*, Public Awareness Campaigns, online at http://www.mpaa.org/contentprotection/public-service-announcements (visited Sept 20, 2012); MPAA, *So You Got a Notice. . . .*, Respect Copyrights, online at http://www.respectcopyrights.org (visited Sept 23, 2012). See Peter K. Yu, *P2P and the Future of Private Copying*, 76 U Colo L Rev 653, 758–63 (2005).

[428] See, for example, Gordon B. Hinckley, *A Tragic Evil among Us* (Church of Jesus Christ of Latter-day Saints Nov 2004), online at http://www.lds.org/ensign/2004/11/a-tragic-evil-among-us (visited Sept 20, 2012); Focus on the Family, *Pornography*, Social Issues, online at http://www.focusonthefamily.com/socialissues/social-issues/pornography.aspx (visited Sept 20,

dictory: socially conservative Utah, for example, is the largest per capita consumer of pornographic Internet content, as measured by the number of adult service subscriptions per broadband user.[429] Views on Internet gambling are more mixed,[430] while filtering content that represents a perceived threat to national security enjoys broad popularity.[431] Thus, norms regarding blocking access vary greatly depending on the material at issue. This heterogeneity undercuts the strength of norms as a constraint, since they will wax or wane depending upon the context. Even people opposed to censorship in some circumstances might not have a principled objection to it: they dislike the blocking of certain content, rather than censorship as a method. Thus, careful targeting of disfavored content by the state can further undercut norms-based constraints.

Careful framing by censors, collective action problems, and heterogeneous preferences regarding censorship all weaken the potential constraining power of norms on filtering.

E. Paradox

This Part envisions the New Chicago School's modalities as means of constraining regulation, not merely implementing it. It reviews each method in the context of soft censorship and finds, surprisingly, that they check content blocking by the state minimally, if at all. This is counterintuitive: Supreme Court jurisprudence on hard censorship, and American values regarding free expression, suggest that the government would be limited in attaining censorial ends, regardless of the means employed. Yet this is not so. Checks on government are practical rather than structural or doctrinal; they depend upon the state's ability to fund censorship, or to push

2012); Stop Porn Culture!, *Mission Statement*, online at http://stoppornculture.org/mission (visited Sept 20, 2012).

[429] See Benjamin Edelman, *Red Light States: Who Buys Online Adult Entertainment?*, 23 J Econ Persp 209, 217 (Winter 2009) (listing Utah with 5.47 subscriptions per 1,000 broadband users). See also Ewen Callaway, *Porn in the USA: Conservatives Are Biggest Consumers* (ABC News Feb 28, 2009), online at http://abcnews.go.com/Technology/Business/story?id=6977202&page=1#.T9axLdX2anw (visited Sept 20, 2012).

[430] See, for example, *Online Gambling Debate: Barney Frank vs. Spencer Bachus*, Opinion (US News June 1, 2009), online at http://www.usnews.com/opinion/articles/2009/06/01/online-gambling-debate-barney-frank-vs-spencer-bachus (visited Sept 20, 2012); Ryan D. Hammer, Note, *Does Internet Gambling Strengthen the U.S. Economy? Don't Bet on It*, 54 Fed Comm L J 103, 104 (2001).

[431] See, for example, Marist College Institute for Public Opinion, *McClatchy-Marist Poll: National Survey December 2010* 23–24, online at http://maristpoll.marist.edu/wp-content/misc/usapolls/US101202/McClatchy/McClatchy_Marist%20Poll_National%20Survey_December%2010,%202010.pdf (visited Sept 20, 2012) (showing support for prosecuting those who publish confidential government documents on sites such as WikiLeaks).

intermediaries to perform it, rather than on careful legal justification of its efforts. This freedom of action is disturbing in light of the legitimacy analysis of Part II—government has the greatest freedom to act where its methods are least legitimate. The next Part proposes that if censorship is to occur, it should be performed through specific legislation that realigns Internet blocking with the historical treatment of prior restraint.

IV. HOW TO SILENCE THE TOWN CRIER

America, like most other countries, has moved to counteract disfavored online material not merely through punishing consumption after the fact but also by preventing access to it initially. Filtering via legal mandates to intermediaries was set back when the Supreme Court invalidated first the CDA and then COPA, and government provides too little Internet access for significant blocking directly. In response, government regulators turned to soft censorship. This Article argues that soft censorship is less legitimate than hard methods. It next proposes that *if* interdicting online content is normatively desirable—a point I do not concede—then America should return to legal filtering mandates, but ones that are significantly more protective of our shared commitment to free expression.

Counterintuitively, this means that proposed filtering legislation, such as the PROTECT IP Act and the Stop Online Piracy Act[432] (SOPA), is a step in the right direction. While the PROTECT IP Act and SOPA suffer significant shortcomings, such as their focus on DNS filtering,[433] grant of filtering power to private plaintiffs,[434] and lack of procedural protections,[435] they are admirably open and transparent about the censorship they seek to impose, and the process of considering the Acts in Congress scores well on accountability measures.[436] This Part first evaluates filtering as a potential regulato-

---

[432] HR 3261, 112th Cong, 1st Sess, in 157 Cong Rec H 7133 (Oct 26, 2011), online at http://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf (visited Sept 20, 2012).

[433] See PROTECT IP Act § 3(d)(2)(A), in 157 Cong Rec at S 2938 (cited in note 110).

[434] See PROTECT IP Act § 4(a)(1), in 157 Cong Rec at S 2938 (cited in note 110).

[435] See Mark Lemley, David S. Levine, and David G. Post, *Don't Break the Internet*, 64 Stan L Rev Online 34, 36 (2011), http://www.stanfordlawreview.org/sites/default/files/online/articles/64-SLRO-34_0.pdf (visited Sept 20, 2012).

