Duke Law Journal

VOLUME 59 DECEMBER 2009 NUMBER 3

CYBERSIEVES

DEREK E. BAMBAUER†

ABSTRACT

This Article offers a process-based method to assess Internet censorship that is compatible with different value sets about what content should be blocked. Whereas China's Internet censorship receives considerable attention, censorship in the United States and other democratic countries is largely ignored. The Internet is increasingly fragmented by nations' different value judgments about what content is unacceptable. Countries differ not in their intent to censor material—from political dissent in Iran to copyrighted songs in America—but in the content they target, how precisely they block it, and how involved their citizens are in these choices. Previous scholars have analyzed Internet censorship from values-based perspectives, sporadically addressing key principles such as openness, transparency, narrowness, and accountability. This Article is the first

† Assistant Professor of Law, Brooklyn Law School. The author thanks Michael Abramowicz, Sarah Abramowicz, Tim Armstrong, Fred Bloom, Susan Cancelosi, Richard Clayton, Steve Davidoff, Ron Deibert, Jeff Engerman, Rob Faris, Terry Fisher, Lance Gable, Joel Gora, Noah Hall, Peter Hammer, Justin Hughes, Gordon Hull, Orin Kerr, Melissa Jacoby, Ted Janger, Gail Klavinger, Raymond Ku, Lili Levi, Michael Madow, Rebecca MacKinnon, Jason Mazzone, Bill McGeveran, Thinh Nguyen, John Palfrey, Joe Perry, C.J. Peters, Dana Brakman Reiser, Rafal Rohozinski, Colette Routel, Dave Schwartz, Nart Villeneuve, Jonathan Weinberg, Aaron Williamson, Tim Wu, Peter Yu, Jonathan Zittrain, and the OpenNet Initiative for comments; thanks Jelena Kristic and Brad Reid for research; and thanks the Dean's Summer Research Stipend Program and Joan Wexler, at Brooklyn Law School, for financial support. This Article's concept emerged from a debate between the author and Richard Epstein at Legal Affairs' Debate Club. The author welcomes comments at derek.bambauer@brooklaw.edu.

to unite these principles into a coherent methodology. Drawing upon scholarship in deliberative democracy, health policy, labor standards, and cyberlaw, this Article applies this new framework to contentious debates about sales of censorship technology by Western companies, public law regulation of these transactions, and third-party analysis of Internet censorship.

TABLE OF CONTENTS

> It's taken governments a long time to realize that you don't need to manipulate unwelcome news. Just don't show it.
>
> – P.D. James, THE CHILDREN OF MEN[1]

INTRODUCTION

How can legal scholars make normative distinctions among Saudi Arabia's decision to censor Internet pornography, China's efforts to suppress political dissent online, and America's moves to filter illegal MP3 files from the Web? Is it acceptable for Cisco to sell networking gear to China, knowing that it will be used to block dissident views,[2] or for Verizon to drop Usenet newsgroups at the New York State Attorney General's behest?[3] Whereas China's Internet censorship receives considerable attention, censorship in the United States and other democratic countries is largely ignored. The Internet's increasing fragmentation, driven by technological censorship, derives from different value judgments made by countries about the relative importance of free expression, protection of minority interests, concern for societal cohesion, and other goals. The common thread, though, is censorship: most countries use cybersieves to try to filter undesirable content and make it disappear from the Web. Whether it is copyrighted songs in America or political dissent in Iran, the goal is the same; only the targeted material varies. Countries differ not in their intent to limit access to material online, but in the content they ban, the precision of their blocking, and the voice they offer citizens in decisionmaking. This Article offers a new, process-based method to measure the legitimacy[4] of these efforts,

---

1. P.D. James, THE CHILDREN OF MEN 123 (1992).

2. *See* Sarah Lai Stirland, *Cisco Leak: "Great Firewall" of China Was a Chance to Sell More Routers*, WIRED, May 20, 2008, http://blog.wired.com/27bstroke6/2008/05/leaked-cisco-do.html.

3. *See* Danny Hakim, *3 Net Providers Will Block Sites with Child Sex*, N.Y. TIMES, June 10, 2008, at A1; *see also* Declan McCullagh, *N.Y. Attorney General Forces ISPs to Curb Usenet Access*, CNET NEWS, June 10, 2008, http://news.cnet.com/8301-13578_3-9964895-38.html (quoting statements from Time Warner Cable and Verizon that they would block Usenet groups but not Web sites).

4. While there are multiple normative positions on legitimacy, this Article argues for a process-based approach that embodies an increasingly universal set of governance norms, as embodied in documents such as the Universal Declaration on Human Rights. Authoritarian countries tend to adhere outwardly to the forms of process-based governance, even if their actions contravene its substance. I argue that process-based legitimacy maps sufficiently well onto widely shared norms that it should enjoy analytical primacy, and that it is likely to be the most helpful tool for multiple actors with different values-based agendas.

advancing debate about the balance between information sharing and control on the Internet, and about how that balance is struck.[5] Its analytical framework is compatible with divergent views on what material should be banned, strengthening norms-based assessments.

Scholars who have addressed Internet filtering have approached the issue from multiple values-based perspectives. But this Article is the first to recognize that values-based analysis is unhelpful in a world of pervasive Internet censorship and to offer an integrated methodology for evaluating how decisions about online information controls are made. This new framework examines critically the processes of Internet censorship to evaluate how well a country describes what it censors and why, whether it effectively blocks proscribed material while leaving permitted content untouched, and how much its citizens can participate in filtering decisions. Because online censorship is sharply on the rise worldwide—in democratic states[6] as well as in authoritarian ones[7]—corporations, citizens, and governments will increasingly be forced to make difficult judgments about filtering practices.[8]

Part I examines current approaches to Internet censorship and details their shortcomings; it then introduces a process-based solution (which this Article refers to as the "Framework") and explores its roots in contemporary legal thinking. Part II describes the Framework's four components, with examples from countries that censor the Internet. Part III advocates development of competing quantitative metrics to measure these components, and then explains how the metrics can help resolve three contentious policy debates. First, how should companies decide when to sell technology enabling

5. *See generally* John G. Palfrey, Jr. & Robert Rogoyski, *The Move to the Middle: The Enduring Threat of "Harmful" Speech to the End-to-End Principle*, 21 WASH. U. J.L. & POL'Y 31 (2006) (describing recent changes in Internet regulation practices).

6. *See, e.g.*, Danny O'Brien, *Turkish Censor Lacks Others' Subtle Touch*, IRISH TIMES, Mar. 23, 2007, at 7 (noting that Great Britain and the European Union have expressed interest in blocking access to terrorism materials).

7. Kevin Voigt, *Internet Censorship Gathers Steam*, CNN.COM, Apr. 24, 2007, http://edition.cnn.com/2007/BUSINESS/04/18/online.censorship/index.html; *see also* Matthew Quirk, *The Web Police*, ATL. MONTHLY, May 2006, at 50, *available at* http://www.theatlantic.com/doc/print/200605/chinese-internet (detailing widespread censorship in China, Iran, and other authoritarian nations).

8. *See, e.g.*, Bruce Schneier, *Access Denied*, 452 NATURE 155, 155 (2008); Christopher S. Rugaber, *Google Fights Global Internet Censorship*, WASH. POST, June 25, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/06/25/AR2007062500364_pf.html.

a country's censorship?[9] Second, how should governments decide whether to regulate these transactions using public law? Finally, how can other nations, activists, and scholars evaluate countries' online information restrictions, such as when naming countries as human rights violators?[10] Part IV assesses the Framework's challenges and limitations, and the Article concludes with observations about the rise of filtering worldwide.

I. THE INTERNETS

A. Series of Filtered Tubes

Current analytical approaches to Internet censorship are inadequate to assess filtering that is increasingly ubiquitous. This Section describes the problem of multiple Internets, explains why extant theories are unworkable, and explains how the divergence of norms around what content is and is not permissible challenges filtering analysis.

There is no longer one Internet.[11] Technological censorship by countries worldwide means that how the Net appears depends upon where you access it.[12] In Beijing, one cannot reach sites criticizing the Chinese Communist Party.[13] In Mumbai, Internet Service Providers

---

9. *See generally* Jonathan Zittrain & John Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 103 (Ronald Deibert et al. eds., 2008) (arguing that corporations themselves are best positioned to take the lead in establishing a code of conduct); Press Release, Ctr. for Democracy & Tech., Companies, Human Rights Groups, Investors, Academics and Technology Leaders to Address International Free Expression and Privacy Challenges (Jan. 18, 2007), http://www.cdt.org/press/20070118press-humanrights.php (announcing a meeting of various stakeholders "to seek solutions to the free expression and privacy challenges faced by technology and communications companies doing business internationally").

10. *See generally* U.S. DEPT. OF STATE, 2007 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES (2008), *available at* http://www.state.gov/g/drl/rls/hrrpt/2007/ (describing individual countries' human rights advances and setbacks within a democratic government framework).

11. *See* Jonathan Zittrain & John Palfrey, *Introduction*, *in* ACCESS DENIED, *supra* note 9, at 1, 2–4.

12. *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006) (describing the success of governments in controlling Internet access and content).

13. *See* OPENNET INITIATIVE, INTERNET FILTERING IN CHINA 17 (2009), http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf; *see also* U.S. DEP'T OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES—2007: CHINA (2008), *available at* http://www.state.gov/g/drl/rls/hrrpt/2007/100518.htm (describing China's human rights practices generally, including Internet censorship); James Fallows, *"The Connection Has Been Reset,"* ATL. MONTHLY, Mar. 2008, at 64, *available at* http://www.theatlantic.com/doc/200803/chinese-firewall.

(ISPs) block the religious extremist Web site Hindu Unity.[14] A user searching Google for "stormfront" in Paris will see the game designers' site, but not that of the white supremacist group.[15] From Boston, someone looking for copyrighted music files may find them removed from search engines or host sites.[16] The decision to hold the 2008 Summer Olympic Games in the People's Republic of China focused attention—and criticism—on China's online restrictions,[17] but other countries[18] such as Iran,[19] Indonesia,[20] Japan,[21] Australia,[22] New Zealand,[23] and Brazil[24] also censor cyberspace. Increasingly, countries

14. OPENNET INITIATIVE, INDIA 4 (2007), http://opennet.net/sites/opennet.net/files/india.pdf; *see also* Nart Villeneuve, *Evasion Tactics*, INDEX ON CENSORSHIP, Nov. 2007, at 71, 76.

15. *See, e.g.*, Declan McCullagh, *Google Excluding Controversial Sites*, CNET NEWS, Oct. 23, 2002, http://www.news.com/2100-1023-963132.html. *See generally* OPENNET INITIATIVE, EUROPE (2007), http://opennet.net/research/regions/Europe (describing filtering practices by category in European countries).

16. *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 622 (2006). *See generally* Google, Digital Millennium Copyright Act, http://www.google.com/dmca.html (last visited Oct. 23, 2009) (describing policies for removing infringing sites or material).

17. *See, e.g.*, Edward Cody, *IOC Allows China to Limit Reporters' Access to Internet*, WASH. POST, July 31, 2008, at A10 (describing Olympic journalists finding certain Web content blocked); *I.O.C. Member Accuses Committee of Betrayal on Censorship Issue*, N.Y. TIMES, Aug. 1, 2008, at D7 (same); Andrew Jacobs, *Beijing Games Denying Media Full Use of Web*, N.Y. TIMES, July 31, 2008, at A1 (same).

18. *See generally* Anick Jesdanun, *Is It Censorship or Protection?*, WASH. POST, July 20, 2008, at A3 (describing censorship practices of various ISPs and Web sites).

19. *Iran Launches Fresh Crackdown on Websites: Report*, AFP, May 20, 2008, http://afp.google.com/article/ALeqM5jgPmlgFydl8ifBE-OLsLXcyQYUgg. *But see* JOHN KELLY & BRUCE ETLING, BERKMAN CTR. FOR INTERNET & SOC'Y, HARVARD UNIV. PUB. NO. 2008-01, MAPPING IRAN'S ONLINE PUBLIC: POLITICS AND CULTURE IN THE PERSIAN BLOGOSPHERE 21 (2008), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf (noting researchers' "surprise that such a large proportion of that part of the blogosphere, which the regime must consider oppositional, is in fact visible within Iran").

20. *Indonesia Seeks to Block YouTube over Anti-Koran Film*, REUTERS, Apr. 2, 2008, http://www.reuters.com/article/technologyNews/idUSSP23588120080402.

21. *See, e.g.*, J. Mark Lytle, *Internet Censorship Body Swings into Action*, TECHRADAR UK, July 4, 2008, http://www.techradar.com/news/internet/web/internet-censorship-body-swings-into-action-415849 (describing filtering of sites accessible to minors via mobile phones).

22. Derek E. Bambauer, *Filtering in Oz: Australia's Foray into Internet Censorship*, 31 U. PA. J. INT'L L. (forthcoming 2009), *available at* http://ssrn.com/abstract=1319466.

23. Jacqui Cheng, *New Zealand Moves Forward with Child Porn Filtering System*, ARS TECHNICA, July 17, 2009, http://arstechnica.com/tech-policy/news/2009/07/new-zealand-moves-forward-with-child-porn-filtering-system.ars.

24. *Google in Deal with Brazil to Fight Child Porn*, REUTERS, July 2, 2008, http://www.reuters.com/article/internetNews/idUSN0237672120080702.

use computer technology to block access to prohibited content—a practice known as Internet "filtering."[25] Their objective is to shape citizens' information environments and thereby alter behavior.[26] A persistent challenge for Internet law scholars has been to define a set of criteria to evaluate the legitimacy of such restrictions.[27] These efforts, however, are unsatisfactory in addressing filtering that is ever more common and more technologically sophisticated. Pioneers such as John Perry Barlow[28] and John Gilmore[29] advocate cyberlibertarianism, arguing that nothing should be blocked, and that perhaps nothing can be blocked. Amitai Etzioni has written that implementing localized standards is technically possible and desirable, particularly to protect minors.[30] Cheryl Preston has sought filtering of "harmful" content based on American norms.[31] David Johnson and David Post look to Internet-specific forms of democratic organization to resolve the question.[32] Thomas Schultz supports filtering to protect a country's core values, based on social contract theory and a Hegelian state that embodies collective will.[33] Kevin Werbach opposes filtering because of censorship's threat "to the structure and universality of the Internet."[34]

---

25. *See generally* Zittrain & Palfrey, *supra* note 11, at 2 (defining "filtering").

26. Filtering is information regulation via code—computer hardware and software—rather than law, though its technical measures are frequently backed by legal mandates. *See* LAWRENCE LESSIG, CODE: VERSION 2.0, at 24, 121–32 (2006) (describing modes of regulation).

27. *See, e.g.*, Ann Bartow, *Women in the Web of Secondary Copyright Liability and Internet Filtering*, 32 N. KY. L. REV. 449, 481–87 (2005) (noting that filtering criteria reflect broader patterns of gender and social power).

28. John Perry Barlow, A Declaration of the Independence of Cyberspace (1996), *available at* http://homes.eff.org/~barlow/Declaration-Final.html. *But see* Glenn Harlan Reynolds, *Does Power Grow Out of the Barrel of a Modem? Some Thoughts on Jack Goldsmith and Tim Wu's* Who Controls the Internet?, 18 STAN. L. & POL'Y REV. 432, 433 (2007) ("Barlow's vision of a separate and untouchable cybersphere is increasingly unrealistic.").

29. Gilmore famously stated that "[t]he Net interprets censorship as damage and routes around it." Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62.

30. *See* Amitai Etzioni, *On Protecting Children from Speech*, 79 CHI.-KENT L. REV. 3, 50–52 (2004).

31. See Cheryl B. Preston, *Making Family-Friendly Internet a Reality: The Internet Community Ports Act*, 2007 BYU L. REV. 1471, 1483–85.

32. *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1391–1402 (1996).

33. Thomas Schultz, *Carving Up the Internet: Jurisdiction, Legal Orders and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 799, 806 (2008).

34. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 367 (2008).

These approaches have significant shortcomings. Some approaches treat restrictions as binary—either all-pervasive censorship or an unlimited marketplace of ideas. Other approaches canonize one normative view of content as ideal: banning hate speech is bad, but blocking pornography is desirable. And some approaches defer to local standards without offering methods to assess them. Searching for a robust evaluative methodology has particular salience given the surge in efforts to filter the Internet in the United States[35]—for example, suggestions that ISPs should filter copyrighted material,[36] pornography should be segregated onto a separate "channel,"[37] or ISPs should limit subscribers' access to Web sites[38] or Usenet news groups (on topics from SCUBA diving[39] to radio astronomy[40]) to reduce distribution of child pornography.[41] Current theoretical approaches to Internet filtering falter when confronted with censorship by democratic countries.

Moreover, although these countries increasingly agree that Internet users should be prevented from accessing certain content, their norms regarding banned content vary widely. There is scant agreement on what material ought to be off-limits—that is, material whose viewing should be blocked proactively rather than punished after the fact.[42] This divergence makes it hard to assess filtering's legitimacy other than by whether the country blocks material one finds objectionable and leaves other content accessible.[43] Importing

35. The FCC, though, has punished ISPs that unilaterally filter, voting to require Comcast not to block customers' file-sharing traffic. *E.g.*, John Dunbar, *FCC Rules Against Comcast*, WASH. POST, Aug. 2, 2008, at D2.

36. *See* Tim Wu, *Has AT&T Lost Its Mind?*, SLATE, Jan. 16, 2008, http://www.slate.com/id/2182152/.

37. Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BYU L. REV. 1417, 1426.

38. *See* Jasa Santos, *Qwest Blocks Access to Known Child Porn Sites*, CASPER STAR-TRIBUNE, July 7, 2008, *available at* http://www.trib.com/articles/2008/07/08/news/wyoming/8d7cbb0a6413fa718725747e007d4326.txt.

39. *E.g.*, *Rec.scuba*, http://groups.google.com/group/rec.scuba/topics.

40. *E.g.*, *IAC Indian Astronomy Club*, http://groups.google.com/group/indianastronomyclub.

41. McCullagh, *supra* note 3.

42. *Cf.* Jack M. Balkin, Beth S. Noveck & Kermit Roosevelt, *Filtering the Internet—A Best Practices Model*, *in* PROTECTING OUR CHILDREN ON THE INTERNET: TOWARDS A NEW CULTURE OF RESPONSIBILITY 199, 210 (Jens Waltermann & Marcel Machill eds., 2000) (noting the "wide cultural and ideological diversity" that filtering must reflect).

43. *See generally* Gordon Hull, *Overblocking Autonomy: The Case of Mandatory Library Filtering Software*, 42 CONTINENTAL PHIL. REV. 81 (2009), *available at* http://www.springerlink.

U.S. standards for content is unhelpful—the limited restrictions on expression permitted by America's Constitution are atypically narrow.[44] Many Americans would object to the United Arab Emirates' (UAE) decision to block all sites hosted in Israel's top-level domain;[45] UAE citizens might object to the United States' willingness to tolerate sites offering pornography or endorsing alcohol consumption.[46] Britain[47] and Canada[48] filter child pornography, and Australia is testing this approach,[49] yet in Japan, possession of child pornography is lawful.[50] British defamation law prohibits more speech than its American counterpart doctrine, despite their shared historical roots.[51] Anti-Semitic speech is permitted in Skokie but banned in Toronto.[52] Even U.S. standards vary by subject matter. American government officials criticize search engines when they help censor

---

com/content/71742w01k1432463/fulltext.pdf (describing library filtering of pornography as the construction of a space purged of "deviant" sexuality).