[436] Ironically, Senator Ron Wyden's "hold" on the Act, which likely blocked its adoption, seems problematic from an accountability perspective. See Ron Wyden, *Wyden Places Hold on PROTECT IP Act*, Press Releases (May 26, 2011), online at http://wyden.senate.gov/newsroom/press/release/?id=33a39533-1b25-437b-ad1d-9039b44cde92 (visited Sept 20, 2012).

ry method. Then, it turns to the key components that a filtering statute must include to meet both constitutional and legitimacy concerns. It concludes by proposing to realign treatment of online censorship with American approaches to prior restraint generally.

A. In Praise of Filtering

I have previously argued that Internet filtering's legitimacy depends upon the processes involved in its creation and implementation. This framework implicitly concedes that some censorship may be permissible.[437] It may also be necessary. Filtering is a technological response to the permeability of geographic borders in Internet communication.[438] With analog communication, such as printed matter, governments can control what enters their jurisdictions with some success. Once illicit material enters their polity, they can interdict it at the point of distribution to consumers. Law enforcement can seize counterfeit music CDs[439] or block obscene materials from flowing through the postal service.[440] Online, governments can attack unlawful content when it is resident on computers within their jurisdiction. However, it is difficult to prevent transport of material from outside the United States to consumers within the country. Online borders are highly porous. Filtering seeks to plug some of those holes.

Conceptually, it is difficult to object to blocking access to material that users could not lawfully possess and that could be removed if it were hosted on servers within US control. A site hosting child pornography, obscenity, or true threats[441] could be lawfully removed from domestic servers. Objections to Internet filtering tend to concentrate on mistakes, and their collateral effects. Censorship opponents correctly critique overblocking and underblocking that plague most filtering systems,[442] and attack the lack of transparency of many cen-

437 See Bambauer, 59 Duke L J at 386–88 (cited in note 32).

438 See Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* 92 (Oxford 2006).

439 See William C. Thompson Jr, Comptroller, *Bootleg Billions: The Impact of the Counterfeit Goods Trade on New York City* 12–13 (Office of Comptroller, City of New York Nov 2004), online at http://www.comptroller.nyc.gov/bureaus/bud/04reports/Bootleg-Billions.pdf (visited Sept 20, 2012).

440 See 18 USC § 1461. See also *Roth v United States*, 354 US 476, 492 (1957).

441 See, for example, *Planned Parenthood of the Columbia/Willamette, Inc v American Coalition of Life Activists*, 290 F3d 1058, 1086–88 (9th Cir 2002).

442 See, for example, Gordon Hull, *Overblocking Autonomy: The Case of Mandatory Library Filtering Software*, 42 Continental Phil Rev 81, 91–93 (2009); Ozer, 11 NYU J Legis & Pub Pol at 554–55 (cited in note 417).

sorship procedures.[443] These problems are real. But, they are not an objection to censorship itself. They are an objection to *badly done* censorship.

Filtering, like any law enforcement mechanism, is inevitably imperfect. Deciding whether to turn to filtering as a response to unlawful content necessarily involves comparing its costs to its benefits. This is more than a quantitative exercise: the American normative commitment to the free flow of information weighs heavily in the calculus.[444] There are other costs beyond the loss of open communication, such as the overblocking of innocent content, the administrative cost of determining whether online material is lawful, the judicial costs from challenges to filtering, the potential harm to US efforts to guarantee Internet freedom abroad, and the expenses of implementation for ISPs.[445] Yet, there are countervailing benefits as well: greater equality of treatment for domestic and foreign content providers, reduced access to unlawful material, and potential decreased costs of other enforcement methods that address unlawful content. The outcome of this weighing is not certain. What this Article makes clear is that the underlying policy question of whether to censor is open since soft censorship is not significantly constrained by law or other methods.

The legitimacy of Internet censorship depends importantly on the design and implementation of decisions about what content to block. Here, the border-enforcement aspect of filtering presents a difficult problem.[446] Filtering targets content hosted on sites beyond American territory.[447] The authors or owners of that content, though, might lack the resources or incentive to defend their rights in the

---

443 See, for example, Nart Villeneuve, *The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace* (First Monday Jan 2, 2006), online at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227 (visited Sept 20, 2012).

444 See generally Jane Yakowitz Bambauer, *The New Intrusion*, 88 Notre Dame L Rev (forthcoming 2012) (defending free expression as a key element in privacy tort analysis).

445 For a discussion of the natural connection between administrative costs and government efforts to police IP rights, see Jonathan M. Barnett, *Property as Process: How Innovation Markets Select Innovation Regimes*, 119 Yale L J 384, 394 n 15 (2009).

446 See, for example, Bambauer, 59 Duke L J at 381–86 (cited in note 32).

447 There are numerous take-down provisions under US law. Some, such as that applicable to material that infringes copyright, are structured as safe harbors. See, for example, 17 USC § 512(c). Others impose criminal penalties for intermediaries such as ISPs who refuse to take down content. See, for example, Julia Scheeres, *ISP Guilty in Child Porn Case* (Wired Feb 16, 2001), online at http://www.wired.com/culture/lifestyle/news/2001/02/41878 (visited Sept 20, 2012) (discussing an ISP pleading guilty for knowingly providing access to child pornography after it failed to take down images).

United States.[448] Travel and legal representation are costly, and the site might not consider its American audience worth the bother. This might mean that audience interests are inadequately represented in any proceeding to determine whether filtering is lawful, or desirable. Foreign content providers might create a positive externality for American users: they generate more benefit than they capture through fees or advertising. Unless there is a mechanism that creates standing for American Internet users during censorship proceedings, the societal harm of filtering a site might be greater than the loss to the site's owner. Designing a system to prevent such a discrepancy is difficult.

Yet, this Article proposes to try. Whether America should prevent its citizens from accessing certain content online is a difficult normative question. I am skeptical. Should the government censor the Net, however, it should do so directly—using legislation that is tailored to the problem, that incorporates safeguards informed by the history of prior restraint, and that creates a system that is open, transparent, narrow, and accountable. Hard censorship is superior to soft censorship in achieving legitimacy. This article envisions a statute whereby the government could obtain an order that would compel ISPs to block access to specific unlawful material online. A statute that could legitimately impose such censorship would have five key features: limited standing, procedural protections, heightened proof requirements, narrow content targeting, and public funding. This Part next describes each requirement.

B. Limited Standing

A statute enabling censorship of Internet material should limit requests for filtering to the US Attorney General.[449] Prior restraint is a constitutionally significant step: it limits access preemptively and thereby implicates the First Amendment.[450] Government officials are ultimately (if somewhat indirectly, for the Attorney General) accountable politically for decisions and thus have incentive to weigh

---

448 Only one domain name owner has challenged a seizure to date. David Kravets, *US Facing Legal Challenge to Domain Name Seizures* (Ars Technica June 13, 2011), online at http://arstechnica.com/tech-policy/news/2011/06/us-facing-legal-challenge-to-domain-name-seizures.ars (visited Sept 20, 2012).

449 Compare PROTECT IP Act § 4(a)(1), in 157 Cong Rec at S 2938 (cited in note 110) (authorizing suits against domain name registrants or site operators by intellectual property owners), with Combating Online Infringement and Counterfeits Act § 2(b)–(c), in 156 Cong Rec at S 7208 (cited in note 108) (limiting standing to the Attorney General).

450 See *Kingsley Books, Inc v Brown*, 354 US 436, 445 (1957); *Near v Minnesota*, 283 US 697, 716 (1931).

competing interests in deciding whether and how to restrict information. While this incentive is hardly perfect—censorship can be popular[451]—it is preferable to the incentives of private plaintiffs such as IP owners, who are unlikely to engage in any weighing whatsoever.[452] Limiting standing to seek censorship is conceptually similar to the narrower ambit of criminal penalties versus civil ones for IP infringement: the power of state authority should only be deployed for serious offenses.[453] And censorship mandated by law is per force the application of state power.[454]

C. Procedural Protections

The statute should incorporate strong procedural protections for content owners. Most critically, it should provide defendants with notice and opportunity to respond and prohibit injunctions or orders affecting the material before adjudication occurs.[455] Since most content owners would reside outside the United States, it would be harder to provide adequate notice and for the defendants to obtain local counsel. The Attorney General should be required to notify content owners via e-mail to addresses listed as points of contact on the allegedly unlawful Web page(s) and for the domain name under which they are hosted,[456] via physical mail to all such addresses, and via the method of service of process for the jurisdiction in which the content owner resides,[457] if it can be determined. Next, the statute should toll further action for at least ninety days, to provide time for the defendant to retain counsel and formulate a response.[458] Lastly, until there has been adjudication on the merits of the government's claim that the relevant material is unlawful, the material should remain available. The burden must remain on the state to show that information should be blocked, rather than requiring the content owner to demonstrate its lawfulness.

---

451 See Depken, *Who Supports Internet Censorship?* (cited in note 62) (reporting that 46 percent of people support censorship in some form).

452 See Ryan Singel, *RIAA Believes MP3s Are a Crime: Why This Matters—Updated* (Wired Jan 9, 2008), online at http://www.wired.com/threatlevel/2008/01/riaa-believes-m (visited Sept 20, 2012).

453 See, for example, 17 USC § 506.

454 Consider Cover, 95 Yale L J at 1628–29 (cited in note 40).

455 See Martin H. Redish, *The Proper Role of the Prior Restraint Doctrine in First Amendment Theory*, 70 Va L Rev 53, 57 (1984) (stating that "prior restraints are especially disfavored because they authorize abridgment of expression prior to a full and fair determination of the constitutionally protected nature of the expression by an independent judicial forum").

456 See PROTECT IP Act § 4(c)(1), in Cong Rec at S 2939 (cited in note 110).

457 See FRCP 4(f)(2)(A).

458 See, for example, 18 USC § 983(a)(3)(A) (providing the government with ninety days to file a complaint for forfeiture after the property owner has filed a claim).

Filtering decisions should also be reviewed regularly. Orders generated under a filtering statute should expire after one year at most. The law should also provide a means for the content owner to challenge the order, either because the classification of the material as unlawful is in error or because the content has changed or been removed. However, to reduce administrative costs, the government should be able to renew the order if it can demonstrate to the court that the content at the blocked location is substantially unchanged. Similarly, the state should be able to make the required showing of illegality more easily if content migrates. Thus, if a site hosts child pornography images at one location, and faces a filtering order, the government should be able to readily obtain a modified order, without the procedural requirements listed above, if the site's owner moves those images to a new domain name or Web host. The content remains illegal; only the location has shifted.

These requirements seek to balance the risk of overblocking that occurs when content changes or migrates with the burden on the government to obtain filtering orders. There is an inevitable arms race between censors and content; material moves, and censors strive to catch up. The key is focusing on the content at issue, not its location—previous efforts such as the Pennsylvania anti–child pornography statute,[459] or the PROTECT IP Act[460] and SOPA,[461] have this backwards.