44. *See, e.g.*, Adam Liptak, *Unlike Others, U.S. Defends Freedom to Offend in Speech*, N.Y. TIMES, June 12, 2008, at A1; Frederick Schauer, *The Exceptional First Amendment* 23 (John F. Kennedy Sch. of Gov't Faculty Research Working Paper Group, Paper No. 05-021, 2005), *available at* http://web.hks.harvard.edu/publications/getFile.aspx?Id=167.

45. OPENNET INITIATIVE, INTERNET FILTERING IN THE UNITED ARAB EMIRATES 6 (2009), http://opennet.net/sites/opennet.net/files/ONI_UAE_2009.pdf.

46. *Id*.

47. Martin Bright, *BT Puts Block on Child Porn Sites*, OBSERVER, June 6, 2004, at 7.

48. *See* Cybertip.ca, Cleanfeed Canada, http://cybertip.ca/app/en/cleanfeed (follow "Does the system filter legitimate, non-child pornography sites? (show)" hyperlink) (last visited Oct. 23, 2009) (stating that Canada's Cleanfeed system blocks "access to Internet addresses specifically containing child pornography images").

49. Bambauer, *supra* note 22, at 10.

50. Jake Adelstein, *This Mob Is Big in Japan*, WASH. POST, May 11, 2008, at B2 (noting that producing or distributing child pornography, while illegal, is rarely investigated).

51. *See, e.g.*, Harrods Ltd. v. Dow Jones & Co., [2003] EWHC (QB) 1162, [38]–[39] (Eng.); Demon v. Godfrey Internet Ltd., [2001] Q.B. 201, 204 (Eng.) (explaining that under English law, unlike in the United States, a defendant publisher has the burden of proving innocence). Protections for reporting on issues of public interest, however, have expanded recently. Jameel v. Wall St. J. Europe SPRL, [2006] UKHL 44 (U.K.); Reynolds v. Times Newspapers Ltd., [2001] 2 AC 127, 176–77 (Eng.).

52. *Compare* Nat'l Socialist Party of Am. v. Village of Skokie, 432 U.S. 43, 43 (1978) (per curiam) (overturning an injunction prohibiting public display of "hatred against persons of Jewish faith or ancestry"), *with* Can. (Human Rights Comm'n) v. Taylor, [1990] 3 S.C.R. 892, 941 (Can.) (upholding a cease and desist order prohibiting telephone calls containing "statements denigrating the Jewish race or religion").

political speech in China[53] and when they fail to censor copyrighted materials there.[54]

Even in democratic countries, the types of content restricted and the standards for doing so diverge. Comparing nations' online censorship from one normative perspective is unhelpful. Countries with similar views on banning information fare well, and countries with contrary attitudes fare poorly. Evaluators tend to approve of like-minded thinkers. Restricting Internet information is a policy question about choosing among multiple regulatory endpoints that are both possible and legitimate.[55] This dilemma—choosing among divergent substantive values—parallels classic problems in American constitutional law. Scholars such as Alexander Bickel, John Hart Ely, and Jeremy Waldron have come to a similar solution: turning from the fight over normative choices to building consensus about the process used to resolve that contest.[56] Law's historic focus on process can serve debates over Internet censorship well. Thus, this Article argues that to assess whether a given approach to censorship is legitimate, legal scholars need an analytical tool that recognizes different tradeoffs but enables rigorous comparative analysis.

B. A New Hope

This Article proposes an alternative methodology that addresses these shortcomings: a process-oriented framework to evaluate the legitimacy of Internet filtering. The approach draws upon scholarship in deliberative democracy, health care decisionmaking, labor and environmental law, and cyberlaw. To assess legitimacy, the Framework asks four questions. First, is the country *open* about its Internet censorship and why it restricts information? Second, is the state *transparent* about what material it filters and what it leaves untouched? Third, how *narrow* is the country's filtering—that is, how well does the content actually blocked and not blocked by filtering correspond to the country's filtering criteria? Finally, to what degree can citizens participate in decisionmaking about these restrictions, such that censors are *accountable*? Legitimate censorship is open,

53. *See, e.g.*, *Yahoo Criticized in Case of Jailed Dissident*, N.Y. TIMES, Nov. 7, 2007, at C3.

54. OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2008 SPECIAL 301 REP. 7, *available at* http://www.ustr.gov/sites/default/files/asset_upload_file553_14869.pdf (criticizing the Chinese search engine Baidu).

55. I thank Peter Hammer for this point.

56. *See infra* notes 181–85 and accompanying text.

transparent about banned content, effective yet narrowly targeted, and responsive to citizens' preferences (but not overly so).

Evaluating legitimacy from a process-oriented perspective does not replace values-driven normative analysis. Indeed, the Framework bolsters process-oriented examinations by enabling application of different normative models.[57] If a state's censorship program is openly and fully described, carefully targeted, and responsive to popular demand, then objections are properly aimed not at the state's filtering program, but at the country's larger values and policy choices. For example, Saudi Arabia might filter sites about minority faiths in a way that is straightforward, narrow, and popular, yet one might still find that decision unacceptable.[58] The Framework's goal is not to end analysis or discussions based on values, but to spark and clarify them. A process-based approach to this question best comports with the diversity of views on banning Internet materials.

C. The Framework's Roots

The Framework's approach is rooted in the law's historical preoccupation with questions of process, and it parallels proposals based on deliberative democracy in other contested policy areas.[59] Similar tools have been deployed when multiple legitimate outcomes are possible and even likely, such as allocating health care and regulating working conditions.

Process-based approaches often seek to mediate policy disagreements based on strongly held values, with the goal of convincing participants that an outcome is reasonable even if they disagree with it. Consider a dying patient in the United States who wants a health care plan to pay for experimental treatment.[60] (Assume that the treatment may have clinical benefit, but it has not been proven effective.) The plan and the patient have different, competing

---

57. Jack Balkin, Beth Noveck, and Kermit Roosevelt propose an analogous method for rating Web sites' content via application of different third-party "templates." *See* Balkin et al., *supra* note 42, at 210.

58. *See generally* HUMAN RIGHTS WATCH, COUNTRY SUMMARY: SAUDI ARABIA (2008), http://hrw.org/wr2k8/pdfs/saudiarabia.pdf (assessing the human rights climate in Saudi Arabia).

59. *See generally* JAMES S. FISHKIN, DEMOCRACY AND DELIBERATION (1991) (analyzing methods for combining political equality and deliberation); DELIBERATIVE DEMOCRACY AND HUMAN RIGHTS (Harold Hongju Koh & Ronald C. Slye eds., 1999) (seeking to reconcile human rights and political deliberation).

60. *See* Norman Daniels & James E. Sabin, *Last Chance Therapies and Managed Care: Pluralism, Fair Procedures, and Legitimacy*, HASTINGS CENTER REP., Sept.–Oct. 1998, at 27, 28.

value sets. The plan seeks to ensure all its members have access to scarce medical resources, discover new therapies through clinical trials, and avoid negative public attention. The patient wants to receive therapy that may extend her life, improve her life's quality, or cure a disease. There is no single way to balance these competing claims; it may be reasonable to provide women with breast cancer autologous bone marrow transplants[61] but deny them access to experimental cancer drugs (which may be highly toxic).[62] The health plan seeks outcomes that seem legitimate to affected patients, other members, and the public.

Norman Daniels and James Sabin suggest that the keys to such legitimacy are process-oriented: making decisions public; explaining how decisions reasonably provide benefits to a heterogeneous group of members given resource constraints; allowing appeal; and creating regulation to enforce these factors.[63] Daniels and Sabin extend the proposal to all limit-setting decisions by providers such as health management organizations (HMOs), arguing that decisionmaking criteria should be public, relevant, and subject to challenge, such that "all fair-minded parties" would agree they are germane.[64] Patients or health plan accountants may disagree with a particular outcome—and, given their differing preferences and values, one side is likely to do so—but they are more likely to accept the legitimacy of the outcome if they trust how the decision was made.[65] As with censorship, allocating health care resources requires selecting from multiple legitimate options. Outcome-based normative analysis is not determinative, and so legitimacy must rest upon a process viewed as relevant and fair.

Similarly, setting labor standards can result in multiple legitimate outcomes that prioritize different interests and values. Under

---

61. *But see* Peter D. Jacobson, Richard A. Rettig & Wade M. Aubry, *Litigating the Science of Breast Cancer Treatment*, 32 J. HEALTH POL. POL'Y & L. 785, 790 (2007) (noting that randomized clinical trials showed transplants to be no more effective than standard chemotherapy).

62. *Cf.* Abigail Alliance for Better Access to Developmental Drugs v. Eschenbach, 485 F.3d 695, 711 (D.C. Cir. 2007), *cert. denied*, 128 S. Ct. 1069 (2008) (finding no constitutional right to access experimental therapies).

63. *See generally* Daniels & Sabin, *supra* note 60 (analyzing the allocation of benefits among breast cancer patients).

64. Norman Daniels & James Sabin, *The Ethics of Accountability in Managed Care Reform*, 17 HEALTH AFF. 50, 57 (1998).

65. *Id.* at 59 (noting that with a legitimate process, "even those who say that the specific outcome is wrong must admit that it is a case of reasonable disagreement").

pressure from activists, corporations have begun to adopt voluntary codes of conduct for working conditions.[66] These codes, while oriented around the International Labour Organization's principles, differ significantly in their requirements for issues such as wages, nondiscrimination, and freedom of association.[67] Should factories pay workers (at least) the legal minimum wage, or a living wage?[68] May they discriminate based on sexual orientation? (American federal employment law permits such discrimination;[69] however, French law bans it.[70]) While participants tend to agree that labor regulation is needed, they diverge about what rules are proper.

The Ratcheting Labor Standards (RLS) approach tackles this heterogeneity by combining voluntary regulation, monitoring, reporting, and external analysis to measure how well firms such as Nike comply with their adopted code of conduct.[71] Companies select both the standards by which they are measured and the evaluator. Analysis and public scrutiny assess what behavior suffices for legitimacy and improve monitoring through feedback and competition. RLS inherently accepts that more than one labor code can be valid—standards for a factory in Vietnam will necessarily differ from those in Vienna.[72] Rather than assessing labor standards from a single values-based perspective, RLS focuses on process: self-regulation, checked by monitoring and disclosure, with feedback to refine standards, and thus develop legitimacy.

---

66. *See generally* Richard Locke et al., *Beyond Corporate Codes of Conduct: Work Organization and Labour Standards at Nike's Suppliers*, 146 INT'L LABOR REV. 21, 22–24 (2007) (discussing Nike's efforts to enforce minimum labor standards in the wake of public pressure).

67. *See* Dara O'Rourke, *Outsourcing Regulation: Analyzing Nongovernmental Systems of Labor Standards and Monitoring*, 31 POL'Y STUD. J. 1, 7–9 (2003).

68. *See id.* at 9.

69. *See, e.g.*, James E. Snyder & Reva S. Bauch, *Sexual Orientation Discrimination in the Workplace*, CHI. BAR ASS'N REC., Nov. 2006, at 44, 45.

70. Julie Chi-Hye Suk, *Equal by Comparison: Unsettling Assumptions of Antidiscrimination Law*, 55 AM. J. COMP. L. 295, 302–03 (2007).

71. Archon Fung, Dara O'Rourke & Charles Sabel, *Realizing Labor Standards: How Transparency, Competition, and Sanctions Could Improve Working Conditions Worldwide*, BOSTON REV., Feb.–Mar. 2001, at 4 [hereinafter Fung et al., *Realizing Labor Standards*]; *see also* Archon Fung, *Deliberative Democracy and International Labor Standards*, 16 GOVERNANCE: INT'L J. POL'Y, ADMIN., & INSTITUTIONS 51, 60 (2003) [hereinafter Fung, *Deliberative Democracy*].

72. *See* Fung et al., *Realizing Labor Standards*, *supra* note 71, at 4 ("RLS encourages the incremental realization of demanding labor standards over time without imposing a uniform, and potentially protectionist, standard upon diverse contexts.").

Regulation becomes more challenging when there are multiple sets of guiding norms with plausible claims to legitimacy. As health care rationing, working condition ordinances, and Internet filtering demonstrate, regulators should utilize an approach that allows different sets of tradeoffs and that achieves legitimacy through a rigorous, inclusive process. The next Part describes the application of this approach to Internet filtering by elucidating the four parts of this Article's new, process-based evaluative method.

II. A METHOD IN FOUR PARTS

To evaluate a country's Internet filtering practices, the Framework assesses openness, transparency, narrowness, and accountability. These principles draw together common elements from scholarly analysis of Internet filtering and proposals to regulate it. These principles have not previously been used to create an integrated methodology, however. The goal of the Framework is to evaluate how well a country describes what it censors and why, whether it effectively blocks proscribed material while leaving permitted content untouched, and how much its citizens can participate in filtering decisions.

A. Openness

The Framework's first criterion is openness: does the country admit to filtering the Internet and describe clearly its rationale for blocking? Whereas censorship that is clearly disclosed and carefully explained is more likely to be legitimate, censorship that is covert, or that rests on flimsy pretexts, is less acceptable.

Compare Saudi Arabia and China, for example. Saudi Arabia prevents users from accessing most pornographic and erotic material, along with some pages on certain sects of Islam, other minority faiths, alcohol, and illegal drugs.[73] The Kingdom is open about censorship: its Communications and Information Technology Commission explains the filtering on its Web site.[74] Saudi Arabia justifies these practices by citing supporting materials that discuss social harms from pornography, such as the Koran, an article on Internet pornography

73. *See* OPENNET INITIATIVE, INTERNET FILTERING IN SAUDI ARABIA 3–5 (2009), http://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf.

74. *See* Internet.gov.sa, Content Filtering in Saudi Arabia, http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia (last visited Oct. 23, 2009).

written by Cass Sunstein, and the 1986 U.S. Attorney General's Commission on Pornography.[75] Moreover, Saudi Arabia's Council of Ministers promulgated a 2001 resolution describing prohibited Internet content, including material "breaching public decency," "infringing the sanctity of Islam," and running "contrary to the state or its system."[76] Finally, users who attempt to reach a filtered site receive a "block page" to inform them that the disruption is deliberate.[77]

Saudi Arabia discloses its online censorship and elucidates its underlying rationales. China, by contrast, operates the world's most extensive and sophisticated Internet censorship system, yet rarely admits that the country filters information.[78] The Chinese filtering apparatus is multilayered.[79] Users are not informed when they are prevented from reaching proscribed material; instead, their Internet connections are reset, or their e-mail messages never reach their destinations.[80] Intentional censorship is difficult to distinguish from technical errors. Queries for sensitive terms, such as "free tibet," on Chinese search engines generate results that deliberately purge blocked sites.[81] (Some search engines voluntarily notify users that

---

75. Internet Servs. Unit, King Abdulaziz City for Sci. & Tech., Introduction to Content Filtering, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm (last visited Oct. 23, 2009).

76. Arab Media: Saudi Internet Rules, Council of Ministers Resolution (Feb. 12, 2001), http://www.al-bab.com/media/docs/saudi.htm.

77. *See* Internet.gov.sa, New Block Page, http://www.internet.gov.sa/news/new-block-page/view?set_language=en (last visited Oct. 23, 2009) (describing and linking to the block page that a user will receive when trying to reach a filtered site). *See generally* Alfred Hermida, *Saudis Block 2,000 Websites*, BBC NEWS, July 31, 2002, http://news.bbc.co.uk/2/hi/technology/2153312.stm (discussing Saudi Arabia's Internet filtering practice).

78. *See, e.g.*, *Access to Information and Media Control in the People's Republic of China: Hearing Before the U.S.-China Economic and Security Commission*, 110th Cong. 77 (2006) (statement of Dr. Ronald J. Deibert, Associate Professor of Political Science and Director of Citizen Lab, University of Toronto), *available at* http://www.uscc.gov/hearings/2008hearings/transcripts/08_06_18trans/08_06_18_trans.pdf ("Official acknowledgement of these practices has been inconsistent at best, deceitful at worst."); Declan McCullagh, *China: We Don't Censor the Internet. Really*, CNET NEWS, Oct. 31, 2006, http://news.cnet.com/China-We-dont-censor-the-Internet.-Really/2100-1028_3-6130970.html ("In China, we don't have software blocking Internet sites. . . . We do not have restrictions at all." (quoting a Chinese government official)). *See generally* OPENNET INITIATIVE, *supra* note 13 (describing China's Internet filtering system); Carolyn Duffy Marsan, *Chinese Internet Censorship: An Inside Look*, NETWORK WORLD, May 12, 2008, http://www.networkworld.com/news/2008/051208-china-internet.html (same).

79. OPENNET INITIATIVE, *supra* note 13, at 9.

80. *Id.* at 17, 22.

81. OpenNet Initiative, Probing Chinese Search Engine Filtering (Aug. 19, 2004), http://opennet.net/bulletins/005/.

results are censored.[82]) Even users who are generally aware that China prevents access to some material may be frustrated in attempting to determine what content is blocked, and why. China's lack of openness is pernicious. Many Internet users do not know they are operating in an information environment deliberately skewed by the government; formally, they have no reason to be wary because China does not usually admit to filtering.

Yet openness is easy to achieve. Nearly all filtering technology can display a block page when a user is prevented from accessing banned material.[83] The page, which can be customized, informs the user that their inability to reach a Web site is a deliberate policy choice rather than a technical error.[84] It is easy and inexpensive to be open about filtering. Countries that nonetheless obfuscate their censorship—such as Uzbekistan, which redirects users from banned sites to innocuous ones—seek to conceal this filtering from citizens.[85]

Governments generally advance two reasons for censoring the Net. The first reason offered for filtering is that banned content harms the community, regardless of any individual benefit. Singapore bans "material that is objectionable on the grounds of public interest, public morality, public order, public security, [and] national harmony."[86] The second reason offered for filtering is that filtered material harms the individual, who may not realize the danger of the material or who may find it attractive nonetheless. Vietnam claims its censorship "policy is to apply measures to prevent youngsters from unhealthy sites."[87] Neither of these rationales is strengthened by undisclosed restrictions—rather, notice that a country blocks access reinforces the material's harmfulness and the societal judgment that it

82. Nart Villeneuve, Perspectives on Transparency (June 26, 2008), http://www.nartv.org/2008/06/26/perspectives-on-transparency/.

83. *See, e.g.*, CISCO SYSTEMS, CISCO SECURITY APPLIANCE COMMAND LINE CONFIGURATION GUIDE, VERSION 7.2–CONFIGURING HTTP FILTERING (2008), http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/filter.html#wp1042538 (explaining how to configure HTTP filtering so that users are redirected to a block page when trying to reach a blocked site).

84. *See, e.g.*, Internet.gov.sa, *supra* note 77.

85. Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, *in* ACCESS DENIED, *supra* note 9, at 5, 13.

86. Internet Code of Practice § 4(1) (1997) (Singapore), *available at* http://www.mda.gov.sg/wms.file/mobj/mobj.981.internet_code_of_practice.pdf.

87. *Politics a No-No but Porn OK*, AUSTRALIAN, Aug. 15, 2006, at 33 (quoting Vietnamese Foreign Ministry spokesperson Le Dung).

deserves to be proscribed.[88] In short, countries confident that censorship advances their citizens' welfare have no reason to hide their actions. Countries that disclose restrictions are more likely to have legitimate controls rather than ones designed to protect those governing, but not the governed.

The openness criterion probes whether a state admits that it censors the Internet and why.