D. Heightened Proof Requirements

To interdict material online, the government should have to prove, by clear and convincing evidence, that the targeted content is illegal. At present, when the federal government seizes domain names, it need only show by a preponderance of the evidence that the domain name is subject to forfeiture.[462] The preponderance standard is insufficient. Governmental interference with speech necessitates a more demanding showing. In addition, the more stringent standard helps resolve the externality problem discussed above: some foreign defendants will not appear to vindicate the lawfulness of their material. Holding the government to a more exacting burden of proof will partially offset its advantage in such cases and provide at least some protection for audience interests.

---

459 Internet Child Pornography Act, 18 Pa Cons Stat Ann § 7621-30. See also *Center for Democracy & Technology v Pappert*, 337 F Supp 2d 606, 619–21 (ED Pa 2004).

460 See PROTECT IP Act § 2(d)(2), in 157 Cong Rec at S 2937.

461 See SOPA § 102(c)(2).

462 18 USC § 983(c)(1).

Moreover, the burden should apply to each URL that the government seeks to censor. If the Attorney General wants to block every page on a website, she should have to prove under the clear and convincing standard that each page is independently unlawful. This will helpfully press the government to limit blocking requests only to parts of a website, or other Internet locations, that are demonstrably illegal. Overall, the goal of the heightened proof standard is to align treatment of content that is hosted within the United States with that for material hosted abroad: if a page, file, or torrent can be taken down via injunction here, it can be blocked if it resides outside American borders.

E. Narrow Content Targeting

To avoid overblocking, even unlawful content should be filtered narrowly. Past filtering, such as that performed by Pennsylvania ISPs under the state's anti–child pornography statute, employed blocking by IP address, which resulted in massive overblocking of lawful content. The domain name blocking used by the Department of Homeland Security, and proposed for the PROTECT IP Act and SOPA, can similarly interfere with legitimate content.[463] Thus, filtering should take place at the URL or page level, at its most expansive, and preferably would occur at an even more granular level. Britain's Cleanfeed system, for example, can block an offending image in a web page but permit access to the remainder of that page's content.[464] This minimizes overblocking.

DNS filtering also results in underblocking. One critique of the domain name seizures carried out recently by the US government is that they are readily evaded: putatively unlawful content migrates to new domain names, where it can be reached by users who employ search engines to locate it.[465] Indeed, WikiLeaks used just such a method to overcome court-ordered blocking of its primary domain name in 2008.[466] Underblocking is problematic: it increases the likelihood that the state is acting pretextually or arbitrarily, it leaves al-

---

463 *Pappert*, 337 F Supp 2d at 633–34.

464 See Richard Clayton, *Failures in a Hybrid Content Blocking System*, in George Danezis and David Martin, eds, *Privacy Enhancing Technologies* 78, 78–79 (Springer 2006).

465 See Grazzini, *Four Rounds of ICE Domain Name Seizures* (cited in note 148); Nate Anderson, *Do Domain Seizures Keep Streaming Sites Down?* (Ars Technica Apr 17, 2011), online at http://arstechnica.com/tech-policy/news/2011/04/do-domain-seizures-keep-streaming-sites-down.ars (visited Sept 20, 2012).

466 Thomas Claburn, *Swiss Bank Abandons Lawsuit against WikiLeaks* (InformationWeek Mar 6, 2008), online at http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=206902154 (visited Sept 20, 2012).

legedly harmful content available, and it wastes enforcement resources on ineffectual efforts. As such, both DNS- and IP-based filtering are undesirable.

Thus, a filtering order should require US-based ISPs to block access to the specified content using technically feasible, financially reasonable efforts other than domain name or IP address filtering.[467] The method of compliance—and even whether compliance itself is possible—will vary among ISPs. Providers such as Mediacom, who employ deep-packet inspection to redirect search requests (a dubious tactic), can readily implement granular filtering.[468] Smaller ISPs may not be able to do so without absorbing a significant cost burden. When a user attempts to reach filtered content, the ISP should display a block page informing her that the material has been censored, and why.[469] Optimally, ISPs would include a link on the block page to a copy of the filtering order. Google, for example, notifies users when it has removed links from its search results due to a takedown notice under the DMCA.[470] The search engine submits all such notices to the nonprofit "Chilling Effects" project and provides a link to the relevant notice at the bottom of the filtered search results.[471] Block pages are important to open, transparent filtering—they inform users that content has been deliberately preempted rather than being unreachable due to technological problems or the content owner's choice.

F. Public Funding

Finally, the filtering statute should include public funding for additional costs that ISPs incur to block access to content.[472] The filtering support should cover the entirety of ISP costs directly attributable to censorship orders, such as additional routers or software, technical

---

467 See, for example, PROTECT IP Act § 3(d)(2)(A)(i), in 157 Cong Rec at 2938.

468 See mmjrogers, *Why Mediacom's DPI Policy is Both Wrong and Dangerous*, Customer Support (Mediacom Apr 26, 2011), online at http://mediacomcable.com/CustomerSupport/forum/index.php?topic=1824.0 (visited Sept 20, 2012).

469 See, for example, Websense, *Block Pages*, online at http://www.websense.com/content/support/library/web/v75/triton_web_help/block_pages.aspx (visited Sept 20, 2012).

470 See Electronic Frontier Foundation, *Chilling Effects Supporters Fight Back against Perfect 10 Challenge*, Press Room (Dec 23, 2010), online at https://www.eff.org/press/archives/2010/12/22 (visited Sept 20, 2012); Bruce Byfield, *Chilling Effects Site Defends Online Freedom of Expression* (Linux May 24, 2006), online at http://archive09.linux.com/feature/54387 (visited Sept 20, 2012).