B. Transparency

The Framework's second prong is transparency: is the country clear about what material it filters, and is the country specific about the criteria it uses to determine which material to block? Transparent categories and criteria allow users to assess how the list of banned content maps onto the government's rationales for information control. A country that filters the Internet to prevent harm to minors, for example, could plausibly censor Web sites offering medication without a prescription,[89] violent games,[90] or encouragement for anorexia.[91] A system targeting sexually explicit material could potentially block sites ranging from pornography to lingerie catalogs to sex education. Thailand censors pornography;[92] Iran blocks

88. *See* Schultz, *supra* note 33, at 823–28 (describing judging as catharsis). There may be a "forbidden fruit" appeal to banned material, but it seems more likely to attract users to specific contraband content, rather than general categories of sites.

89. *Cf.* Erik Eckholm, *Abuses Are Found in Online Sales of Medication*, N.Y. TIMES, July 9, 2008, at A21 (discussing possible solutions to the problem that "anyone of any age can obtain dangerous and addictive prescription drugs with the click of a mouse," including requiring certification for online pharmacies).

90. *Cf.* Commission of the European Communities, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Protection of Consumers, in Particular Minors, in Respect of the Use of Video Games, at 8 COM (2008) 207 final (Apr. 22, 2008), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0207:FIN:EN:PDF (recommending a "swift and effective mechanism for age verification" to protect minors from harmful online video games).

91. *See, e.g.*, Doreen Carvajal, *French Legislators Approve Law Against Web Sites Encouraging Anorexia and Bulimia*, N.Y. TIMES, Apr. 15, 2008, http://www.nytimes.com/2008/04/15/world/europe/15iht-paris.4.12015888.html; *cf.* Thomas Catan, *Online Anorexia Sites Shut Down Amid Claims They Glorify Starvation*, TIMES ONLINE, Nov. 22, 2007, http://www.timesonline.co.uk/tol/life_and_style/health/article2916356.ece (discussing Spain's decision to shut down four pro-anorexia websites after receiving a complaint that they were endangering the lives of teenage girls).

92. OPENNET INITIATIVE, THAILAND 4 (2007), http://opennet.net/sites/opennet.net/files/thailand.pdf.

provocative attire sites as well;[93] Saudi Arabia adds family planning sites.[94] Rationales are general. Transparency presses a state to go beyond the reasons for filtering and explain precisely which content runs counter to its goals.

Disclosure also pushes a government to go on record about the types of content it purports to block; testing (covered in the next Section, under narrowness) reveals the accuracy of those statements. Transparency extends the openness analysis. A country could be open without being transparent. For example, Tunisia blocks information "likely to upset public order"[95] and "contrary to public order and good morals"[96] but disguises what it actually censors.[97] When users try to reach a filtered site, they get an error message stating the site is unavailable, rather than one indicating it is blocked. It is also possible to have transparency without openness: China hedges about whether it filters, but some domestic search engines disclose when they censor query results.[98] Yahoo!'s Chinese search engine is a contrast in transparency: it lists sites censored for copyright violations,[99] but does not list those blocked for political reasons.[100] Openness assesses whether a state discloses *why* it censors. Transparency evaluates whether it describes *what* it censors.

States can disclose what material they block either formally, such as through codification in press regulations,[101] or informally, such as in

93. OPENNET INITIATIVE, INTERNET FILTERING IN IRAN 9 (2009), http://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf.

94. OPENNET INITIATIVE, *supra* note 73, at 5.

95. OPENNET INITIATIVE, TUNISIA 3 (2007), http://opennet.net/sites/opennet.net/files/tunisia.pdf (quoting Art. 9, DECREE OF THE MINISTRY OF TELECOMMUNICATIONS OF MARCH 22, 1997, and Art. 9, CODE DE LA PRESSE (translated by Harvard Law School Langdell Library)).

96. *Id.* (citing Art. 49, DECREE OF THE MINISTRY OF TELECOMMUNICATIONS OF MARCH 22, 1997 (translated by Harvard Law School Langdell Library)).

97. Tunisia displays a "404 Not Found" error page (stating that the site does not exist or cannot be found) rather than a "403 Forbidden" page (stating that the user may not reach the requested site). *Id.*; Nart Villeneuve, Tunisia: Internet Filtering (June 7, 2005), http://www.nartv.org/2005/06/07/tunisia-internet-filtering/.

98. Villeneuve, *supra* note 82 (suggesting that Western search engines such as Google have established a norm of transparency).

99. *See* http://search.help.cn.yahoo.com/h3_9.html.

100. Nart Villeneuve, *Search Monitor Project: Toward a Measure of Transparency* 7 (Citizen Lab, Occasional Paper No. 1, 2008), http://www.citizenlab.org/papers/searchmonitor.pdf.

101. Iran's Press Law of 2000, for example, prohibits insulting Islam, attacking the Leader of the Iranian Revolution, or quoting articles from groups opposing Islam. OPENNET INITIATIVE, *supra* note 93, at 4–5.

statements by government officials.[102] Formal criteria are more transparent; citizens have greater access to documented rules than to oral utterances. Clarity in blocking disclosure varies greatly. France requires filtering of hate speech,[103] which is well-defined under its civil and criminal laws as targeting a person or group based on their origin, ethnic group, nationality, race, or religion.[104] China, by contrast, is vague about the material it filters, typically describing it as "unhealthy,"[105] "spread[ing] rumours,"[106] "destroy[ing] national unity,"[107] or even just not "wholesome."[108] Moreover, China's formal regulation of Internet content comprises a morass of statutes, regulations, and decrees from numerous government entities.[109] This complicates determining what content is subject to censorship. China's opacity is deliberate: it presses online service providers such as Google and Sina to censor widely, given that the consequences of erroneously allowing access to prohibited material can include loss of an operating license or even criminal sanctions.[110] It is more difficult to assess what types of content are subject to blocking in China than in France; therefore, France's censorship is more transparent overall than China's censorship.

In addition to disclosing what content is filtered, states vary in how clearly they describe criteria for determining whether material is proscribed. More precise definitions enhance transparency. For

---

102. *See supra* note 87 and accompanying text.

103. OPENNET INITIATIVE, *supra* note 15; *see also, e.g.*, Tribunal de Grande Instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, Ordonnance de référé (Order for Summary Judgment), No. RG 00/05308, at 3, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf (requiring Yahoo!'s French subsidiary to disable access to auctions of Nazi memorabilia).

104. Arts. 23–24, Law on Press Freedom, J.O., July 29, 1881, at 4202, *available at* http://www.lexinter.net/lois/provocation_aux_crimes_et_delits.htm (translation by author).

105. Ben Blanchard, *China Won't Guarantee Web Freedom over Olympics*, REUTERS, May 8, 2008, http://www.reuters.com/article/GCA-Olympics/idUSPEK14583520080508 (quoting Technology Minister Wan Gang).

106. Mark O'Neill, *Beijing Closes Net Around Web Sites*, S. CHINA MORNING POST, Oct. 4, 2000, at 10.

107. *Id.*

108. Marsan, *supra* note 78.

109. Melinda Liu & Quindlen Krovatin, *Big Brother Is Talking*, NEWSWEEK (PACIFIC ED.), Oct. 17, 2005, at 20 (estimating thirty-eight different regulations); Cong.-Executive Comm'n on China, Agencies Responsible for Censorship in China, http://www.cecc.gov/pages/virtualAcad/exp/expcensors.php (last visited Oct. 23, 2009) (listing nine governmental agencies).

110. *See, e.g.*, Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. TIMES MAG., Apr. 23, 2006, at 64 (describing Chinese pressure to censor and Google's acquiescence).

example, blocking "child pornography,"[111] when that material is defined carefully in a state's criminal code,[112] is more transparent than banning "nudity"[113] when that content includes pornographic images, pictures of Michelangelo's statue of David, and photos of prisoner abuse at Abu Ghraib.[114] The clearer the criteria, the less discretion government officials or ISPs have to define other sites as proscribed. Uzbekistan's Law on Principles and Guarantees on Access to Information permits restricting information "in the name of maintaining safety and protecting the moral values of society"—a vague guideline that offers cover for censoring political opposition sites and coverage critical of the authoritarian government.[115] Generality in defining what material is subject to filtering confers considerable power on censors, whose ad hoc judgments are more difficult to challenge when criteria are broad and can act as a pretext for covert censorship.

Transparency checks how clearly a state describes the material that it seeks to block. It enables comparison between stated motives and the content a state targets based on these motives. Transparent censorship specifies both the categories of banned content and rules for determining whether material falls within them. Together, transparency and openness reveal a sovereign's public claims about its information control.

C. Narrowness

The third criterion of the Framework is narrowness: how closely does empirical data about what a country actually blocks match the government's description of its censorship? This Framework prong

---

111. *E.g.*, Cybertip.ca, *supra* note 48 (describing a system deployed in Canada to "prevent access to . . . child pornography images").

112. CRIMINAL CODE, R.S.C., ch. C-46, § 163.1(1) (1985) (Can.) (defining "child pornography").

113. *See* McAfee, 4.x Database: Secure Computing, http://www.securecomputing.com/index.cfm?skey=86#categories (last visited Oct. 23, 2009) (defining nudity as "non-pornographic images of the bare human body").

114. *See, e.g.*, Xeni Jardin, *BoingBoing Banned in UAE, Qatar, Elsewhere*, BOING BOING, Feb. 27, 2006, http://www.boingboing.net/2006/02/27/boingboing-banned-in.html (describing the blocking of the blog Boing Boing because the filtering software SmartFilter classified it as "nudity" even though less than 1 percent of posts contain nudity).

115. Inera Safargalieva, *Uzbek Media and the Authorities—A Strange Relationship*, *in* Fifth Central Asian Media Conference, Sep. 17–18, 2003, *OSCE Representative on Freedom of the Media, Central Asia—In Defence of the Future* 259, 263, *available at* http://www.osce.org/publications/rfm/2004/02/12243_101_en.pdf.

validates the claims a state makes (if any) about its filtering through empirical testing by third parties. The openness and transparency criteria assess what a country says about its censorship; the narrowness criterion examines what it does.

Narrowness considers both overinclusiveness and underinclusiveness. Most, if not all, Internet filtering systems will be overbroad (blocking innocent content), underbroad (failing to block proscribed material), or both. Both overinclusion and underinclusion are problematic. Overbroad filtering keeps citizens from accessing legitimate material. Underbroad blocking means a country fails to censor content it views as dangerous.

Overinclusive censorship can be deliberate or inadvertent. Vietnam claims to only filter Web sites that are harmful to minors, yet its system concentrates on ensuring that political opposition sites remain inaccessible.[116] This is a deliberate strategy to protect Vietnam's single-party Communist system.[117] Overbreadth may also represent a considered policy choice to tolerate false positive results to minimize false negative ones. Inadvertent filtering can result from classification errors, such as when Secure Computing's SmartFilter software categorized a Kentucky newspaper as pornography,[118] or from crude censorship techniques, such as when ISPs prevented access to over a million unrelated Web sites to filter 400 with child pornography, at Pennsylvania's behest.[119]

Underinclusive censorship occurs when users can routinely reach banned content. (This differs from accessing blocked content via circumvention techniques that deliberately evade filtering.[120])

---

116. *See supra* note 87 and accompanying text.

117. *See* U.S. DEP'T OF STATE, BUREAU OF DEMOCRACY, HUMAN RIGHTS & LABOR, VIETNAM: 2007 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES (2008), *available at* http://www.state.gov/g/drl/rls/hrrpt/2007/100543.htm (describing Vietnam's efforts to restrict publication of alternative political viewpoints and its Internet censorship practices).

118. OPENNET INITIATIVE, INTERNET FILTERING IN THE UNITED ARAB EMIRATES IN 2004–2005: A COUNTRY STUDY 13 n.50 (2005), http://opennet.net/sites/opennet.net/files/ONI_UAE_Country_Study.pdf.

119. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 633–34, 650–52, 655 (E.D. Pa. 2004).

120. *See generally* Nart Villeneuve, *Technical Ways to Get Round Censorship*, *in* REPORTERS WITHOUT BORDERS, HANDBOOK FOR BLOGGERS AND CYBER-DISSIDENTS (2005), *available at* http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf (providing a list of filter-circumvention techniques and their associated advantages and disadvantages); Hiawatha Bray, *Beating Censorship on the Internet*, BOSTON GLOBE, Feb. 20, 2006, at A10 (discussing the use of networks of proxies to obfuscate web-surfers' computer identities).

Singapore operates an underinclusive filtering system by design; though all pornography is eligible for blocking, only a few sites are symbolically targeted.[121]

Countries can have both overbroad and underbroad censorship. Vietnam's filtering demonstrates both flaws: it fails to block any pornographic sites, which are formally banned, but heavily censors political sites.[122] Australia blocks some—but by no means all—pornographic sites, yet also censors a dentist and a canine kennel.[123]

Commentary on filtering tends to ignore the problem of underinclusion. Underbroad censorship, however, causes concern for three reasons. First, assuming that a country adequately justifies blocking access to harmful content, allowing users to view it is undesirable. In 2006, British Telecom detected 35,000 daily attempts to access child pornography.[124] Until the end of 2007, however, it was the only British ISP to block such attempts.[125] If child pornography should be censored, then allowing users to see it because of different ISP practices is normatively problematic.[126]

Second, censorship that targets some, but not all, content that is nominally proscribed may enable selective enforcement. Egypt has used a court decision that sanctioned the blocking of sites threatening national security to prevent online access to Muslim Brotherhood, the country's major political opposition movement.[127] Censorship

---

121. OPENNET INITIATIVE, SINGAPORE 1 (2007), http://opennet.net/sites/opennet.net/files/singapore.pdf.

122. OPENNET INITIATIVE, *supra* note 116, at 4; *see also supra* note 87 and accompanying text.

123. David Kravets, *WikiLeaks Exposes Australian Blacklist*, WIRED, Mar. 19, 2009, http://www.wired.com/threatlevel/2009/03/wikileaks-expos/. The list is available at http://www.wikileaks.org/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist%2C_18_Mar_2009.

124. Tim Richardson, *Cleanfeed Working Overtime, Says BT*, REGISTER, Feb. 7, 2006, http://www.theregister.co.uk/2006/02/07/bt_cleanfeed_iwf/.

125. Britain's other ISPs "voluntarily" adopted Cleanfeed by the end of 2007, as demanded by UK Home Office Minister Vernon Croaker. Frank Fisher, *Caught in the Web*, GUARDIAN, Jan. 17, 2008, http://www.guardian.co.uk/commentisfree/2008/jan/17/caughtintheweb.

126. *But see* Richard Clayton, *Failures in a Hybrid Content Blocking System*, *in* PRIVACY ENHANCING TECHNOLOGIES: 5TH INTERNATIONAL WORKSHOP PET 2005, at 78, 82–89 (George Danezis & David Martin eds., 2006) (describing technical problems with Cleanfeed and demonstrating how it can be used to create an index of child pornography sites).

127. HUMAN RIGHTS WATCH, COUNTRY PROFILES: EGYPT (2005), http://www.hrw.org/reports/2005/mena1105/4.htm; *see also* Sarah El Sirgany, *Al-Ahram Reverses Internet Block on Blogs*, DAILY NEWS EGYPT, Aug. 15, 2006, *available at* http://www.dailystaregypt.com/article.aspx?ArticleID=2615.

becomes a weapon in a government's arsenal, deployed arbitrarily rather than enforced consistently.

Finally, filtering that fails to block forbidden material—especially badly flawed or nominal blocking—undercuts the justification for restricting access. The rationale for censorship is that some content is sufficiently harmful to warrant suppression; if much of it remains available, the country's efforts are likely pretextual.

Therefore, assessing whether a state's censorship is underbroad, overbroad, or both, requires careful empirical testing. This is challenging; the number of Web sites is effectively infinite, and testing even a representative sample is nearly impossible. Watchdog organizations such as the OpenNet Initiative, Human Rights Watch, and Reporters Without Borders employ two approaches. First, they test an index of popular Web sites in a representative set of categories (such as news sources, human rights, and pornography) that may be blocked.[128] Second, they check sites on topics sensitive to a given country, such as pages about the Falun Gong movement in China.[129] For countries employing commercial filtering software, they can check sites with known categories to establish which ones that nation wants to block.[130]

In future research, particularly under the Framework's aegis, testing that assesses narrowness should include a range of sites in zones of content a state has vowed to restrict, in areas it is suspected of covertly filtering (if any), and in categories that other states block. The first list checks the effectiveness of a country's blocking. The second and third evaluate whether the government is forthright about material it restricts.

Testing results show what types of sites a country filters (though not a comprehensive list of blocked sites). This empirical data also demonstrates underbreadth and overbreadth, along with how broad

---

128. *See, e.g.*, OPENNET INITIATIVE, INTERNET FILTERING IN VIETNAM IN 2005–2006: A COUNTRY STUDY app. 2 (2006), http://opennet.net/studies/vietnam (displaying which sites on ONI's "[G]lobal List" were blocked in Vietnam); *see also id.* § 3.A (describing testing methodology).

129. *See, e.g.*, Paul Wiseman, *In China, a Battle over Web Censorship*, USA TODAY, Apr. 23, 2008, at 1A (describing searches for specific banned keywords on the Internet in China); HUMAN RIGHTS WATCH, CHINA: WORLD REPORT 2007 (2007), http://hrw.org/englishwr2k7/docs/2007/01/11/china14867.htm (describing China's official reaction to Falun Gong); *see also* REPORTERS SANS FRONTIÈRES, INTERNET ENEMIES 19–20 (2009), http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_-3.pdf (providing a list of specific sites censored within Syria).

130. *See infra* note 319.

(measured by the number of categories filtered) and deep (measured by the percentage of sites per category) overblocking and underblocking is.[131] This enables comparison of a country's actions to its rhetoric.

One normative challenge with the narrowness evaluation is deciding whether a site—blocked or unblocked—falls within the parameters of what a country claims to filter. The more vague or unclear the criteria, the more likely a site will fall within prohibited content, or at least its penumbra. This uncertainty may be useful: it can reveal innocent content that is swept up for blocking. Some material is inherently susceptible to multiple classifications: gay or lesbian dating sites may be blocked because a country objects to dating services,[132] discussion of gay and lesbian issues,[133] or both.[134] Categorizing content involves subjective decisions; censors may be lax, strict, or simply wrong. Some overblocking and underblocking is likely even in a carefully defined, narrowly implemented filtering regime. Assessing legitimacy, in terms of narrowness, is likely to reveal a spectrum of practices rather than binary distinctions.

The three factors discussed thus far interoperate. Openness assesses how straightforward a country is in revealing its reasons for censorship. Transparency maps the content the country purports to restrict. And narrowness checks how successful the country's filtering program is and whether it suppresses different matter than it claims.

D. Accountability

The Framework's fourth criterion is accountability: to what degree can citizens influence policymaking regarding what content is censored? What measures or structures push officials to respond to constituents? What recourse is available to content owners who contend that they have been blocked erroneously?

The accountability criterion assesses how closely a country's censorship aligns with its citizens' views. It also considers how responsive blocking practices are to changes in those views. Accountability has four major aspects: participation in censorship

131. *See* Faris & Villeneuve, *supra* note 85, at 11, 18–20 (describing a method for testing Internet filtering and then listing results of those tests).

132. *See* OPENNET INITIATIVE, *supra* note 45, at 6.

133. *See, e.g.*, OPENNET INITIATIVE, INTERNET FILTERING IN YEMEN 4 (2009), http://opennet.net/sites/opennet.net/files/ONI_Yemen_2009.pdf.

134. *See* OPENNET INITIATIVE, *supra* note 93.

decisions, specification of authority, opportunity to challenge, and countermajoritarian constraints.

1. *Participation*. The accountability criterion's participation prong looks both at whether citizens influence the state's decision to block access to Internet material at all and at whether citizens influence the state's subsequent selection of sites to filter. The most accountable method of developing a state filtering program involves a democratic government's adoption of a filtering policy after public debate.[135] Though it has faced significant criticism,[136] the Digital Millennium Copyright Act (DMCA) enacted by the United States in 1998[137] is a good example of an accountable filtering program: it enjoyed public hearings and was widely supported in Congress.[138] Under the DMCA, online service providers must filter access to allegedly copyright-infringing materials[139]—either on their servers or in search results—to obtain safe harbor from secondary liability.[140] Filtering emerged from an established, participatory public regulation process.

Citizens can participate in shaping a state's filtering policy indirectly, by electing a government that implements online restrictions, and directly, by suggesting or "tagging" sites for addition to a block list. France's Interior Minister announced that French ISPs had agreed, after negotiations with the government, to filter sites containing child pornography, terrorism, or hate speech.[141] French users can submit suspect sites, and the government then decides

135. Michael Best and Keegan Wade propose a quantitative measure of how democratic a country's Internet regulation is. Michael L. Best & Keegan W. Wade, *Democratic and Anti-Democratic Regulators of the Internet: A Framework*, 23 INFO. SOC'Y 405, 410 (2007).

136. *See, e.g.*, David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 739–40 (2000); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 534–37 (1999). *But see* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 67 (2006).

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

138. The DMCA passed unanimously. Urban & Quilter, *supra* note 16, at 635.

139. *See, e.g.*, Chris Sherman, *Google Makes Scientology Infringement Demand Public*, SEARCH ENGINE WATCH, Apr. 15, 2002, http://searchenginewatch.com/2159691; *Google Asked to Delist Scientology Critics (#1)*, CHILLING EFFECTS CLEARINGHOUSE, Mar. 8, 2002, http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=232.

140. 17 U.S.C. §§ 512(c)–(d) (2006).

141. *France Blocks Online Child Porn, Terrorism, Racism*, USA TODAY, June 10, 2008, *available at* http://www.usatoday.com/tech/world/2008-06-10-france-online-porn_N.htm.

whether to include them on the list blocked by ISPs.[142] Thus, French citizens guide general censorship as well as specific filtering decisions.

Democratic government does not, however, guarantee participation. Thailand generally functions as a democracy (albeit with intermittent military coups[143]), but it operates a censorship regime with minimal citizen participation.[144] The Thai government must theoretically obtain a court order to force ISPs to block a Web site, but a government minister in May 2008 unilaterally ordered filtering of a prominent independent news portal and a social criticism site, both with popular discussion boards.[145]

It is increasingly difficult to assess whether a country is "democratic," and using formal structures of government as a reliable indicator of accountability is becoming problematic.[146] For example, a country may have the outward indicators of democratic governance, yet subvert them via voter intimidation, arbitrary arrest, media control, and state ownership of key information outlets. Russia,[147] Venezuela,[148] and Zimbabwe[149] are examples of states in which the

142. *U.S., France Move to Block Online Child Pornography*, CBC NEWS, June 10, 2008, http://www.cbc.ca/technology/story/2008/06/10/isps-porn-block.html.

143. *See, e.g.*, Seth Mydans, *Ousted Premier Is Set to Return to Thailand, Officials Say*, N.Y. TIMES, Feb. 27, 2008, at A4 (discussing the return of the former Thai Prime Minister Thaksin Shinawatra after being ousted in a 2006 military coup).

144. OPENNET INITIATIVE, *supra* note 92, at 3.

145. It is not clear whether the Thai government has legal authority to censor the Internet at all. ACCESS DENIED, *supra* note 9, at 158–59; C.J. Hinke, *Censoring Free Speech in Thailand*, GLOBAL VOICES ADVOCACY, May 17, 2008, http://advocacy.globalvoicesonline.org/2008/05/17/censoring-free-speech-in-thailand/.

146. *See generally* Andreas Schedler, *The Menu of Manipulation*, 13 J. DEMOCRACY 36 (2002) ("[Transitions from authoritarian rule] have given birth to new forms of authoritarianism that do not fit into our classic categories of one party, military, or personal dictatorship. They have produced regimes that hold elections and tolerate some pluralism and interparty competition, but at the same time violate minimal democratic norms so severely and systematically that it makes no sense to classify them as democracies, however qualified.").

147. *See, e.g.*, Clifford J. Levy, *Putin Aide Secures His Assured Victory in Russian Vote*, N.Y. TIMES, Mar. 3, 2008, at A3 ("Throughout the campaign, the Kremlin, having essentially prevented any meaningful opposition, focused on getting enough people to the polls to allow the vote to be depicted as legitimate."); *Russia Goes to the Polls*, HUMAN RIGHTS WATCH, Nov. 29, 2007, http://hrw.org/english/docs/2007/11/29/russia17440.htm (noting that Russian citizens will be going to the polls "in a deteriorating human rights situation where fundamental freedoms vital to free and fair elections are curtailed").

148. *See, e.g.*, Fabiola Sanchez, *Venezuela's Chavez Pushes Through 26 Decrees*, USA TODAY, Aug. 5, 2008, *available at* http://www.usatoday.com/money/economy/2008-08-05-2755377644_x.htm (reporting that the new laws enacted by presidential decree aim to move Venezuela toward a "centralized, state-run economic system").

appearance of democracy can be at odds with the reality of governance, and in which accountability is diminishing.

Even U.S. efforts can generate accountability problems. In June 2008, New York's Attorney General pressed three major ISPs to drop a wide range of Usenet news groups—only eighty-eight of which had illicit material—to reduce online distribution of child pornography.[150] By July 2008, AT&T and AOL agreed to do so as well.[151] Beyond narrowness concerns, the agreement with the Attorney General limits Usenet access for all of the providers' customers, not just those in New York.[152] Customers in other states, however, cannot hold a New York official accountable. Other regulators, state or federal, might have sought a different solution. For example, they might have included other major ISPs (such as Comcast[153]), narrowed the restrictions (perhaps to the eighty-eight groups with unlawful images), or broadened the blocking to include Web sites with child pornography (as initial reports indicated that New York had required[154]). Other states have begun to echo New York's demands of ISPs,[155] increasing the likelihood of fragmented regulation and diminished accountability.

Conversely, some citizen participation in developing filtering policy is possible even in the absence of democratic government. For

149. *See, e.g.*, HUMAN RIGHTS WATCH, ALL OVER AGAIN: HUMAN RIGHTS ABUSES AND FLAWED ELECTORAL CONDITIONS IN ZIMBABWE'S COMING GENERAL ELECTIONS (2008), http://hrw.org/reports/2008/zimbabwe0308/ (noting that Zimbabwe's "deeply flawed and rushed electoral process," and the government's "continuing violations of civil and political rights" make it unlikely that upcoming elections "will help Zimbabwe either establish democracy or bring an end to the country's ongoing political crisis"); Celia W. Dugger & Barry Bearak, *Mugabe Rival Quits Zimbabwe Runoff, Citing Attacks*, N.Y. TIMES, June 23, 2008, at A1 ("It remains to be seen whether southern Africa's leaders will collectively censure [the incumbent president] or take tougher steps, such as economic sanctions, to isolate his government. They have never done so before, despite [previous] elections . . . that were widely believed to have been marked by rigging and fraud, but that his regional peers declared legitimate.").

150. McCullagh, *supra* note 3.

151. Linda Rosencrance, *ISPs Join to Block Child Porn*, PC WORLD, July 13, 2008, http://www.pcworld.com/article/148295/isps_join_to_block_child_porn.html.

152. Hakim, *supra* note 3.

153. Comcast was the second-largest U.S. ISP for the third quarter of 2008. Alex Goldman, *Top 23 U.S. ISPs by Subscriber: Q3 2008*, ISP-PLANET, Dec. 2, 2008, http://www.isp-planet.com/research/rankings/usa.html.

154. Peter Grier, *ISPs Take Major Step in Curbing Child Porn*, CHRISTIAN SCI. MONITOR, June 11, 2008, at 1, *available at* http://www.csmonitor.com/2008/0611/p01s09-usgn.html; *see also* Hakim, *supra* note 3.

155. *See, e.g.*, Marguerite Reardon, *California Pols Ask ISPs to Block Child Porn*, CNET NEWS, June 20, 2008, http://news.cnet.com/8301-10784_3-9973966-7.html.

example, Saudi Arabia permits only limited political participation,[156] but it invites local users to suggest sites that should be blocked or to challenge a decision to censor material. The Saudi censors receive hundreds of requests each day to censor additional material (but only a few to unblock sites).[157] Such participation has had some effect, though it has been limited in scope. In 2001, a Saudi official reported that 30 percent of requests to block additional sites resulted in additions to the Kingdom's "black list," and 3 percent of requests to unblock material were granted.[158] This example demonstrates that, even if citizens have limited participation in a state's governance, they may be able to shape the state's Internet censorship.

2. *Delineated Authority*. The accountability criterion also takes into account whether citizens are able to hold government censors to task. This assessment is eased considerably when the basis for censorship is specified formally. The codification of censorship criteria not only puts citizens on notice regarding prohibited content but also constrains blocking decisions. When challenging a censor's decision is not possible, filtering that is at odds with a country's rules detracts from its legitimacy. And when citizens can contest censorship, such contradictions weaken the basis for upholding it.

Italy passed legislation in 2005[159] allowing a government agency to specify gambling sites that Italian ISPs must block (namely, sites that did not register with the agency).[160] The agency created and published a list of the sites in February 2006.[161] Thus, online gambling

156. *See* FREEDOM HOUSE, SAUDI ARABIA: 2007 (2007), http://www.freedomhouse.org/template.cfm?page=22&year=2007&country=7265 ("Saudi Arabia organized elections for municipal councils in the first half of 2004, giving Saudi men a limited opportunity to select some of their leaders at the local level.").

157. Robin Miller, *Meet Saudi Arabia's Most Famous Computer Expert*, LINUX.COM, Jan. 14, 2004, http://linux.com/archive/articles/33695.

158. ABDULAZIZ HAMAD AL-ZOMAN, THE INTERNET IN SAUDI ARABIA (TECHNICAL VIEW) 26–28 (2001), *available at* http://www.isu.net.sa/library/CETEM2001-Zoman.pdf.

159. Disposizioni per la Formazione del Bilancio Annuale e Pluriennale dello Stato (Legge Finanziaria 2006) [Orders Concerning the Formation of the Annual and Multi-Year State Budgets (Budget Law 2006)], Dec. 29, 2005, Gazz. Uff. No. 302, *available at* http://www.camera.it/parlam/leggi/05266l.htm.

160. Andrea Glorioso, *Betting Websites Are Blocked in Italy*, EUR. DIGITAL RIGHTS, June 21, 2006, http://www.edri.org/edrigram/number4.12/italybetting.

161. Elenco di Cui al Decreto del Direttore Generale di AAMS 7 febbraio 2006 Relativo alla Rimozione dei Casi di Offerta in Assenza di Autorizzazione, Attraverso Rete Telematica, di Giochi "[List Pursuant to the Decree of the Director General of the AAMS (Autonomous State Monopolies Administration on Technical Regulations) of 7 February 2006 on the

enterprises knew whether they had been filtered, and why. Indeed, Malta-based bookmaker Astrabet successfully challenged its ban in court.[162] Specifying the criteria for filtering and the individual sites to be blocked limited the government's discretion in banning online content and enabled the affected sites to contest blacklisting.

Formalizing censorship standards, though, may not sufficiently constrain officials—or provide grounds to argue that a ban contravenes applicable law. Singapore, for example, carefully specifies its filtering requirements via statute (the Media Development Authority Act[163] and the Broadcasting Act[164]), regulation (broadcasting class licenses[165]), and ISP industry policy documents (the Media Development Authority's Internet Code of Practice[166]). Singapore, however, broadly defines prohibited content—such as content that is "objectionable on the grounds of public interest, public morality, public order, [or] public security." These elastic guidelines provide discretion to government censors.[167] Although the putative focus of Singapore's filtering is pornography, the government has employed these elastic guidelines to block popular gay and lesbian sites.[168] The ability to argue that the government has exceeded its mandate is limited by the broad regulatory language defining what constitutes banned content. Thus, the case of Singapore demonstrates that even a country that specifies

---

Prohibition of Gaming or Betting Through the Internet Without Authorization]", AMMINISTRAZIONE AUTONOMA DEI MONOPOLI DI STATO, http://www.aams.it/site.php?page=20060213093814964&
op=download.

162. Glorioso, *supra* note 160.

163. Media Development Authority Act, ch. 172 (2003) (Singapore), *available at* http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-172&doctitle=MEDIA%20DEVELOPMENT%20AUTHORITY%20OF%20SINGAPORE%20ACT%0A&date=latest&method=part.

164. Broadcasting Act, ch. 28 (2002) (Singapore), *available at* http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-28&doctitle=BROADCASTING%20ACT%0A&date=latest&method=part.

165. Broadcasting (Class Licence) Notification, Broadcasting Act, ch. 28, § 9 (1996) (Singapore), *available at* http://www.mda.gov.sg/wms.file/mobj/mobj.487.ClassLicence.pdf.

166. Internet Code of Practice (1997) (Singapore).

167. *Id.* § 4(1).

168. *See Singapore Bans Gay Website*, SYDNEY MORNING HERALD, Oct. 28, 2005, *available at* http://www.smh.com.au/news/breaking/singapore-bans-gay-website/2005/10/28/1130400335787.html (reporting that the Media Development Authority banned a gay Web site "after receiving complaints about the promotion of promiscuous homosexual behaviour and recruitment of underage boys for sex and nude photography . . . . [and] [i]nvestigations showed the two sites breached the Internet Code of Practice, which governs the content of websites in Singapore").

filtering criteria in formal regulations may not be accountable to citizens. Overall, the more clearly authority for censorship is demarcated, the more legitimate decisions on restricting information will be.

3. *Opportunity to Challenge*. Censors make mistakes. In addition to challenging erroneous classifications, content owners may want to challenge decisions that correctly classify their Web sites by attacking the rationale underlying the state's censorship. One aspect of accountability is whether a state provides citizens with the means to contest censorship. This aspect of accountability interacts with a state's mode of governance—democratic institutions generally provide for redress, whether via legislatures or courts. This aspect also interacts with the level of specificity of the state's filtering program; the more concrete the guidelines are, the easier it is to show whether a particular decision contravenes them. Allowing challenges to state censorship enhances legitimacy because it forces a state to justify its decisions, presses censors to align their decisions with the stated criteria for censorship, and allows content creators to argue for their material's legality.

China, for example, fares poorly on this front. The country implements its filtering policies via a congeries of statutes, agency regulations, and informal measures.[169] Censorship mixes legal restrictions and tacit cooperation by Internet companies.[170] It is

169. *See, e.g.*, State Admin. of Radio, Film, and Television, *Provisions on the Administration of Internet Video and Audio Programming Services*, Dec. 20, 2007, *available at* http://www.chinasarft.gov.cn/articles/2007/12/29/20071229134709730745.html; Ministry of Info. Indus. & Gen. Admin. of Press and Publ'n, *Interim Provisions on the Administration of Internet Publication*, June 27, 2002, http://www.lawinfochina.com/law/displayModeTwo.asp?id=2393; Ministry of Info. Indus., *Measures for the Administration of Internet Information Services*, CHINA TRADE SERVICES, Sept. 25, 2000, *available at* http://tradeinservices.mofcom.gov.cn/en/b/2000-09-25/18565.shtml; Internet Soc'y of China, Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry (July 19, 2002), http://www.isc.org.cn/20020417/ca102762.htm (noting that the public pledge was drafted in order "to establish a self-regulating mechanism for China's Internet Industry, improve the conduct of Internet Industry Participants and promote and ensure the sound development of the Internet Industry consistent with the law"). *See generally* Liu & Krovatin, *supra* note 109 (describing how local Chinese governments have recruited "Internet moles" to "tout the party line online and by doing so, to nip unrest in the bud").

170. *See generally* Kristen Farrell, *The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on the Freedom of Expression*, 15 MICH. ST. J. INT'L L. 577, 590 (2007) ("U.S.-based companies continue to capitulate on the new Chinese restrictions on speech. Google agreed to exclude from a list of links publications that the Chinese government finds objectionable. Microsoft sends an error message to Internet users in China who use its search

difficult to determine how to contest censorship, and who to hold responsible. Even citizens bold enough to challenge restrictions—such as a dog owner who filed a lawsuit over the removal of his post criticizing Beijing's animal size limits[171]—face legal hurdles (the court rejected his case) and informal pressures such as harassment from government agents. Chinese citizens—many of whom endorse a governmental role in regulating Internet content[172]—evidently view formal challenges as futile; only two such lawsuits have ever been filed.[173]

It is not surprising that states with independent judicial systems are the most likely to allow citizens to challenge filtering decisions. Astrabet sued in Italian court to overturn government-mandated blocking of its site, and won.[174] In the United States, the Center for Democracy & Technology successfully sued to overturn a Pennsylvania law mandating blocking of Internet child pornography that also caused filtering of over one million unrelated sites.[175] Although there is a strong connection between citizens' ability to challenge censorship meaningfully and the overall form of governance in place in a country, it is possible for citizens to contest filtering decisions even in nondemocratic countries. For example, Saudi Arabia allows requests for sites to be unblocked.[176] And efforts by civic actors in Tajikistan and Azerbaijan have led those governments to reverse filtering of political opposition sites.[177]

---

engine for words such as democracy, freedom, human rights, or demonstration."); Lokman Tsui, Internet in China: Big Mama Is Watching You 27 (July 2001) (unpublished M.A. thesis, Univ. of Leiden), *available at* http://www.lokman.nu/thesis/010717-thesis.pdf ("The basic principle behind the concept of internet regulation in China is 'one is responsible for what one publishes.' As a result, internet-related companies in China practice a high degree of self-censorship . . . [which] is necessary in order to gain the trust and cooperation of the government.").

171. Edward Cody, *Dog Owner Takes on China's Web Censors*, WASH. POST, Dec. 26, 2007, at A18.

172. Deborah Fallows, *Few in China Complain About Internet Controls*, PEW INTERNET & AM. LIFE PROJECT, Mar. 27, 2008, http://pewresearch.org/pubs/776/china-internet (reporting that 80 percent of respondents support Internet regulation, and that 85 percent believe that the government should undertake it).

173. Cody, *supra* note 171.

174. *See* Glorioso, *supra* note 160.

175. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 610–11, 662 (E.D. Pa 2004).

176. *See* AL-ZOMAN, *supra* note 158, at 28.

177. Rafal Rohozinski & Vesselina Haralampieva, OpenNet Initiative, Commonwealth of Independent States, http://opennet.net/research/regions/cis (last visited Oct. 23, 2009).

Although they are less robust than Italian or American methods for challenging censorship, these examples show that there is a continuum of means to contest filtering and that a country's governance is not a perfect proxy for this variable. Enabling citizens to contest censorship decisions is a key component of legitimacy.

4. *Countermajoritarian Constraints*. A final factor in measuring accountability is the existence of countermajoritarian constraints. Even under a democratic government, a state may discriminate against minority groups, whose limited numbers impede their ability to counteract majoritarian rule. Discrimination, unfortunately, may be popular.