471 See Electronic Frontier Foundation, *Chilling Effects Supporters* (cited in note 470).

472 See Derek E. Bambauer, *Conundrum*, 96 Minn L Rev *584, 635–38, 651–53 (forthcoming 2012), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1807076 (visited Sept 20, 2012) (proposing federal funding for cybersecurity investments by private firms).

staff, and support personnel.[473] The statute should establish a process whereby ISPs can apply for reimbursement if they are able to document such expenses. Public funding is likely to be controversial during a time of sensitivity to budget deficits, and it raises concerns about strategic behavior by providers in assessing costs.[474] However, funding is important for at least two reasons.

First, absent such support, the state can effectively force ISPs to fund its content restrictions. This will increase the cost of broadband access for ISP subscribers—in effect, the cost of filtering is passed through to consumers, but invisibly. The pass-through operates like a covert filtering tax, but without the checks on taxation that the political process imposes.[475] Paying for censorship from the federal treasury forces at least some attention to its costs and to competing demands for resources.

Second, public funding causes the state to internalize more of the economic costs of censorship, which act as rough, though incomplete, proxies for societal costs. The less expensive a tactic is for the government, the more likely it is to employ that tactic. Chris Soghoian and Stephanie Pell document how the sharply falling cost of obtaining the geolocation of a cell phone has led to a dramatic increase in government requests for such information.[476] Censorship, too, becomes more attractive as it becomes cheaper. Forcing government to pay to censor checks this natural tendency.

G. Prior Restraint

To achieve greater legitimacy in restricting content online, Congress should pass, and the president should sign, a specialized filtering statute. The law would authorize the Attorney General to seek a court order that would compel ISPs, using technically and financially reasonable measures, to block access to content. To obtain such a measure, the government would need to provide adequate notice to the content owner and sufficient time to prepare a defense. Filtering would be permitted only after the material was proved to be unlawful through clear and convincing evidence. And the gov-

---

473 See, for example, 47 USC § 1008 (reimbursing telecommunications carriers for limited retrofitting of their facilities to comply with the Communications Assistance to Law Enforcement Act).

474 See *Verizon Communications, Inc v FCC*, 535 US 467, 503, 539 (2002) (upholding FCC authority to set rates for the leasing of telephone networks to market entrants but noting the possibility of "pervers[e]" incentives).

475 Bambauer, 31 U Pa J Intl L at 515 (cited in note 250) (discussing filtering tax).

476 See Pell and Soghoian, 26 Berkeley Tech L J at 47 n 206 (cited in note 241).

ernment should fund the additional capacity necessary for ISPs to filter via general public revenues.

This statute would align America's Internet censorship practices with its historic treatment of prior restraints on information.[477] Like prior restraints in other media, filtering orders would issue only when the government met a demanding standard. Supreme Court precedent repeatedly emphasizes the critical role played by procedural protections, and by standards that cabin or preferably eliminate official discretion.[478] The statute leaves material available until the government proves, by a heightened standard, that the content is unlawful. And unlike the PROTECT IP Act and SOPA, the proposed statute places the risks of delay on the government, not on content providers.[479] Finally, this hard censorship proposal conforms to an underappreciated aspect of prior restraint: it is difficult for the government to muzzle speech, but not impossible.[480] Censorship remains a powerful tool that the state can employ, but only when it demonstrates extraordinary need.

H. The Wisdom of Gag Orders

This Part argues that hard censorship—in particular, a statute that requires the Attorney General to demonstrate that specified content is unlawful before filtering it—is preferable to soft censorship. Accordingly, it proposes the key features of such a statute, in an effort to make any such censorship maximally legitimate by being open, transparent, narrow, and accountable. It does *not* argue that censorship is desirable. Instead, and perhaps pessimistically, this Article contends that online censorship is inevitable: nearly every government seeks to block some material on the Net.[481] The constraints on soft censorship in the United States are weak, and the government operates in a zone of considerable discretion. The Arti-

---

477 See John Calvin Jeffries Jr, *Rethinking Prior Restraint*, 92 Yale L J 409, 412–18 (1983).

478 See, for example, *Freedman v Maryland*, 380 US 51, 59–60 (1965) (holding insufficient the procedural protections provided by a censoring regime that allowed a censor to disapprove of a work without justifying, by some burden of proof, its disapproval).

479 Consider *FW/PBS, Inc v City of Dallas*, 493 US 215, 223–24 (1990) (holding that the failure to set time limits on a determination of unlawful speech is a species of "unbridled discretion").

480 See *Kingsley Books*, 354 US at 441.

481 See Deibert, et al, eds, *Access Controlled* at 5–6 (cited in note 81) (introducing a study that documents censorship in the fifty-six nations comprising the Organization for Security and Cooperation in Europe and in nations comprising the postcommunist Commonwealth of Independent States).

cle's proposal seeks to cabin that discretion and to make the debate over the propriety of censorship an overt, active one.

Proposing a hard censorship law will be unpopular. Censorship is anathema to most legal scholars, and to many Americans. Yet it is likely the least bad solution. The debate is similar to that over Alan Dershowitz's proposal for torture warrants after the terrorist attacks of September 11, 2001.[482] Dershowitz, who is opposed to torture on normative grounds, nonetheless argued that when national security was at grave risk, officials should be able to obtain judicial authorization to employ nonlethal torture.[483] He was roundly attacked.[484] Dershowitz's point, though, was that the debate was not over whether to torture suspects—the United States has already done so, either directly or by proxy.[485] It was whether to torture them in an open and accountable way. It was whether Americans should have to confront openly the consequences of their choices, and accept moral responsibility for them.

So, too, with censorship. America is already censoring the Internet. At the moment, the government does so haphazardly and somewhat ineffectively. But the ambit of censorship is expanding. I propose that the United States admit openly that it is engaged in censorship, justify its practices, and encode them in specific public law. Doing so is likely to lead to less censorship rather than more, and it will make the filtering that does occur more legitimate.