Censorship of minority-interest Internet content is common. For example, Vietnam blocks pages about the Montagnards, who are both a political minority (having aided the U.S. during the Vietnam War) and a religious one (being predominantly Christian).[178] Oman blocks gay and lesbian sites.[179] Pakistan blocks sites advocating independence for its Balochistan and Sindh provinces.[180]

When a minority of citizens wants access to certain material and the majority wants to prevent it, filtering poses a difficult normative problem. When should the minority's objections be upheld? Ultimately, this is a question of system design—that is, of determining what structures (if any) limit popular sovereignty. Here, censorship is one example of a larger puzzle in governance and legal philosophy. American legal scholars have long struggled to describe the proper constraints on majoritarian decisionmaking and to defend the rationale for imposing such limits in a representative democracy. Alexander Bickel described the "Counter-Majoritarian Difficulty," noting that having an independent judiciary review (and, potentially, disallow) democratic decisions could cause legislatures to overly rely on courts to save them from illegitimate or unlawful actions.[181] Bickel concluded, however, that judicial training and judges' focus on a

178. OPENNET INITIATIVE, *supra* note 116, at 4. *See generally Vietnam: Montagnards Face Religious, Political Persecution*, HUMAN RIGHTS WATCH, June 13, 2006, http://hrw.org/en/news/2006/06/13/vietnam-montagnards-face-religious-political-persecution (documenting Vietnamese mistreatment of Montagnard refugee and asylum seekers).

179. OPENNET INITIATIVE, OMAN 3 (2007), http://opennet.net/sites/opennet.net/files/ONI_Oman_2007.pdf.

180. OPENNET INITIATIVE, PAKISTAN 4 (2007), http://opennet.net/sites/opennet.net/files/pakistan.pdf.

181. ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH 16–23 (1962).

case's specific facts usefully enable reconsideration of controversial regulation.[182]

Another perspective frames these limits as a second-order problem: they should prevent a majority from altering systemic structures to deprive minority voices of the ability to be heard and to participate in governance. John Hart Ely saw courts, and constitutional interpretation more broadly, as focused primarily upon ensuring procedural protections, while deferring normative judgments to government's representative branches.[183] Checks on popular sovereignty create perils, though—particularly when implemented through institutions with limited accountability. Thus, political philosopher Jeremy Waldron attacks countermajoritarian constraints as disenfranchising citizens and privileging the value preferences of judges who are subject only to limited political constraints.[184] Whether, and to what degree, popular will should be limited—to protect shared values[185] or to prevent discrimination against weaker minority groups[186]—is highly contested, and beyond the scope of this Article.

Internet censorship may, however, make countermajoritarian constraints particularly important for two reasons. First, filtering is not always transparent: it can be difficult to detect what content is inaccessible or what sites are removed from search engine results.[187] (Contrast this with the ease of detecting censorship in physical media, as when copies of *National Geographic* in China had pages on disputed borders or ethnic minorities glued together.[188]) Filtering risks altering not government's systemic structures, but the information citizens use to make decisions. Russian citizens may not know about political opposition, or its grounds for complaint, if contrary views are

182. *Id.* at 131–32.

183. JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 73–77 (1980).

184. Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 YALE L.J. 1346, 1353 (2006).

185. *See, e.g.*, Laurence H. Tribe, *The Puzzling Persistence of Process-Based Constitutional Theories*, 89 YALE L.J. 1063, 1079–80 (1980).

186. *See, e.g.*, United States v. Carolene Prods. Co., 304 U.S. 144, 152–53 n.4 (1938).

187. *See, e.g.*, Nart Villeneuve, Degrading Transparency: Comparing Google, Yahoo and Microsoft (Jan. 25, 2008), http://www.nartv.org/2008/01/25/degrading-transparency-comparing-google-yahoo-and-microsoft/.

188. Geoffrey A. Fowler, *Glued Geographic*, WALL ST. J., June 4, 2008, http://blogs.wsj.com/chinajournal/2008/06/04/glued-geographic/.

purged from mass media.[189] Thus, censorship subtly raises Ely's concerns about skewing process.

Second, censorship prevents access to material that might influence views regarding its necessity. It is easier to undercut political opponents or critics when material supporting their views is unavailable.[190] Subjective preferences are not independent or static; they evolve in response to available information.[191] As Oliver Wendell Holmes noted, today's minority viewpoint may be tomorrow's accepted wisdom.[192]

Accountability may, therefore, require limiting censorship's responsiveness to popular sentiment. This could include both regulatory inertia—dampening or delaying shifts with changes in social views—as well as countermajoritarian protections for minority expression. Filtering must be responsive to citizens' preferences, but not too responsive. At a minimum, accountability analysis should include assessing how a country addresses minority concerns and the risks of majoritarian control.

Accountability, the Framework's final factor, complements the previous three by measuring how responsive censorship practices are to the people they are supposed to protect. With the Framework's overview complete, the next question is how to translate the Framework into concrete tools for assessing censorship.

III. IMPLEMENTATION

The Framework is only as useful as its implementation. The best way to apply it is for multiple entities, public and private, to construct quantitative metrics that measure how a censorship program fares on each criterion. As these metrics are used, they will inevitably compete, refining and improving their measurements. The metrics can, and should, guide corporate decisions, government regulation, and third-party assessments regarding Internet censorship.

---

189. *See, e.g.*, Clifford J. Levy, *It Isn't Magic: Putin Opponents Vanish From TV*, N.Y. TIMES, June 3, 2008, at A1.

190. *See id.*

191. *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE (2008) (discussing how the design of "choice environments" can lead to optimal decisions); Derek E. Bambauer, *Shopping Badly: Cognitive Biases, Communications, and the Fallacy of the Marketplace of Ideas*, 77 COLO. L. REV. 649 (2006) (arguing that perceptual biases in information accumulation and processing undercut traditional decisionmaking models).

192. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

A. Developing the Metrics

The Framework's purpose is to enable rigorous assessments of the legitimacy of Internet censorship. Implicit in this goal is comparison: evaluating whether China's Internet is more legitimate than Iran's, or whether that blocking has become more legitimate over time. Comparison based upon general principles is difficult. It is challenging, for example, to establish why a particular state is transparent without a means of measuring that quality. Metrics provide that means.

When all countries are evaluated under the same rules, it is possible to compare scores to determine relative position. Establishing a metric system with numeric criteria would be useful to rate a country on each of the Framework's four factors. For example, a metric could evaluate openness by awarding points for disclosure, such as formal, written admissions of censorship; availability of rationales for filtering in official documents or Web sites; use of a block page when citizens attempt to access banned material; willingness of government officials to discuss filtering, and so forth. Freedom House uses an analogous metric system to assess the effects of a country's political environment on press freedom, asking (among other questions) whether media regulatory bodies can operate freely and independently (scored from 0 to 2 points); whether the constitution or other basic laws protect freedoms of the press and expression, and whether those provisions are enforced (0 to 6 points); and whether there are penalties for libeling state officials, and the degree of enforcement (0 to 3 points).[193]

In analyzing narrowness, a metric could check how effectively a country blocks material it seeks to censor (with 100 percent efficacy the goal); how many categories of material other than those officially targeted are blocked, and how heavily (using, for example, Open Directory Project's classification system,[194] or the OpenNet Initiative's categories[195] or global list[196]); and how precise the method used is (with less credit awarded for crude methods such as IP address blocking).

Using metrics would consistently quantify filtering for the Framework's four axes. Metrics have also been helpfully employed

193. FREEDOM HOUSE, SURVEY METHODOLOGY 3–4 (2008), *available at* http://www.freedomhouse.org/uploads/fop08/Methodology2008.pdf.

194. Open Directory Project Home Page, http://www.dmoz.org/ (last visited Oct. 23, 2009).

195. *See* Faris & Villeneuve, *supra* note 85, at 7.

196. *See, e.g.*, OPENNET INITIATIVE, *supra* note 128.

for analyzing other contested issues, including corruption,[197] press freedom,[198] economic freedom,[199] labor conditions,[200] environmental friendliness,[201] and ICT (information and communication technology) readiness.[202]

Metrics serve at least four useful purposes. First, metrics translate abstract standards into concrete evaluations. Second, they can exert pressure upon laggards (at least, those who purport to espouse the relevant standards) to improve compliance. Third, they can help guide decisions—from where to locate a factory to whether to list a country as a human rights violator. Finally, metrics direct critical attention back to their standards. Implementation challenges can highlight criteria that are insufficiently precise or too difficult to measure accurately.[203]

Designing a metric involves challenging, subjective choices in measurement. What considerations should be included? How should the components be weighed relative to one another? How should a metric account for internal inconsistencies, such as when ISPs filter to

197. *See, e.g.*, TRANSPARENCY INT'L, BRIBE PAYERS INDEX 2006, at 3–5 (2006), *available at* http://www.transparency.org/content/download/9757/71853/version/1/file/BPI_2006_Analysis_Report_270906_FINAL.pdf; Transparency Int'l, Corruption Perceptions Index 2007, http://www.transparency.org/policy_research/surveys_indices/cpi/2007 (last visited Oct. 23, 2009).

198. *See, e.g.*, FREEDOM HOUSE, *supra* note 193, at 4.

199. *See, e.g.*, JAMES GWARTNEY ET AL., ECONOMIC FREEDOM OF THE WORLD: 2007 ANNUAL REPORT 3–4 (2007), *available at* http://www.freetheworld.com/2007/EFW2007BOOK2.pdf; Heritage Found. & Wall St. J., 2009 Index of Economic Freedom, http://www.heritage.org/index/Download.aspx (last visited Oct. 23, 2009).

200. *See, e.g.*, Richard M. Locke, Fei Qin & Alberto Brause, *Does Monitoring Improve Labor Standards?: Lessons from Nike*, 61 INDUS. & LABOR RELATIONS REV. 3, 4 (2007); Nike, Audit Tools, http://www.nikebiz.com/nikeresponsibility/#workers-factories/audit_tools (last visited Oct. 23, 2009) (providing the tools and measures that Nike uses to determine factory compliance with its labor standards).

201. *See, e.g.*, ADVANCE, SUSTAINABLE VALUE OF EUROPEAN INDUSTRY: A VALUE-BASED ANALYSIS OF THE ENVIRONMENTAL PERFORMANCE OF EUROPEAN MANUFACTURING COMPANIES 6 (2006), *available at* http://www.advance-project.org/downloads/advancesurveyfullversion.pdf; Global Reporting Initiative, Reporting Framework Overview, http://www.globalreporting.org/ReportingFramework/ReportingFrameworkOverview/ (last visited Oct. 23, 2009).

202. *See, e.g.*, BRIDGES.ORG, E-READINESS ASSESSMENT TOOLS COMPARISON 1–3 (2005), *available at* http://www.bridges.org/files/active/0/ereadiness_tools_bridges_10Mar05.pdf; INFODEV, E-READY FOR WHAT? E-READINESS IN DEVELOPING COUNTRIES: CURRENT STATUS AND PROSPECTS TOWARD THE MILLENNIUM DEVELOPMENT GOALS 5 (2005), *available at* http://www.infodev.org/en/Publication.3.html.

203. *See, e.g.*, Robert M. Stern, *Labor Standards and Trade*, *in* NEW DIRECTIONS IN INTERNATIONAL ECONOMIC LAW 425, 425–36 (Marco Bronckers & Reinhard Quick eds., 2000).

varying degrees,[204] or when government officials waver on admitting to censorship?[205] The next normative choice involves comparing and weighing the different factors of the Framework. Should openness count more than narrowness? Finally, the metric must select the level at which countries can be compared. Can scores for each component be aggregated into a composite? Is it too difficult to comprehend factor-by-factor comparisons? Transparency International, for example, creates an overall measure of how corrupt a country is perceived to be.[206] These are all hard decisions, and there are no obviously correct choices. As with filtering itself, there are likely multiple defensible answers.

The best path is to generate multiple metrics, reflecting the range of defensible answers to these value-driven questions.[207] Different entities could create and apply metrics. It would be optimal to have a mix of public actors (such as the U.S. Department of State or the Internet Governance Forum) and private entities (such as the Center for Democracy & Technology, Human Rights Watch, or the OpenNet Initiative) create measurement tools. Analysts will measure compliance with each factor differently—and will weigh the relative importance of each factor variously. Each metric should make clear both how it resolves these questions and why. This level of clarity would not only illuminate how censoring countries fare when the methodology for each factor changes, but it would also reveal the values that each rating entity prioritizes.[208]

This is an unusual proposal: achieving greater insight and comparing countries more readily by using more than one metric to

204. Yemen's two ISPs, for example, filter varying levels of content. OPENNET INITIATIVE, *supra* note 133, at 4.

205. *Compare* McCullagh, *supra* note 78 (noting Chinese government officials' denial of Internet filtering in China), *with* Andrew Jacobs, *China Angered by U.S. Lobbying on Rights*, N.Y. TIMES, Aug. 1, 2008, http://www.nytimes.com/2008/08/01/sports/olympics/01dissidents.html (documenting Chinese authorities' decision to maintain a firewall on the Internet during the Olympics).

206. JOHANN GRAF LAMBSDORFF, THE METHODOLOGY OF THE CORRUPTION PERCEPTIONS INDEX 2007, at 2–9 (2007), *available at* http://www.transparency.org/content/download/23965/358196.

207. *Cf.* ROBERTA ROMANO, THE ADVANTAGE OF COMPETITIVE FEDERALISM FOR SECURITIES REGULATION 1–12 (2002) (making a similar argument for competition in securities regulation).

208. *Cf.* Balkin et al., *supra* note 42, at 9–10 (discussing how templates that rate Web content reveal preferences).

rate them.[209] There are several key benefits to having multiple, competing metrics. First, quantifying the Framework's four principles involves subjective judgments. Analysts will differ, reasonably, on such choices. By making explicit their weighting, metrics can assess a country under different tests that could generate a consensus view, or expose key zones of disagreement. Second, competition presses creators to refine measurements.

Demand from metrics users—nongovernmental organizations, state actors, and companies—will elucidate the benefits and shortcomings of each tool. As some metrics are used, and others are ignored, the set of reputable tools for future use will decrease. In addition, organizations that develop metrics can reassess their choices and how they implement them by examining the choices of other entities. The World Bank[210] and Freedom House[211] can address political accountability in ways from which other entities can learn, and OpenNet Initiative's narrowness criteria will have refinements to offer other entities.[212] Metrics should get better and fewer over time through competition.

Finally, adopting an open, competitive methodology for measuring filtering is consistent with the Framework's focus on process rather than substance. Metrics will not reflect a single view of how to measure factors, but will rely on interaction and competition to arrive at workable models.

B. Alternatives

There are other paths to produce metrics—most notably, a cooperative effort among stakeholders to produce a consensus tool, or a top-down approach. The proposed competitive process, however, appears more effective: cooperation has proven inadequate thus far, and no one entity has sufficient power to force adoption of its criteria.

---

209. *See generally* Steven M. Davidoff, *Regulating Listings in a Global Market*, 86 N.C. L. REV. 89 (2007) (discussing challenges of multiple regulatory standards in securities listings).

210. *See, e.g.*, Daniel Kaufmann, Aart Kraay & Massimo Mastruzzi, *Governance Matters VII: Aggregate and Individual Governance Indicators 1996–2007*, at 7–11, 28, 37 (World Bank Policy Research, Working Paper No. 4654, 2008), *available at* http://ssrn.com/abstract=1148386.

211. *See* FREEDOM HOUSE, COUNTRIES AT THE CROSSROADS 2007: SURVEY METHODOLOGY *passim* (2007), *available at* http://www.freedomhouse.org/uploads/ccr/page-38.pdf.

212. *See, e.g.*, Faris & Villeneuve, *supra* note 85, at 7–9, 18–22.

1. *Collaboration*. A metric produced through collaboration among affected parties and experts on Internet censorship is intuitively appealing. Such a metric would be more likely to be broadly accepted, and could eliminate the time necessary for competing models to coalesce and adapt.[213] It could draw upon expertise to reflect best practices and avoid past errors. But collaboration suffers from two key shortcomings, namely, selection problems and risk of gridlock. Moreover, collaborative attempts at establishing a code of conduct for Internet companies have dragged on without producing readily measurable results. After years of frustration[214] and press releases,[215] these attempts have generated principles but no means to measure their implementation.

The Global Network Initiative (GNI), a consortium[216] of activist groups, civil society organizations, academics, investment funds, and three technology companies (Google, Microsoft, and Yahoo!), finally released a set of principles intended to guide technology companies in dealing with governmental pressures on human rights issues.[217] The Initiative sets forth principles similar to this Article's Framework, such as governance, accountability, and transparency, but it confronts three critical limitations.[218] First, only three companies have signed on to GNI, and although they are significant market players, it is not clear that they will induce other firms, such as Cisco or Skype, to join. Similarly, watchdogs such as Amnesty International have pointedly

213. *Cf.* Fung, *Deliberative Democracy*, *supra* note 71, at 53–54 (describing a "grand consensus" approach to labor standards).

214. *See Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing Before the Subcomm. on Human Rights and the Law of the S. Judiciary Comm.*, 110th Cong. 9 (2008) (statement of Aryind Ganesan, Deputy General Counsel, Google, Inc.), *available at* http://hrw.org/english/docs/2008/05/20/usint18894.htm (describing an effort by technology companies, human rights organizations, and scholars "to develop a voluntary code of conduct and process of enforcement to try to curtail censorship and protect user information," but noting "almost 18 months later, it would be great to tell you that a code is finalized and a system is in place to address these problems, but instead, we are still negotiating, and in the meantime, internet users are no safer, and censorship continues").

215. *See, e.g.*, Press Release, Ctr. for Democracy & Tech., *supra* note 9.

216. Global Network Initiative, Participants, http://www.globalnetworkinitiative.org/participants/index.php (last visited Oct. 23, 2009).

217. Global Network Initiative, Principles, http://www.globalnetworkinitiative.org/principles/index.php (last visited Oct. 23, 2009).

218. Global Network Initiative, Governance, Accountability & Learning Framework, http://www.globalnetworkinitiative.org/governanceframework/index.php (last visited Oct. 23, 2009).

declined to join the effort over concerns about its standards.[219] Second, reaching agreement on principles is straightforward, whereas implementing them and measuring that implementation is complicated. The Initiative sets up a methodology for implementation, but its use in practice remains uncertain.[220] Finally, companies can avoid breaching the Initiative's code by delegating control to local partners; firms need only use "best efforts" to ensure compliance with the principles.[221] To date, the GNI is a cautionary tale about collaborative efforts rather than a success story.

The GNI underscores the challenges of choosing participants in a collaborative effort. Selection reflects subjective values about which participants are and are not appropriate, relevant, and useful. For example, a consensus approach would include companies whose financial results might be affected by the metric they would help develop, such as Microsoft and Google.[222] Companies with the most insight to contribute would be those with the greatest conflicts of interest: filtering software companies such as Secure Computing and Fortinet. Excluding these firms would detract from the effort to include all stakeholders, but including them would harm the metric's credibility.

A consensus effort could easily splinter. Those not selected might become disaffected, opting not to recognize the metric or even developing a competing one. It might be possible to launch a truly participatory, open source project to measure the Framework's criteria, but Internet censorship is controversial, and open source projects often struggle to accommodate divergent views on contested issues.[223] Consensus dissolves readily, as demonstrated by "forks" in open source projects.[224]

---

219. Bobbie Johnson, *Amnesty Criticises Global Network Initiative for Online Freedom of Speech*, GUARDIAN, Oct. 30, 2008, http://www.guardian.co.uk/technology/2008/oct/30/amnesty-global-network-initiative.

220. *See* Global Network Initiative, Implementation Guidelines, http://www.globalnetwork initiative.org/implementationguidelines/index.php (last visited Oct. 23, 2009).

221. *Id.*

222. *See* discussion *infra* Part III.C. If China's filtering were rated as illegitimate by the new metric, and transactions by technology companies enabling China's censorship attracted heightened scrutiny, Microsoft and Google might be pressured to reduce such business, and hence lose revenue.

223. Wikipedia, for example, has frequently limited edits to its entry on George W. Bush for this reason. *See* Ulrik Brandes & Jürgen Lerner, *Visual Analysis of Controversy in User-Generated Encyclopedias*, 7 INFO. VISUALIZATION 34, 36, 46 (2008); Stacy Schiff, *Know It All:*

Even a collaborative effort that does not splinter may falter due to gridlock. Members may be unable to resolve differences of opinion. Some may delay due to strategic behavior—it may be beneficial to appear to work on evaluating Internet censorship without risking unfavorable analysis from the final product. The broader the range of participants, the more likely disagreement is to occur—technology companies, governments, and human rights monitors have divergent goals and normative approaches. Debates over the Global Network Initiative, which was styled as a collaborative approach, exemplify this problem.[225] Thus, collaboration is unlikely to generate the necessary metrics.

2. *Top-Down*. A metric created through a top-down process could be developed more rapidly than one built through collaboration or competition and would enable standardized analysis. But a top-down process would require a sufficiently powerful stakeholder to press for its adoption and use. For Internet filtering, there is no single entity able to impose its preferences on other stakeholders. This may be beneficial: any party sufficiently powerful to require use of its metric would be strongly tempted to codify its normative preferences on filtering into a mandatory standard. Measurements propagated by the U.S. government would likely include, even if only implicitly, American views about free expression. This would undermine the Framework's agnosticism on substantive issues.

Attempts to force a single metric would likely founder because dissenters could, and would, produce their own criteria. Thus, the two major alternatives for producing metrics—collaboration and a mandatory standard—are likely to dissolve into competition. It is preferable to begin with, and leverage, the inevitable jockeying among standards.

Can Wikipedia Conquer Expertise?, NEW YORKER, July 31, 2006, at 36, 42, *available at* http://www.newyorker.com/archive/2006/07/31/060731fa_fact.

224. *See, e.g.*, Paul Adams, *In Response to User Demand, Pidgin Forks*, WEBMONKEY, Apr. 22, 2008, http://webmonkey.com/blog/In_Response_to_User_Demand__Pidgin_Forks (announcing that Pidgin, an open source instant-messaging software, has "forked"); *cf.* Jill Coffin, *Analysis of Open Source Principles in Diverse Collaborative Communities*, FIRST MONDAY, June 5, 2006, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1342/1262 (analogizing the Burning Man community in the Black Rock Desert of Nevada to an open source project and describing its eventual "fork").

225. *See supra* notes 214–21 and accompanying text.

Finally, using competing alternatives to evaluate censorship fits well with the Internet's ethos. Leaders or standards from TCP/IP[226] to Google[227] emerged from a welter of competitors. Even the core Internet protocols are framed as consensual standards,[228] where usage is voluntary and replacement is commonplace.[229] The Internet itself could be a valuable tool for creating, promulgating, and developing metrics.[230]

An open, competitive process for producing metrics to measure filtering best enables development of useful tools to measure the Framework's prongs quantitatively.

C. Using the Metrics

Metrics that measure the legitimacy of filtering can contribute to three contentious debates: corporate decisions on whether to sell censorship-enabling technology to a country; government deliberations on whether to regulate these choices through public law; and normative evaluations of filtering by third parties.

1. *Corporate Decisions*. Western corporations have stirred controversy by supplying technology that enables countries to filter the Internet, and by censoring the services they offer to these nations.[231] California-based firm Fortinet sold firewall technology to Burma that lets its military dictatorship limit citizens' access to online

226. *See* Laura Chappell, *Migrating to IP*, NETWORK WORLD FUSION, Oct. 18, 1999, http://www.networkworld.com/news/1999/1018feat.html (describing the "inevitable upgrade to TCP/IP" from Novell's IPX/SPX, the previously dominant network protocol).

227. *See* Jefferson Graham, *The Search Engine That Could*, USA TODAY, Aug. 26, 2003, at 1D, *available at* http://www.usatoday.com/tech/news/2003-08-25-google_x.htm.

228. *See* S. BRADNER, THE INTERNET STANDARDS PROCESS – REVISION 3 (1996), ftp://ftp.rfc-editor.org/in-notes/bcp/bcp9.txt (noting the Internet relies on "voluntary adherence to open protocols and procedures").

229. *See, e.g.*, P. Mockapetris, *Domain Names – Concepts and Facilities [RFC 1034]* (Nov. 1987), http://www.ietf.org/rfc/rfc1034.txt?number=1034 (replacing RFC 973).

230. *See generally* Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369 (2002) (describing the emerging "phenomenon of large- and medium-scale collaborations among individuals that are organized without markets or managerial hierarchies" on the Internet); Jonathan Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1987–96 (2006) (arguing that Internet reforms should be tailored to minimize their "impact on generativity").

231. *See generally* David Bandurski, *Pulling the Strings of China's Internet*, 171 FAR E. ECON. REV. 18 (2007) (describing how Internet censorship technology is enabling the Chinese government to use the Beijing Association of Online Media as its agent to monitor and filter Internet content).

material about human rights, political dissent, and ethnic minority groups.[232] Cisco's routers form a key component of China's censorship system.[233] Internal documents reveal not only that Cisco knows that China uses its products to censor the Internet but also that the company views this practice as a business opportunity.[234] Secure Computing sells its Internet filtering software and content classification database to Saudi Arabia, Tunisia,[235] and Sudan;[236] Websense provides its version to Yemen.[237] Google, Yahoo!, and Microsoft operate search engines in China that remove results linking to blocked sites.[238] Google's localized French, German, and Canadian search engines similarly delist hate speech pages.[239] Microsoft's Chinese MSN Spaces blog site prevents users from posting sensitive keywords including "democracy" and "demonstration."[240]

Although they are profitable, these transactions generate criticism. In May 2008, U.S. Senator Richard Durbin compared Google's justification for its Chinese search engine censorship to arguments for doing business with South Africa under apartheid.[241] The U.S. Congress has held numerous hearings on corporate

232. OPENNET INITIATIVE, INTERNET FILTERING IN BURMA IN 2005: A COUNTRY STUDY 4–5, 18, 24 (2005), http://opennet.net/sites/opennet.net/files/ONI_Burma_Country_Study.pdf; *see also* Nart Villeneuve, Fortinet for Who? (Oct. 13, 2005), http://www.nartv.org/2005/10/13/fortinet-for-who/.

233. *See* ETHAN GUTMANN, LOSING THE NEW CHINA 130–32, 158–60 (2004).

234. CISCO SYS., OVERVIEW OF THE PUBLIC SECURITY SECTOR 57–58 (2002) (on file with the *Duke Law Journal*) (describing the Chinese government's goal to "[c]ombat 'Falun Gong' evil religion and other hostiles" and concomitant Cisco business opportunities in technical training, security, and operational maintenance); Glenn Kessler, *Cisco File Raises Censorship Concerns*, WASH. POST, May 20, 2008, at D1.

235. Ben Arnoldy, *When US-Made "Censorware" Ends Up in Iron Fists*, CHRISTIAN SCI. MONITOR, Oct. 10, 2007, at 1, *available at* http://www.csmonitor.com/2007/1010/p01s01-ussc.html.

236. *See generally* OPENNET INITIATIVE, SUDAN (2009), http://opennet.net/sites/opennet.net/files/ONI_Sudan_2009.pdf (describing Internet filtering technology and its usage in Sudan).

237. Xeni Jardin, *Exporting Censorship*, N.Y. TIMES, Mar. 9, 2006, at A23.

238. Villeneuve, *supra* note 100.

239. *See Global Internet Freedom: Corporate Responsibility and the Rule of Law*, *supra* note 214, at 9 (statement of Nicole Wong, Deputy General Counsel, Google, Inc.), *available at* http://judiciary.senate.gov/hearings/hearing.cfm?id=3369; *see also supra* note 15.

240. *Microsoft Censors Chinese Blogs*, BBC NEWS, June 14, 2005, http://news.bbc.co.uk/1/hi/technology/4088702.stm.

241. Nate Anderson, *Sen.: Iron Curtain Swapped for Virtual Curtain of Censorship*, ARS TECHNICA, May 20, 2008, http://arstechnica.com/news.ars/post/20080520-sen-iron-curtain-swapped-for-virtual-curtain-of-censorship.html.

participation in Internet censorship,[242] and members such as Representative Christopher Smith have introduced legislation that would ban these sales.[243] Nongovernmental organizations such as Human Rights Watch, Amnesty International, and Reporters Without Borders[244] have attacked sales to censoring countries. Owners of Web sites targeted for blocking have protested, and even offered guides to bypassing censorship.[245] Although corporations concede the need for some constraints, they advocate for self-regulation through voluntary codes of conduct, intergovernmental efforts to press for openness,[246] and treating filtering as a trade barrier.[247]

Operating in or trading with a country that censors online content can create conflicts: companies have a duty to shareholders to pursue profitable transactions.[248] But their corporate values—and the values of the countries in which they are based—may counsel against such sales.[249] For example, Microsoft opted not to locate its Chinese-language Hotmail servers within China to avoid state demands for private user data,[250] even though doing so would lessen the technical problems that occasionally plague Hotmail.[251] Yahoo!, in contrast,

242. Anne Broache, *Politicos Attack Tech Firms over China*, CNET NEWS, Feb. 1, 2006, http://news.cnet.com/2100-1028_3-6033976.html.

243. *See* Global Online Freedom Act of 2007, H.R. 275, 110th Cong. (2007).

244. *See, e.g.*, Verena Dobnik, *13 Nations Denounced for Web Censorship*, MSNBC.COM, Nov. 8, 2006, http://www.msnbc.msn.com/id/15621193.

245. *See, e.g.*, Jardin, *supra* note 237; Boing Boing, BoingBoing's Guide to Defeating Censorware, http://www.boingboing.net/censorroute.html (last visited Oct. 23, 2009).

246. *See, e.g.*, Foster Klug, *U.S. Tech Companies Urge Washington to Confront China on Internet Censorship*, PITTSBURGH POST-GAZETTE, Feb. 4 2007, http://www.post-gazette.com/pg/07035/758377-96.stm.

247. *Id.* (quoting Andrew McLaughlin, senior counsel for Google, testifying that Google wants censorship to be treated as a trade barrier); *see also* Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J. INT'L LAW 263, 276–80 (2006) (analyzing whether internet filtering violates trade laws).

248. *See, e.g.*, Dodge v. Ford Motor Co., 170 N.W. 668, 682 (Mich. 1919) (holding that corporations are organized for the purpose of shareholder profit, and that directors must pursue this goal); *see also* Stephen M. Bainbridge, *Director Primacy: The Means and Ends of Corporate Governance*, 97 NW. U. L. REV. 547, 548–49 (2003).

249. *See infra* note 255 and accompanying text.

250. Rebecca MacKinnon, *America's Online Censors*, NATION, Feb. 24, 2006, http://www.thenation.com/doc/20060313/mackinnon (noting that Microsoft's instant messaging and Hotmail services are "hosted on servers outside of China so it doesn't have to hand over data").

251. Sumner Lemon, *Microsoft Restores Hotmail Service in China*, INFOWORLD, May 22, 2006, http://www.infoworld.com/article/06/05/22/78548_HNhotmailchina_1.html (discussing recent Hotmail problems in China).

placed its e-mail servers inside China, improving service but making it easier for security services to get the company to disclose user information. This information has been used to convict and imprison at least four dissidents.[252] The tension is clear: offering Internet services from outside China reduces their performance and hence their attractiveness (some Chinese users switched from Hotmail to Google's Gmail due to outages),[253] but locating servers within the country increases the risk that a technology company may assist political repression.

This challenge of deciding when to help censor becomes particularly acute when the filtering country represents an important market (China boasts the greatest number of Internet users of any nation)[254] or when ethical behavior is particularly significant to a company (Google's philosophy includes, "You can make money without doing evil.")[255] Many technology companies have a core business function of making information easier to access, and filtering runs counter to this basic goal. Though Yahoo! believes "information is power" and commits to "open access to information and communication on a global basis,"[256] the company censors its Chinese search engine. Indeed, Yahoo! filters out more results than either Google or Microsoft.[257]

How a company reconciles its choices with corporate values is up to each firm. Those decisions, however, will be challenged by

252. Rebecca MacKinnon et al., *"Race to the Bottom": Corporate Complicity in Chinese Internet Censorship: How Multinational Internet Companies Assist Government Censorship in China*, HUMAN RIGHTS WATCH, Aug. 2006, at 1, 31, *available at* http://www.hrw.org/reports/2006/china0806/china0806web.pdf (discussing Yahoo's role in the convictions of four Chinese dissidents); *Yahoo Criticized in Case of Jailed Dissident*, N.Y. TIMES, Nov. 7, 2007, at C3 (noting that Democratic Representative Tom Lantos of California criticized Yahoo! CEO Jerry Yang and General Counsel Michael J. Callahan during a House Foreign Affairs Committee meeting).

253. Sumner Lemon, *Microsoft's Hotmail Problems Persist in China*, COMPUTERWORLD, May 18, 2006, http://www.computerworld.com/s/article/9000605/Microsoft_s_Hotmail_problems_persist_in_China (discussing how one Chinese Hotmail user switched to Google's Gmail service because of Hotmail's technical problems).

254. Calum MacLeod, *China Vaults Past USA in Internet Users*, USA TODAY, Apr. 21, 2008, at 1A, *available at* http://www.usatoday.com/tech/world/2008-04-20-Internetusers_N.htm.

255. Google, Corporate Information, Our Philosophy, http://www.google.com/corporate/tenthings.html (last visited Oct. 23, 2009).

256. Press Release, Yahoo!, Yahoo!: Our Beliefs as a Global Internet Company (Feb. 13, 2006), *available at* http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=187401.

257. Villeneuve, *supra* note 100, at 3 (finding that Yahoo! blocked 20.8 percent of sites tested on average, while Google filtered 15.2 percent and Microsoft filtered 15.7 percent).

observers ranging from activists to government officials. Employing a rigorous, defensible, public methodology for decisions will improve a company's ability to justify its actions. Companies could use the Framework introduced in this Article to assess a country's censorship, and incorporate this analysis into the company's decision whether to sell filtering technology there. The Global Network Initiative expressly requires participating companies to make such assessments before entering new markets, and mandates that they review policies in existing ones.[258] Using the Framework to guide decisions on where to do business would enable companies to make more responsible decisions and to use their analysis to justify choices if challenged.

Technology firms appear to prefer self-regulation to independent review through efforts such as the Global Network Initiative. Even self-regulation, though, implies that corporations must assess internally whether to sell filtering technology. It also implies that some countries are not suitable customers. Self-regulation is suboptimal for two reasons. First, firms face pressure to resolve doubts in favor of consummating deals. Corporate governance—at least for American companies—centers on producing shareholder value.[259] Companies will pursue sales when their internal standards do not clearly forbid them. Second, abstaining from questionable deals becomes difficult in a competitive environment. Another company may resolve doubts in favor of the sale, reaping benefits and placing virtuous competitors at a disadvantage.[260] Firms also face displacement by domestic producers friendly to filtering in some markets, particularly China, which has moved to develop censorship technologies.[261] Market pressures are likely to undercut self-regulation.

Companies inevitably face external pressures over their decisions. Freedom of expression groups have begun to use market pressures to push technology firms to consider filtering transactions

258. Global Network Initiative, *supra* note 220.

259. *See supra* note 248.

260. *See, e.g.*, Peter K. Yu, *Bridging the Digital Divide: Equality in the Information Age: Forward*, 20 CARDOZO ARTS & ENT. L.J. 1, 38 (2002) (discussing News Corporation's agreement to censor a controversial book and television channel in order to do business in China).

261. *See, e.g.*, Nart Villeneuve, 6/4 & Censorware (June 4, 2004), http://www.nartv.org/2004/06/04/64-censorware (describing Filter King and Net Police 110 products).

more carefully. These efforts include adopting codes of conduct,[262] factoring human rights explicitly into decisions,[263] and forswearing censorship altogether.[264] Tactics combine financial incentives (including evaluation of filtering transactions in decisions on whether to invest[265]) with corporate governance measures (attempting to mandate consideration of human rights via committees empowered to review a firm's policies[266]) and public relations efforts (seeking to embarrass directors and officers[267]). Investment firms have begun scrutinizing filtering practices by American ISPs, as well as firms operating abroad, using these methods.[268] By using the Framework internally to assess proposed transactions, companies create defensible positions they can articulate to critics.

Even if firms adopt the Framework's metrics to guide corporate actions, there are still two ongoing risks: first, that companies will use them as a cover rather than a genuine component of decisions, and second, that firms will select (or create) metrics designed to legitimize most, if not all, potential clients. These concerns are real, but they can be mitigated. First, using the Framework commits companies to its merit. It forces firms to defend the metrics they use, having conceded the Framework's applicability and the desirability of assessing their conduct. Some measurement constrains better than none. Second, outside watchdogs can check corporate conclusions both from an internal perspective (is the transaction justified under the company's

262. *See, e.g.*, Reporters Without Borders, Joint Investor Statement on Freedom of Expression and the Internet, http://arabia.reporters-sans-frontieres.org/fonds-investissement-en.php3 (last visited Oct. 23, 2009) (listing thirty-five investments firms that signed the statement of principles).

263. *See, e.g.*, Press Release, Boston Common Asset Mgmt. LLC, Human Rights and Internet Fragmentation Proposal Receives Record Shareholder Support (Nov. 15, 2006), http://www.bostoncommonasset.com/news/cisco-agm-111506.html.

264. *See, e.g.*, Google, Definitive Proxy Statement (Schedule 14A), Proposal Number 4, (Mar. 25, 2008) (listing a shareholder proposal calling on Google "not [to] engage in pro-active censorship").

265. *See, e.g.*, Reporters Without Borders, *supra* note 262.

266. *See, e.g.*, Google, Definitive Proxy Statement (Schedule 14A), Proposal Number 5 (Apr. 6, 2007) (proposing the establishment of a Board Committee on Human Rights "authorized to review the implications of company policies, above and beyond matters of legal compliance, for the human rights of individuals in the US and worldwide").

267. *See, e.g.*, *Photo: Chinese Activists Protest Yahoo*, CNET NEWS, Oct. 19, 2005, http://news.cnet.com/2300-1028_3-5902094-1.html.

268. Press Release, Open MIC, OpenMIC Investor Coalition Files Shareholder Resolutions with Internet Service Providers on Freedom of Expression and Privacy (Jan. 28, 2009), *available at* http://www.openmic.org/node/196.

own measurements?) and an external one (is that particular metric defensible?). Other companies' decisions, and justifications, will serve as reference points.

There is value in framing the supply of Internet-restricting technology by Western firms as a decision requiring analysis, disclosure, and justification. Currently, technology companies are opaque, or even misleading, about their relationships with filtering countries.[269] Companies can use the Framework to improve, and defend, decisions about enabling censorship.

2. *Public Regulation*. The Framework can help governments decide whether, and how, to limit firms' ability to sell censorware. So far, companies have generally resolved debates about supplying filtering technology in favor of transactions, generating calls for governmental regulation.[270] Firms have variously supported and opposed such legal rules.[271] Companies favor legislation as a negotiating tool with countries, but are reluctant to accede to regulation that may bar them from certain markets.[272] Nongovernmental organizations and experts line up on both sides of the debate; some see legislation as necessary due to failure of private ordering,[273] and others view law as too blunt of a tool.[274] Similarly,

---

269. *See, e.g.*, Arnoldy, *supra* note 235 (noting that Secure Computing refused to confirm transactions with Tunisia, Saudi Arabia, and the United Arab Emirates, and that Fortinet misled researchers about sales to Burma).