Some will object that this process legitimates Internet censorship in a manner anathema to deeply held American views on free expression, as enshrined in the Constitution and a host of Supreme Court decisions. I take up this issue in my prior article, *Cybersieves*, and so address it here only briefly. America has a history of censorship, from

---

[482] Alan M. Dershowitz, *Why Terrorism Works: Understanding the Threat, Responding to the Challenge* 247–48 (Yale 2002).

[483] Id. See also Alan M. Dershowitz, *Want to Torture? Get a Warrant*, Open Forum (SFGate Jan 22, 2002), online at http://articles.sfgate.com/2002-01-22/opinion/17527284_1_physical-pressure-torture-terrorist (visited Sept 20, 2012).

[484] See, for example, Charles Fried and Gregory Fried, *Because It Is Wrong: Torture, Privacy and Presidential Power in the Age of Terror* 31–51 (Norton 2010) (critiquing Dershowitz's proposal as, among other things, running afoul of a "grounding commitment" that the law is not brutal); Alan M. Dershowitz, *The Torture Warrant: A Response to Professor Strauss*, 48 NY L Sch L Rev 275, 275 (2003) (collecting critiques).

[485] See, for example, International Committee of the Red Cross, *ICRC Report on the Treatment of Fourteen "High Value Detainees" in CIA Custody* 8–9 (Feb 14, 2007), online at http://www.nybooks.com/media/doc/2010/04/22/icrc-report.pdf (visited Sept 20, 2012); *Vance v Rumsfeld*, 653 F3d 591, 596 (7th Cir 2011), vacd and rehearing en banc granted (7th Cir Oct 28, 2011) (describing psychological and physical torture allegedly suffered by plaintiffs at the hands of the US military in Iraq).

films about prizefighting,[486] to D.H. Lawrence novels,[487] to sedition laws,[488] to encryption software.[489] The Supreme Court has suggested in dicta that even a ban on publishing material in a newspaper might be acceptable under limited circumstances,[490] and a federal district court enjoined publication of information about nuclear weapons.[491] The DMCA pushes intermediaries such as search engines to remove links to material that allegedly infringes copyright, on pain of potential liability for secondary infringement.[492] America's commitment to free communication is quite strong, but it is not absolute. This Article argues that this commitment should yield to countervailing values only under laws carefully and specifically designed to balance those other interests.

V. SOFT CENSORSHIP AS EXEMPLAR

The lessons of Orwell's Armchair have relevance for two major scholarly and policy debates about the role of government in shaping the online information environment. First, both sides in the net neutrality fight contemplate allowing—or even requiring—intermediaries to censor content. However, this debate is veiled under the circumlocutions of "reasonable network management"[493] and protection of "lawful content,"[494] rather than occurring openly. Scholars and advocates on both sides would do better to engage forthrightly about what content may and may not be blocked. Second, recent scholarship that supports providing government greater power to promote information online has failed to account for the state's creativity in pressing a nor-

---

[486] See Barak Y. Orbach, *Prizefighting and the Birth of Movie Censorship*, 21 Yale J L & Humanities 251, 254–55 (2009).

[487] See *Kingsley International Pictures Corp v Regents of the University of the State of New York*, 360 US 684, 684–85 (1959); *Grove Press, Inc v Christenberry*, 276 F2d 433, 437 (2d Cir 1960).

[488] See *Abrams v United States*, 250 US 616, 617, 624 (1919).

[489] See *Bernstein v Department of Justice*, 176 F3d 1132, 1141 (9th Cir 1999), withdrawn, 192 F3d 1308 (9th Cir 1999). See also Thinh Nguyen, Note, *Cryptography, Export Controls, and the First Amendment in* Bernstein v. United States Department of State, 10 Harv J L & Tech 667, 671–75 (1997).

[490] *Near*, 283 US at 716.

[491] See *United States v Progressive, Inc*, 467 F Supp 990, 1000 (WD Wis 1979).

[492] See Bambauer, 59 Duke L J at 401 (cited in note 32).

[493] Chris Riley, *Clear Standards for Reasonable Network Management*, Save the Internet (Free Press Jan 20, 2010), online at http://www.savetheinternet.com/blog/10/01/20/clear-standards-reasonable-network-management (visited Sept 20, 2012); Philip J. Weiser, *The Future of Internet Regulation*, 43 UC Davis L Rev 529, 552 (2009).

[494] Wayne Rash, *Net Neutrality Order Reveals FCC's Concern about Legal Challenges* *2 (eWeek Dec 27, 2010), online at http://www.eweek.com/c/a/Cloud-Computing/Net-Neutrality-Order-Reveals-FCCs-Concern-About-Legal-Challenges-834561 (visited Sept 20, 2012).

mative agenda. Soft censorship demonstrates that reducing scrutiny of government's role with online content is unwise. This Part explores briefly how the Article's analysis illuminates these issues.

A. Net Neutrality

Scholars have been worried about content discrimination by network providers since the commercialization of the Internet.[495] The debate turned largely on descriptive views of how innovation occurs.[496] Net neutrality became an active policy controversy when the FCC moved to impose nondiscrimination via its Internet Policy Statement[497] and when President Obama adopted the cause as a key initiative.[498]

At a conceptual level, the debate over net neutrality appears to recapitulate that over censorship: should providers be permitted to filter Internet content? However, the reality is more complex. Anti-neutrality advocates seek to ensure discretion for network providers in prioritizing and even routing content, without describing how ISPs would disclose their practices in a way that would enable meaningful consumer choice.[499]

Those who favor net neutrality have also been less than straightforward. There appears to be no one who argues for banning ISPs from filtering spam, or malware, or denial-of-service traffic.[500] The FCC, too, disguises value preferences. Its rules ban providers from blocking "lawful content."[501] The challenge is in defining what is lawful. Net neutrality is thus a misnomer. The debate is not one of common carriage versus unfettered discretion. Rather, it is a disa-

---

[495] See, for example, Mark A. Lemley and Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L Rev 925, 940–43 (2001).