270. *See, e.g.*, Declan McCullagh, *Proposed Law Targets Tech-China Cooperation*, CNET NEWS, Feb. 16, 2006, http://news.cnet.com/Proposed-law-targets-tech-China-cooperation/2100-1028_3-6040303.html (discussing the introduction of the first bill regulating how U.S. companies interact with foreign governments).

271. *See, e.g.*, Declan McCullagh, *"Internet Freedom" Bill Targeting China Cooperation Faces Rough Road*, CNET NEWS, May 28, 2008, http://news.cnet.com/8301-13578_3-9952815-38.html (noting Google's support for and Microsoft's opposition to the Global Online Freedom Act of 2007).

272. *See generally* Anne Broache, *Web Giants Ask for Feds' Help on Censorship*, CNET NEWS, Jan. 30, 2007, http://news.cnet.com/Web-giants-ask-for-feds-help-on-censorship/2100-1028_3-6154930.html (noting that tech companies, like Google, support U.S. laws classifying censorship as a trade barrier).

273. *See, e.g.*, MacKinnon et al., *supra* note 252; Press Release, Amnesty Int'l et al., NGO Joint Statement in Support of H.R. 275 (Oct. 19, 2007), *available at* http://www.amnestyusa.org/Internet_Censorship/HR_275_Support/page.do?id=1081016 (sending a letter to the House Committee on Foreign Affairs supporting the Global Online Freedom Act of 2007 signed by Amnesty International, Human Rights Watch, Reporters Without Borders, China Information Center, and the Religious Freedom Coalition).

274. *See, e.g.*, CTR. FOR DEMOCRACY & TECH., ANALYSIS OF THE GLOBAL ONLINE FREEDOM ACT OF 2008 [H.R. 275] (2008), *available at* http://www.cdt.org/international/censorship/20080505gofa.pdf (expressing concern about a specific bill); Brendan Ballou, Global

scholars have varying receptivity to legislation regarding Internet censorship, though most scholars see private corporate efforts as inadequate.[275] Whether regulation via public law is desirable at all is contested, let alone the details of legislation.

The Framework can aid regulators in three ways. First, governments can analyze other countries' censorship to assess which nations engage in illegitimate filtering and then limit transactions in censorware with such countries.[276] These countries could be targets of a ban on filtering technology sales. Second, the new approach can undercut objections to regulation. Lastly, the methodology can help regulators choose among seller-side, buyer-side, or mixed restrictions. Overall, the Framework best supports buyer-side restrictions and improves regulators' ability to craft such limits. Rules crafted using the Framework would improve upon recent regulatory attempts.

a. Regulation by Public Law. Activists and legislators often propose regulation via public law to limit firms' transactions in Internet censorship gear. There have been serious recent proposals for U.S. legislation to regulate how technology companies sell filtering technology, though none of the proposals has come close to enactment.[277] Some firms support such limits on their behavior (albeit

---

Online Freedom Act: Governments Can't Protect Freedom by Themselves (July 24, 2008), http://futureoftheinternet.org/global-online-freedom-act-governments-cant-protect-freedom-by-themselves (arguing that a specific bill may do more harm than good); John Palfrey, Leaked Cisco Document: Chinese Censorship Among "Opportunities" (May 22, 2008), http://blogs.law.harvard.edu/palfrey/2008/05/22/leaked-cisco-document-chinese-censorship-among-opportunities ("I have not been a supporter of passing a law like the Global Online Freedom Act in its current or historic form, because I think it would have too many unintended consequences.").

275. *See, e.g.*, Surya Deva, *Corporate Complicity in Internet Censorship in China*, 39 GEO. WASH. INT'L L. REV. 255, 315 (2007) (arguing that legislation is legitimate to enforce human rights objectives, but the Global Online Freedom Act "is unlikely to achieve its objectives in its current form"); Mark D. Nawyn, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China*, 2007 COLUM. BUS. L. REV. 505, 549 (supporting legislation generally but noting problems with the Act); *cf.* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 100–01 (2006) (describing the risks of targeting Internet intermediaries via regulation).

276. *See infra* Part III.C.2.c.

277. American firms and legislation have been the focus of such efforts, but there are parallel concerns in other Western countries. For example, Nokia Siemens Networks, a Finnish company, recently faced criticism for supplying technology enabling telephone surveillance to Iran. Christopher Rhoads & Loretta Chao, *Iran's Web Spying Aided by Western Technology*, WALL ST. J., June 22, 2009, at A1. *But see* Press Release, Nokia Siemens Networks, Provision of Lawful Intercept Capability to Iran (June 22, 2009), *available at* http://www.nokiasiemens

weakly[278]), but many companies[279] and commentators[280] oppose them. The Global Online Freedom Act of 2007, for example, sought to develop minimum voluntary corporate standards on Internet freedom;[281] identify Internet-restricting countries; prohibit U.S. companies from storing personally identifiable information there or from providing such information to those governments;[282] require American-owned search engines to provide the State Department with terms and parameters used to alter search results;[283] mandate that U.S. companies provide the State Department with filtered URLs;[284] and ban blocking of U.S. government or government-funded Internet content.[285]

Objections made to the Global Online Freedom Act exemplify the challenges of public regulation in this space. The State Department argued that the bill would place American firms at a competitive disadvantage.[286] The Department of Justice raised several concerns, including the concern that requiring ISPs to carry information could implicate American free speech protections. The Act's definition of "Internet-restricting country" would likely include countries in Western Europe that ban hate speech. And the Act's prohibition of the release of "personally identifiable information" could trap technology companies between the Act and foreign laws

networks.com/global/Press/Press+releases/news-archive/Provision+of+Lawful+Intercept+capability+in+Iran.htm (arguing that Nokia Siemens only provided Iran with the capability to monitor local telephone calls and not Web filtering services).

278. *See, e.g.*, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, *supra* note 214 (statement of Nicole Wong, Deputy General Counsel, Google, Inc.).

279. *See, e.g.*, Anne Broache, *Politicos OK Limits for U.S. Firms in Net-Censoring Countries*, CNET NEWS, Oct. 23, 2007, http://news.cnet.com/8301-10784_3-9802616-7.html (discussing Microsoft and the Computer & Communications Industry Association).

280. *See, e.g.*, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, *supra* note 214 (written statement of John G. Palfrey, Jr. & Colin Maclay, Berkman Center for Internet & Society, Harvard Law School), *available at* http://blogs.law.harvard.edu/palfrey/2008/05/20/testimony-on-internet-filtering-and-surveillance/ ("[L]egal regimes cannot adequately address the dilemmas posed by the rise of global filtering, censorship, and surveillance practices worldwide, and are unlikely to be capable of doing so in the near term.").

281. Global Online Freedom Act of 2007, H.R. 275, 110th Cong. § 201 (2007).

282. *Id.* § 202.

283. *Id.* § 203.

284. *Id.* § 204.

285. *Id.* § 205; *see also* Christopher Stevenson, Note, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, 30 B.C. INT'L & COMP. L. REV. 531, 548–53 (2007) (analyzing the predecessor Act of 2006).

286. McCullagh, *supra* note 271.

requiring disclosure.[287] These concerns, along with corporate opposition, effectively destroyed the Act's chances to become law.[288] As the Global Online Freedom Act furor demonstrates and the next Section discusses, parochial issues, such as concerns about hobbling domestic firms in the international marketplace, and a canonical set of policy protests make public law regulation difficult.

b. Answering Objections. Public regulatory efforts to limit transactions with censoring countries, such as the Global Online Freedom Act, encounter objections along four fronts. First, companies argue that information technology is virtually always dual-use: it can be employed for ends both fair and foul.[289] SmartFilter blocks pornography, political sites, and sites that "offer[] different interpretations of significant historical facts" with equal ease.[290] Thus, responsibility should be placed upon users rather than manufacturers. Second, even if companies censor directly, they argue that a limited platform for expression and information exchange is preferable to no platform.[291] Third, firms point to their obligation to obey local laws: much as U.S. intellectual property law pushes Google to remove search results that may infringe copyright, China requires it to delist political opposition content.[292] This hints at hypocrisy—why should the United States complain about censorship when America has its own content restrictions? Fourth, companies worry about

287. Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Dep't of Justice, to the Honorable Howard L. Berman, Acting Chairman, H. Comm. on Foreign Affairs (May 19, 2008), *available at* http://politechbot.com/docs/doj.letter.gofa.052708.pdf.

288. *See* Declan McCullagh, *White House Opposition Likely Dooms Anti-China Internet Bill*, CNET NEWS, May 30, 2008, http://news.cnet.com/8301-13578_3-9956124-38.html (predicting that the Bush Administration's opposition "is likely to doom the legislation").

289. *See* Derek E. Bambauer, *Cool Tools for Tyrants*, LEGAL AFF., Jan./Feb. 2006, *available at* http://www.legalaffairs.org/issues/January-February-2006/feature_bambauer_janfeb06.msp.

290. *See* McAfee Secure Computing, *supra* note 113 (describing "Pornography," "Politics/Opinion," and "Historical Revisionism" content categories).

291. *See, e.g.*, Nate Anderson, *Yahoo on China: We're Doing Some Good*, ARS TECHNICA, May 12, 2006, http://arstechnica.com/old/content/2006/05/6823.ars; Alison Maitland, *Skype Says Texts Are Censored by China*, FIN. TIMES, Apr. 19, 2006, at 25, *available at* http://www.ft.com/cms/s/2/875630d4-cef9-11da-925d-0000779e2340.html; Andrew McLaughlin, *Google in China*, OFFICIAL GOOGLE BLOG, Jan. 27, 2006, http://googleblog.blogspot.com/2006/01/google-in-china.html.

292. *See, e.g.*, Tom Krazit, *Google's Censorship Struggles Continue in China*, CNET NEWS, June 16, 2009, http://news.cnet.com/8301-17939_109-10265123-2.html; G. Jeffrey MacDonald, *Congress's Dilemma: When Yahoo in China's Not Yahoo*, CHRISTIAN SCI. MONITOR, Feb. 14, 2006, at 1, *available at* http://www.csmonitor.com/2006/0214/p01s04-usfp.html.

displacement. If Cisco cannot sell filtering routers to China, then Huawei may displace them from one of the world's most lucrative markets. Finally, laws on filtering require restricting access, but not providing information, making compliance easier—and perhaps less visible—for companies.

The Framework can help evaluate arguments on dual-use and abiding by local law, and, by extension, the merits of claims that export regulation should be minimized or prevented.[293] Regarding the legitimacy of dual-use technology, the Framework helps predict how a country will actually use the technology it procures. Firms generally evade the issue of how a country is likely to employ its new capabilities, which is precisely what the Framework helps uncover.[294] This predictive approach has helped regulate other dual-use technologies. For example, U.S. law prevents handgun sales to felons,[295] but not to fearful homeowners. Companies are liable for products intended or designed to infringe copyrights,[296] but not for those capable of "substantial noninfringing uses."[297]

The legitimacy of selling dual-use technology can be assessed by examining two factors. First, how is the filtering country likely to use the new gear? Cisco had to know that its Policenet system would be used by China not just for crime prevention, but for political control.[298] Second, will the new technology expand the country's capabilities, allowing it to broaden censorship? And is it inclined to

293. The other two contentions are beyond the methodology's reach. Whether a country has a sufficiently developed domestic technology industry to sustain filtering without outside assistance is an empirical question. Whether a censored Internet shaped with Western technology is better than one without is a philosophical question, though recent data suggests Chinese Internet users have access to 20 percent more Web content on controversial topics due to the presence of Google, Microsoft, and Yahoo! Villeneuve, *supra* note 100, at 17.

294. They also elide the question of initial design: when a manufacturer knows a product can be used for multiple purposes—some legitimate and some not—should that producer design it to minimize harmful uses? *See* Bambauer, *supra* note 289; Brief of Amici Curiae Emerging Technology Companies in Support of Respondents at 21–25, MGM Studios v. Grokster, 545 U.S. 913 (2005) (No. 04-480).

295. 18 U.S.C. § 922(d)(1) (2006).

296. *Grokster*, 545 U.S. at 919 ("One who distributes a device with the object of promoting its use to infringe copyright . . . is liable for the resulting acts of infringement by third parties."); *see also* A&M Records v. Napster, 239 F.3d 1004, 1022 (9th Cir. 2001) (affirming the award of a preliminary injunction against an online file-sharing technology company).

297. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 442 (1984).

298. *See, e.g.*, GUTMANN, *supra* note 233, at 167–71; Rebecca MacKinnon, More on Cisco in China (June 30, 2005), http://rconversation.blogs.com/rconversation/2005/06/more_on_cisco_i.html.

do so? Ethiopia blocks some content critical of its government on political and human rights grounds, and it would clearly prefer to expand its filtering. But the state-owned ISP in Ethiopia lacks the sophistication to do so.[299] Thus, selling a comprehensive filtering solution to Ethiopia would likely expand the country's censorship, decreasing its legitimacy. The Framework's analysis reveals what a country does with existing capabilities, and how legitimate those actions are. Thus, regulators can look to this track record to assess the propriety of selling new gear to that nation. In this way, the Framework can help evaluate the desirability of dual-use sales.

Technology companies reiterate their need to comply with local laws and regulations where they operate.[300] This position is a truism—companies are expected to operate lawfully—and also a means of shifting attention from their actions to those of the censoring country. But this argument binds companies as much as it frees them; it requires that a firm's actions comport with express laws or regulations, and not merely governmental preference. Companies, though, are highly responsive to informal government pressures on filtering. This is the case not only in China,[301] but also in Britain,[302] Denmark,[303] Sweden,[304] and the United States.[305] The Framework's methodology can help outside analysts evaluate whether technology companies are simply following the rules or are currying favor by blocking sensitive content while hiding behind legalistic justifications.

---

299. *See* OPENNET INITIATIVE, ETHIOPIA 4 (2007), http://opennet.net/sites/opennet.net/files/ONI_Ethiopia_2007.pdf (describing Ethiopia's hit or miss Internet censorship, in which some sports enthusiasts' blogs are blocked while some opposition political sites remain accessible); Andrew Heavens, You Block Blogspot, I Block Boing Boing (Oct. 8, 2007), http://www.meskelsquare.com/archives/2007/10/ethiopia_blocks.html.

300. *See, e.g.*, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, *supra* note 214 (statement of Michael Samway, Vice President & Deputy General Counsel, Yahoo! Inc.), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7182; Frank Davies, *Holding Their Feet to the Fire: Google, Yahoo, Cisco Face Angry Senators on Rights of Users in Repressive Nations*, SAN JOSE MERCURY NEWS, May 21, 2008, at 1C; Matt Marshall, *Microsoft and Bokee Mired in Chinese Free-Speech Controversy*, MERCURY NEWS, Jan. 4, 2006, http://www.siliconbeat.com/entries/2006/01/04/microsoft_and_bokee_mired_in_chinese_freespeech_controversy.html; *Google to Censor Itself in China*, CNN.COM, Jan. 26, 2006, http://www.cnn.com/2006/BUSINESS/01/25/google.china/.

301. *See, e.g.*, *supra* notes 271, 300.

302. *See supra* notes 124–26 and accompanying text.

303. *Filter Blocks Danes from Accessing Child Pornography*, FIN. MIRROR, Nov. 28, 2005.

304. Press Release, Telenor, Telenor and Swedish National Criminal Investigation Department to Introduce Internet Child Porn Filter (May 17, 2005), *available at* http://press.telenor.com/PR/200505/994781_5.html.

305. *See supra* notes 150–54 and accompanying text.

Companies also worry about being displaced by competitors. Unilateral limits on American firms could lead a country to substitute products or services from companies in nations with more lax regulation. Companies might also evade restrictions through clever restructuring. Yahoo! runs its operations in China through Alibaba, a Chinese corporation in which Yahoo! holds a 40 percent ownership stake.[306] This enables Yahoo! to comply with China's censorship demands while shifting responsibility to Alibaba (which cooperates enthusiastically).[307] In addition, the Justice Department's objection picks up on a potential inconsistency: it seeks to hamper Internet censorship abroad without examining relevant American practices.[308]

Finally, American companies can comply with local laws mandating censorship because they are tilted toward filtering: blocking material is either required or optional, but there are no affirmative requirements to make information available. The Framework thus helps moderate the force of standard objections to regulating sales of censorship technology by assessing their merit more clearly.

c. Selecting Targets. Lastly, the Framework can help in making the choice among regulatory targets. Public law regulation of technology transactions can focus on sellers, buyers, or both. The Framework suggests that buyer-side restraints are likely best and most effective; moreover, the process-based approach makes implementing such restrictions more feasible.

Constraining sellers' behavior limits what one can send abroad—for example, American companies must obtain permission before exporting strong encryption technologies.[309] Limiting buyers prevents firms from conducting business in certain countries. American regulation of technology transactions employs both modes. The United States bans most trade to countries seen as sponsors of terrorism, such as Iran.[310] U.S. companies cannot export goods or

306. Tom Zeller, Jr., *Internet Firms Facing Questions About Censoring Online Searches in China*, N.Y. TIMES, Feb. 15, 2006, at C3.

307. *See* Stuart Biggs, *Under Oath and Under Pressure*, S. CHINA MORNING POST, Feb. 21, 2006, at 1 (quoting Alibaba's chief executive as saying "[w]e are very co-operative with the authorities").

308. Frank Davies, *Internet Freedom: Pressure Growing*, SAN JOSE MERCURY NEWS, July 22, 2006, at A1 (quoting former CNN Beijing bureau chief Rebecca MacKinnon as calling the Act's 2006 predecessor "hypocritical and arrogant" for this reason).

309. 15 C.F.R. § 742.15(b)(2) (2009).

310. *See id.* §§ 742.8, 746.7.

services to Cuba without a license from the Department of Commerce (which customarily denies applications),[311] and foreign firms that do business there face penalties if a transaction involves property confiscated by Cuba's government.[312] There are also technology-specific embargoes on nations such as China.[313] Even these limits have exceptions and uncertainties. Cisco sells police technologies to China's state security forces that may run afoul of the post-Tiananmen Square statute limiting such exchanges—though Cisco argues that they do not.[314]

Targeting sellers is much more challenging for regulators, for three reasons. First, regulating dual-use technology is hard, as previously discussed. Second, seller-side restrictions run counter to the goals of potential customers, who may pressure companies to evade the regulation or opt for non-U.S. providers. Finally, Internet censorship is dynamic, and public law regulation is relatively static. Even well-crafted laws may rapidly become irrelevant. Regulations designed for Web sites may struggle with new issues specific to user-generated video (consider YouTube) or text messaging (think Twitter).[315]

Regulating buyers is the better path, and the Framework can help by enabling evaluation of whether purchasers of censorship technology use it for legitimate purposes. The more legitimate the

311. *Id.* § 746.2; *see also* U.S. DEP'T OF COMMERCE, BUREAU OF INDUSTRY AND SECURITY, 2004 REPORT ON FOREIGN POLICY-BASED EXPORT CONTROLS 40 (2005), *available at* http://www.bis.doc.gov/policiesandregulations/05forpolcontrols/04finalfpreport.pdf (stating that the Department "generally denies license applications for exports" of most items to Cuba, subject to certain "case-by-case" exceptions).

312. 22 U.S.C. § 6082 (2006); *see also, e.g.*, Adam Liptak, *A Wave of the Watch List, and Speech Disappears*, N.Y. TIMES, Mar. 4, 2008, at A16 (describing the actions of the U.S. Treasury Office of Foreign Assets Control to block access to the website of a British national organizing trips to Cuba for European tourists).