[496] Compare Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J Telecomm & High Tech L 141, 154–56 (2003) (arguing that edge-based inventiveness, on the model of Eric von Hippel's decentralized innovation, best generates technological advance), with Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 Georgetown L J 1847, 1874–75 (2006) (contending that content discrimination is critical to create incentives for providers to innovate).

[497] *In the Matters of Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 FCCR 14986, 14887–88 (2005).

[498] See Anne Broache, *Obama Pledges Net Neutrality Laws if Elected President*, News Blogs (CNET Oct 29, 2007), online at http://news.cnet.com/8301-10784_3-9806707-7.html (visited Sept 20, 2012).

[499] For efforts to increase transparency, see *Preserving the Open Internet*, 25 FCCR at 17942 (cited in note 255).

[500] Consider James Temple, *FCC Approves Draft Net-Neutrality Rules*, SF Chron C1 (Oct 23, 2009).

[501] *Preserving the Open Internet*, 25 FCCR at 17942 (cited in note 255).

greement over *what* content can be blocked and over *who* makes that determination.

This Article argues that it is preferable to block content using purpose-specific rules that are open and transparent, that target material narrowly, and that develop from accountable processes. Similarly, the net neutrality debate would be improved if both sides were more forthright. Pro-neutrality advocates want more limited blocking, and they prefer that the state specify what material ISPs can filter, but they do not embrace a mandate for unlimited communication. They fall short, in other words, on openness grounds. Ironically, net neutrality partisans essentially favor governmentally specified blocking: ISPs would be permitted to filter so long as they stayed within officially described limits. Anti-neutrality advocates fail to be sufficiently transparent: they seek to preserve ISPs' flexibility in blocking material but do not commit to a system of disclosure regarding what they filter.

Both camps in the net neutrality arena contemplate private, and perhaps public, blocking of Internet material. The lessons of Orwell's Armchair suggest that the outcome of their contest will be more legitimate if they shift the discourse to focus on what content they consider acceptable to block and why a given decision maker (the government or private providers) should be empowered to make that choice.

B. Content Promotion by Government

Second, the conclusions of Orwell's Armchair strongly suggest that efforts to permit greater governmental promotion of favored content are significantly misguided. Governmental censorship is creative and often carefully disguised. Advocates of content promotion not only misread the history of state efforts to control content but also ignore current circumstances. Maintaining a stringent standard of judicial review will help force the government to overtly defend its efforts to shape the online information environment.[502] Such efforts are not always misguided; indeed, they may be essential.[503] However, checking censorial tendencies necessitates regarding them with skepticism.[504]

A new generation of scholars has advanced arguments favoring a greater governmental role in shaping our information environment.

---

[502] See Stuart Minor Benjamin, *Proactive Legislation and the First Amendment*, 99 Mich L Rev 281, 284 (2000).

[503] See Jerome A. Barron, *Access to the Press—A New First Amendment Right*, 80 Harv L Rev 1641, 1641 (1967).

[504] See Mark G. Yudof, *When Government Speaks: Politics, Law, and Government Expression in America* 178–79 (California 1983).

They view the concentration of ownership of broadcast media outlets as a worrisome aggregation of private power.[505] For example, Marvin Ammori argues prescriptively that governmental content promotion should receive less scrutiny than attempts to impede access to information and that Supreme Court precedent, properly construed, supports this conclusion descriptively.[506] Hannibal Travis seeks to provide support grounded in legal and constitutional theory for the FCC's shift to "prioritizing media consumers' rights to access diverse and antagonistic sources of information and opinion."[507] These scholars envision regulation as a counterweight to an information environment that is dominated by a small group of private entities, insufficiently diverse and frequently frivolous. The state, they argue, can provide needed balance by supporting, through funding or structural rules, content from underrepresented perspectives and on worthy yet insufficiently addressed topics. Thus, injecting the state into the process of shaping online information can have a salutary effect.

Pro-intervention arguments, though, rest on two underexplored assumptions: first, that the current information environment is suboptimal and, second, that governmental action can improve the situation.[508] To defend these assumptions, one must provide an account of what the information ecosystem *ought* to look like. Absent such a model, the risk is that, put crudely, scholars would like to see more discourse that favors their own preferred positions.[509] A principled account of how the information environment should appear must explain why there is, or is not, the correct amount of data on creationism, or skepticism about global warming, or the existence of God.

Unfortunately, neither Ammori nor Travis offers a methodology to evaluate the state of online information, nor to measure whether the government has achieved progress. For example, Ammori supports a theory of the First Amendment that permits the government to advance "democratic content," which he describes as

---

505 See, for example, Travis, 51 Santa Clara L Rev at 491–98 (cited in note 36) (arguing that net neutrality is a constitutional policy in the age of aggregated media power because it guarantees innovative individuals access to crucial resources like high-speed Internet).

506 Ammori, 61 Fed Comm L J at 303–19 (cited in note 35) (supporting a viewpoint-neutral test for government content promotion but a strict-scrutiny test for other content-based laws).

507 Travis, 51 Santa Clara L Rev at 420–21 (cited in note 36).

508 See, for example, Martin H. Redish and Kirk J. Kaludis, *The Right of Expressive Access in First Amendment Theory: Redistributive Values and the Democratic Dilemma*, 93 Nw U L Rev 1083, 1085–86 (1999) (contending that government can "enrich" public debate by intervening to guarantee "expressive access").

509 See, for example, Travis, 51 Santa Clara L Rev at 509–12 (cited in note 36) (criticizing favorable coverage of financial deregulation).

educational, political, and viewpoint-diverse material.[510] There are at least three problems with his interventionist approach. First, it is not clear whether, even under Ammori's vision of the First Amendment, the state can lawfully engage in viewpoint promotion to achieve greater viewpoint diversity.[511] Ammori's description reaches content promotion but does not explain how viewpoint discrimination is permissible. Second, he argues for allowing government to skew toward democratic content but does not describe how to tell that government is doing so.[512] This is the inverse of Cass Sunstein's critique of status quo neutrality: Ammori assumes that the status quo is undesirable without explaining why.[513] Lastly, and crucially, Ammori sees attempts to promote content as less impermissible than state efforts to restrict information.[514] He argues that the history of subsidized speech demonstrates there is little cause to worry about promotion.[515] This conclusion is difficult to defend in light of cases challenging discrimination in subsidized speech, from selective funding of abortion-related speech,[516] to limits on editorializing by broadcasters,[517] to limits on challenges to welfare law.[518] In short, Ammori makes an empirical argument about governmental treatment of speech without empirical support for it.

Soft censorship demonstrates the flaws in the content promotion arguments. Government is unlikely to employ its powers to advance information without regard to its viewpoint. Filters on school computers can block pro-LGBT sites but not anti-LGBT ones. The Treasury Department can seize pro-Cuba domain names, but not anti-Cuba ones. Homeland Security can block sites that the MPAA and RIAA object to but not ones their critics deplore. School boards

---

510 Ammori, 61 Fed Comm L J at 304–05 (cited in note 35).

511 See, for example, *Regan v Taxation With Representation of Washington*, 461 US 540, 548 (1983).

512 Ammori, 61 Fed Comm L J at 309 (cited in note 35).

513 See id at 309 n 230, citing Cass R. Sunstein, *The Partial Constitution* 2–7 (Harvard 1993).

514 Ammori, 61 Fed Comm L J at 310 (cited in note 35).

515 See id (citing public television and other examples as proof that content promotion is not a "cover" for censorship).

516 See *Rust v Sullivan*, 500 US 173, 198–99 (upholding a Title X provision that prevented certain government-funded healthcare providers from discussing abortion with patients).

517 See *FCC v League of Women Voters of California*, 468 US 364, 402 (1984) (striking down a statute that prevented television stations receiving any money from the Corporation for Public Broadcasting from "editorializing").

518 See *Legal Services Corp v Velazquez*, 531 US 533, 548–49 (2001) (finding unconstitutional a provision that conditioned funding for the representation of indigent litigants on the waiver of the right to challenge welfare laws).

can attempt to promote criticism of evolution disguised as balance.[519] Soft censorship demonstrates the wisdom of conventional, strict scrutiny treatment of content-specific governmental action under the First Amendment.[520] The heightened burden of strict scrutiny forces the state to proffer a compelling justification for its actions and increases the likelihood that efforts to guise viewpoint favoritism in content promotion will be detected and nullified.[521]

CONCLUSION

Internet filtering in America has evolved. The content that it targets has shifted, moving from a focus on sex-oriented materials, particularly those inappropriate for minors, to concentrate on gambling, IP infringement, and national security material. The approach employed by the state has shifted from attempts to force intermediaries such as ISPs to act as agents in censorship to less direct and less visible methods such as payment, pretext, and persuasion through pressure. And lastly—and most counterintuitively—the legitimacy has shifted, and not for the better. Hard censorship efforts such as the CDA and COPA were problematic in the wide sweep of their prohibitions and in their attempts to wish problems away by hoping for technological solutions. Nonetheless, they represented censorship that was overt about its goals and rationales, and that attempted—with great imperfection—to engage countervailing concerns such as the rights of adult Internet users and the risks of overcriminalization.

Soft censorship does not share these virtues. It is less open and transparent about its restrictions, and often less precisely targeted. Accountability is diffused, particularly when the state seeks to coerce private parties to block material but then conceals its role. The absence of direct state action limits constitutional redress and the absence of sufficient competition among broadband providers limits market constraints. Soft censorship is both more normatively problematic than hard censorship and less restricted by the safeguards that Americans normally rely upon when their government seeks to shape what they say and what they read.

---

519 See, for example, *Kitzmiller v Dover Area School District*, 400 F Supp 2d 707, 711, 716 (MD Pa 2005) (discussing the growing popularity of "balanced treatment" statutes that require teaching evolution alongside the biblical view of creation); Geoff Brumfiel, *Kansas Backs Lessons Critical of Evolution*, 436 Nature 899, 899 (Aug 18, 2005) (reporting the decision of a Kansas school board to include more robust criticism of evolution in its curriculum).

520 See *Simon & Schuster, Inc v Members of New York State Crime Victims Board*, 502 US 105, 115–16 (1991).

521 See, for example, *R.A.V. v City of St. Paul*, 505 US 377, 391–92 (1991).

This Article proposes an unexpected solution: if Americans decide, through their elected officials, that certain material should not be readily available online, we should admit that we are willing to censor the Internet. And we should use specialized legislation to do so—legislation that is careful in what it targets, thorough in the procedural protections it creates, and balanced in the burdens it places upon intermediaries such as ISPs. The debate is no longer whether to censor: we are already doing that. The key question is how. We should prefer Orwell's Room 101[522] to Orwell's Armchair: censorship that is overt, robustly defended, and carefully limited forces us to take moral responsibility for our actions.

[522] I thank James Grimmelmann for greatly improving this metaphor.