313. *See* Foreign Relations Authorization Act for Fiscal Years 1990–1991, Pub. L. No. 101-246 § 902(a)(4), 104 Stat. 15, 83 (1990) (suspending export licenses for crime control and detection equipment to China after the Tiananmen Square repression of 1989).

314. *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, *supra* note 214, at 88 (statement of Mark Chandler, Senior Vice President Legal Servs., General Counsel and Secretary, Cisco Systems, Inc.), *available at* http://judiciary.senate.gov/pdf/08-05-20Mark_Chandler_Testimony.pdf; *see also* Bambauer, *supra* note 289.

315. *See* Ryan Singel, *Seeking Tighter Censorship, Repressive States Target Web 2.0 Apps*, WIRED, Mar. 4, 2008, http://blog.wired.com/business/2008/03/etech-what-happ.html; Ethan Zuckerman, The Cute Cat Theory Talk at ETech (Mar. 8, 2008), http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech/ (discussing censorship of Web 2.0 technologies and describing a Tunisian video mash-up of Apple's famous "1984" ad used to criticize President Ben Ali).

restrictions, the fewer concerns regulators should have about private firms supporting them. The Framework provides a yardstick to assess countries' behavior, and hence whether corporations should transact business with them. Metrics-based analysis gives regulators more information to evaluate the problem (suspect sales, such as Fortinet's to Burma, may be unusual) and, if necessary, to craft a response. Moreover, the Framework should help simplify any regulation that develops. It is easier to forbid selling filtering technology to Uzbekistan than to define what personally identifiable information can be stored there.[316]

Buyer-targeted regulation offers ancillary benefits such as lower administrative and enforcement costs. For example, American companies cannot lawfully sell software to Iran.[317] Secure Computing has stated that the SmartFilter software used by Iranian ISPs such as ParsOnline is unauthorized.[318]

If the company had sold SmartFilter to ParsOnline, the violation would be clear and inexpensive to detect.[319] In contrast, the legality of sales to China depends upon the products involved.[320] Whether sales of Cisco's Policenet to China contravene export restrictions depends partly on whether Cisco developed the system's database and partly on whether Policenet is an "identification retrieval system."[321] This determination is not only unclear prospectively, it is a complex question that is costly to adjudicate. Regulation that is focused on the

316. *Cf.* Jeffrey Gedmin, *Reporting Among Gangsters*, WASH. POST, July 2, 2008, at A15 (describing the Uzbek regime as authoritarian and prone to human rights abuses).

317. 31 C.F.R. § 560.204 (2008); *see also* Sun Microsystems, Embargoed Countries, http://www.sun.com/sales/its/countries/Embargoed.html (last visited Oct. 23, 2009) (listing Iran as an embargoed country).

318. OPENNET INITIATIVE, INTERNET FILTERING IN IRAN 2004–2005, at n.1 (2005), http://opennet.net/studies/iran#1.

319. *See, e.g.*, OPENNET INITIATIVE, *supra* note 118, § 4.C.2.c (describing test used to determine if an ISP uses SmartFilter).

320. *See* Keith Bradsher, *At Trade Show, China's Police Shop for the West's Latest*, N.Y. TIMES, Apr. 26, 2008, at C1.

321. 15 C.F.R. § 774, Supp. 1, ECCN no. 3A981 (2008) (identifying "automated fingerprint and identification retrieval systems" as controlled for crime control reasons under the Export Administration Regulations (EAR)); *see also* MacKinnon, *supra* note 298 (alleging that Cisco "appear[s] to be directly flaunting" United States export restrictions by advertising its products for use by police in China and by building the structure of the Chinese police database); 15 C.F.R. § 738 Supp. 1 (identifying the export to China of items classified as crime control 1 as subject to EAR license requirements); *id.* § 742.7(a)(1) (defining the export of technology classified as crime control as subject to regulation under the EAR); Bambauer, *supra* note 289 (suggesting that Policenet may have been used to apprehend political prisoner Zheng Yichun).

legitimacy of the buyer's censorship is not only easier to comply with but also cheaper to enforce.

Gathering additional information could improve regulation by providing more data to analyze using the Framework's metrics. Moreover, the Framework can suggest likely initial targets for mandatory data provision efforts. First, if regulators consider seriously regulating technology sales to filtering countries, they should gather data that would improve policymaking via mandatory, limited disclosure of corporate transactions. To assess whether public law is necessary, regulators need accurate information on the scope of the activity at issue. Corporations, though, are loath to provide specifics about sales of filtering technology.[322] Determining this data from public filings or statements can be difficult or impossible.[323] A confidential reporting system would improve regulatory decisions.

Crafting the disclosure system would require care to avoid collecting irrelevant data (exposing companies to unnecessary cost) and to avoid missing relevant transactions (depriving regulators of useful information). Limiting the number of countries for mandatory reporting would be useful. Studying transactions with Mexico, which does not censor the Internet,[324] would not help; capturing data about Vietnam would. To choose which countries to target, the system could select countries in which, according to the Framework, online restraints fall below a minimum threshold of legitimacy. Alternatively, the State Department could select the countries based on its annual Human Rights Reports,[325] or the system could target states identified as repressing Internet content[326] or with documented instances of Internet filtering.[327]

---

322. *See, e.g.*, Arnoldy, *supra* note 235; Bambauer, *supra* note 289 (noting that Cisco does not disclose sales figures for China).

323. Secure Computing, for example, discloses only that 36 percent of 2007 revenues came from international sales, and that major foreign markets include China. Secure Computing Corp. Annual Report (Form 10-K), at 29 (Mar. 5, 2008).

324. Kathleen Connors et al., OpenNet Initiative, Latin America, http://opennet.net/research/regions/la (last visited Oct. 25, 2009).

325. U.S. Dep't of State, Human Rights, http://www.state.gov/g/drl/rls/hrrpt/ (last visited Oct. 23, 2009).

326. Reporters Without Borders, List of the 13 Internet Enemies (Nov. 7, 2006) http://www.rsf.org/spip.php?page=article&id_article=19603 (maintaining a list of countries that "systematically violate online free expression").

327. *E.g.*, Zittrain & Palfrey, *supra* note 11, at 103; Opennet Initiative, Research, http://opennet.net/research (last visited Oct. 23, 2009).

Some technology is irrelevant to Internet filtering—for example, Apple's iPhone—and should be excluded from reporting. To address dual-use items, regulators should again focus on buyers. A simple and cheap, though admittedly imperfect, rule would mandate submitting data about sales to government agencies or service providers in targeted countries, or about transactions in which the reporting entity acts as an online service provider.[328] To avoid evasion, providers could be required to obtain, and report, data from distributors and subsidiaries.

A disclosure requirement—however limited—is likely to be opposed by technology companies. Regulation that focuses on buyers, however, combined with clear requirements from the Framework's metrics, will make mandatory information provision less onerous. Past attempts to require disclosure of transactions with "terrorist-sponsoring states"[329] or potential environmental liabilities[330] elicited substantial corporate opposition. There are, however, analogous programs designed to improve public regulation that suggest that this reporting system need not be onerous or risky for firms. For example, the National Practitioner Data Bank (NPDB) collects information about civil judgments, settlements, and criminal convictions against physicians and health care providers for malpractice.[331] Insurers and other payers must report data to the NPDB.[332] The general public cannot access these records, but regulators such as state licensing boards, professional societies, and federal agencies can.[333] Regulators have used NPDB data to analyze such regulatory questions as the role of malpractice insurance premiums in rising health care costs,[334]

328. The regulation could incorporate the Digital Millennium Copyright Act's definition of "service provider." *See* 17 U.S.C. § 512(k)(1) (2006).

329. *See, e.g.*, Floyd Norris, *S.E.C. Rethinks Lists Linking Companies and Terrorist States*, N.Y. TIMES, July 21, 2007, at C2.

330. *See, e.g.*, William Baue, *SEC Urged to Strengthen Rules Governing Corporate Disclosure of Environmental Risks*, SOCIALFUNDS, Aug. 21, 2002, http://www.socialfunds.com/news/article.cgi/911.html; Barnaby J. Feder, *New Battles over Disclosure*, N.Y. TIMES, June 24, 1990, at F10.

331. Health Care Quality Improvement Act of 1986, 42 U.S.C. §§ 11131–34 (2006); *see also* U.S. Dep't of Health & Human Servs., National Practitioner Data Bank, http://www.npdb-hipdb.hrsa.gov/npdb.html (last visited Oct. 23, 2009).

332. 42 U.S.C. § 11131.

333. *Id.* § 11137.

334. U.S. GAO, NO. GAO-03-836, MEDICAL MALPRACTICE: IMPLICATIONS OF RISING PREMIUMS ON ACCESS TO HEALTH CARE *passim* (2003), *available at* http://www.gao.gov/new.items/d03836.pdf.

and whether to limit damages in medical malpractice lawsuits.[335] Regulators gain access to data otherwise unavailable (settlement agreements are typically confidential), whereas participants remain shielded from public scrutiny. There are similar systems for reporting storage of toxic chemicals[336] and "near miss" aviation safety incidents.[337] Disclosure of transactions involving censorship technology would improve regulators' ability to determine whether such sales are problematic and develop a response if necessary. Confidentiality would protect companies from reputational harm, thereby reducing their opposition and making the system more viable politically.

* * *

Regulating information technology transactions is difficult substantively and politically. The Framework can help regulators determine whether public law constraints on corporate transactions with censoring countries are necessary by analyzing how those customers employ the gear. Its methodology helps address objections based on the challenges of dual-use technology and obeying local law, and suggests that focusing on buyers is the optimal regulatory strategy.

3. *Third-Party Evaluation*. Filtering opens countries to an array of external criticism, including Slashdot discussions,[338] State Department reports,[339] press freedom analysis,[340] and United Nations

335. *See, e.g.*, Richard A. Oppel, Jr., *Bush Enters Fray over Malpractice*, N.Y. TIMES, Jan. 17, 2003, at A24 (citing NPDB data on average malpractice judgment awards).

336. 42 U.S.C. § 11023 (2008); 40 C.F.R. § 372.1 (2008); *see also* U.S. EPA, What Is the Toxics Release Inventory (TRI) Program, http://www.epa.gov/tri/triprogram/whatis.htm (last visited Oct. 23, 2009). Toxics data is publicly available, though. *See* MARY GRAHAM, DEMOCRACY BY DISCLOSURE 21–61 (2002).

337. NASA, ASRS—Aviation Safety Reporting System, http://asrs.arc.nasa.gov/overview/summary.html (last visited Oct. 23, 2009). While incident reports to ASRS are voluntary, they are confidential, and policymakers employ them in crafting regulations. NASA, PUB. 60, ASRS: THE CASE FOR CONFIDENTIAL INCIDENT REPORTING SYSTEMS 7 (2001), *available at* http://asrs.arc.nasa.gov/docs/rs/60_Case_for_Confidential_Incident_Reporting.pdf.

338. *See, e.g.*, *Three ISPs Agree to Block Child Porn*, SLASHDOT, June 10, 2008, *available at* http://yro.slashdot.org/article.pl?sid=08/06/10/1819200.

339. *See* U.S. Dep't of State, *supra* note 325.

340. *See, e.g.*, Reporters Without Borders, Dictatorships Get to Grips with Web 2.0 (Feb. 1, 2007), http://www.rsf.org/article.php3?id_article=20844.

evaluations,[341] among others. Internet censorship has received increased attention in recent years from evaluators such as the U.S. Department of State.[342] There are many organizations that evaluate censorship, freedom of expression, press freedom, and related issues, including Amnesty International, Human Rights Watch, Reporters Without Borders, International Freedom of Expression Exchange (IFEX), the U.S. State Department, and the U.N. Human Rights Council. Their assessments employ different methodologies—from legal probes of a country's censorship[343] to limited quantitative analysis[344] to careful empirical testing.[345] This methodological diversity can paint a more complete picture, but it makes comparison challenging. (Indeed, it can complicate assessing a single country because groups emphasize various factors: Venezuela does not filter, but its media restrictions[346] and informal pressures on independent journalists[347] limit Internet freedom of expression.)[348] By using the process-oriented Framework methodology, third parties can take different normative positions on filtering and on how a country implements it, while increasing their assessments' rigor and improving comparability.

For example, Reporters Without Borders (RSF)[349] classifies countries it regards as violating freedom of expression or the press online as either Internet Enemies or Under Surveillance.[350] At the

341. *See, e.g.*, UN HUMAN RIGHTS COUNCIL, REPORT OF THE WORKING GROUP ON THE UNIVERSAL PERIODIC REVIEW—TUNISIA 10, 12 (2008).

342. Bradley Graham, *Violence Said to Slow Rights Effort in Iraq: Report Lauds Steps Toward Democracy*, WASH. POST, Mar. 9, 2006, at A15 (quoting the Assistant Secretary for Human Rights on "growing attention to government censorship of the Internet").

343. *See, e.g.*, HUMAN RIGHTS WATCH, FREEDOM OF EXPRESSION AND THE INTERNET IN CHINA 2–6 (2001), *available at* http://www.hrw.org/en/reports/2001/08/01/freedom-expression-and-internet-china (analyzing Chinese laws used to regulate Internet content).

344. *See, e.g.*, Reporters Without Borders, Test of Filtering by Sohu and Sina Search Engines Following Upgrade (June 22, 2006), http://www.rsf.org/article.php3?id_article=18015. *But see* Villeneuve, *supra* note 100, at 21 (describing problems with the study's methodology).

345. *See, e.g.*, OPENNET INITIATIVE, *supra* note 116.

346. Human Rights Watch, Venezuela: TV Shutdown Harms Free Expression (May 21, 2007), http://hrw.org/english/docs/2007/05/22/venezu15986.htm.

347. *See, e.g.*, Simon Romero, *Chavez Looks at His Critics in the Media and Sees the Enemy*, N.Y. TIMES, June 1, 2007, at A6.

348. OPENNET INITIATIVE, VENEZUELA (2007), http://opennet.net/research/profiles/venezuela.

349. Reporters Without Borders is better known as Reporters Sans Frontières (RSF); the organization is based in France.

350. *See supra* note 326.

extremes, it is difficult to quarrel with RSF's sorting: North Korea's Internet censorship trumps Jordan's. But the organization's methodology is less clear in the middle. RSF lists Egypt as an Internet Enemy, while classifying Tajikistan as Under Surveillance, a lesser designation. In contrast, OpenNet Initiative finds that Egypt does not filter, although bloggers and journalists have been imprisoned or harassed,[351] but finds that Tajikistan filters political content.[352] What makes Egypt's online controls[353] worse than Tajikistan's,[354] or vice-versa? Assessments of Internet content control would improve with a consistent methodology that does not depend on what material is restricted and that reveals how RSF classifies countries. Employing the Framework here would improve analytical coherence.

External evaluations of censorship face at least two challenges. First, a country may simply (and perhaps plausibly) claim that its filtering prevents social harms and is thereby justified.[355] Second, the country may critique its critics, charging that they too engage in such practices and consequently are hypocritical.[356] China recently rebutted American criticism of its human rights record by pointing to U.S. abuse of prisoners held at military bases in Guantanamo Bay and Iraq, as well as America's surveillance of international communications.[357] These responses achieve two ends: mitigating negative analysis by showing that questionable practices are widespread and reducing a critic's credibility.[358] In the filtering context, countries such as China frequently point to other nations'

351. OPENNET INITIATIVE, EGYPT (2009), http://opennet.net/research/profiles/egypt.

352. OPENNET INITIATIVE, TAJIKISTAN (2007), http://opennet.net/research/profiles/tajikistan.

353. Reporters Without Borders, Internet Enemies: Egypt (Mar. 12, 2009), http://www.unhcr.org/refworld/docid/4a38f987c.html.

354. Reporters Without Borders, Countries Under Surveillance—Tajikistan, http://arabia.reporters-sans-frontieres.org/article.php3?id_article=26127 (last visited Oct. 23, 2009).

355. For a discussion of Vietnamese claims regarding censorship, see *supra* note 87.

356. *Cf.* David J. Rothkopf, *Values Conundrum: Will the U.S. and China Play by the Same Rules?*, WASH. POST, July 11, 2005, at A15 ("The first step is recognizing everyone's hypocrisy.").

357. *See, e.g.*, Calum MacLeod, *China: U.S. Criticism of Human Rights Record Is "Hypocrisy,"* USA TODAY, Mar. 10, 2006, at 9A.

358. *See, e.g.*, Frank Davies, *U.S. Criticizes Abuses of Human Rights but It Has Used Many of the Same Tactics*, ST. PAUL PIONEER PRESS, Mar. 1, 2005, at A5 (noting the U.S. State Department's criticism of Pakistan, Egypt, and Syria for employing methods that the U.S. employed when interrogating captives).

practices and portray their own efforts as similar.[359] The Framework addresses both issues. It offers a consistent means to evaluate Internet censorship by all countries, distinguishing legitimate from illicit practices. In addition, its analysis reveals how well a government sets forth the harms it seeks to prevent and how well filtering targets them.

If third-party analysts moved toward convergent criteria for measuring Internet censorship, it would be easier to compare—and critique—their evaluations. Freedom House and OpenNet Initiative both describe how they rate countries (Freedom House, for press freedom;[360] ONI, for Internet filtering[361]). Thus, one can compare Freedom House's negative evaluation of Oman with ONI's relatively positive one.[362] It is possible to reconstruct these conclusions based on each organization's methodology, and to see how differences result from their distinct analytical focus. Oman suppresses little speech technologically (ONI), but much via legal, economic, and informal pressures (Freedom House).

One criticism is that this proposal assumes away the problem: the difficulty lies in convincing organizations with different goals and values to adopt a similar methodology. This critique is partly correct: some evaluators might not be concerned with accountability, or might ground their analysis in substantive principles. There are two reasons for optimism, though. First, because it is process-focused, the Framework is compatible with disparate normative views on content restrictions. The Framework clarifies what restraints exist and how they are determined, without taking a content-based position. Second, analysts and commentators frequently advert to the Framework's criteria.[363] Openness, transparency, narrowness, and

---

359. *See, e.g.*, Joseph Kahn, *China Defends Internet Censorship*, INT'L HERALD TRIB., Feb. 14, 2006, *available at* http://www.iht.com/articles/2006/02/14/business/net.php (quoting an official in the Information Office of the Chinese State Council that, in view of "the main international practices in this regard, you will find that China is basically in compliance with the international norm").

360. FREEDOM HOUSE, FREEDOM OF THE PRESS: METHODOLOGY (2007), http://www.freedomhouse.org/template.cfm?page=350&ana_page=339&year=2007.

361. Faris & Villeneuve, *supra* note 85, at 5–27.

362. *Compare* FREEDOM HOUSE, MAP OF PRESS FREEDOM: OMAN (2007), http://www.freedomhouse.org/template.cfm?page=251&country=7246&year=2007 (labeling Oman as "Not Free," and ranking it 165 out of 195 countries), *with* OPENNET INITIATIVE, *supra* note 179 (noting that Oman has highly transparent and consistent filtering).

363. *See, e.g.*, OPENNET INITIATIVE, INTERNET FILTERING IN ASIA 11 (2009), http://opennet.net/sites/opennet.net/files/ONI_Asia_2009.pdf (evaluating the transparency of the Thai

accountability comprise the most commonly expressed principles used to analyze Internet censorship. This increases the likelihood that the Framework will be broadly acceptable.

Finally, watchdogs should use the Framework for positive reinforcement as well as criticism. Organizations should use metrics to confer recognition—their "seal of approval"—on countries that score as legitimate as well as technology companies that engage in transactions only with these nations. This certification approach has many analogues. Web sites can obtain certification from the Better Business Bureau[364] and TRUSTe[365] for meeting data privacy requirements. Agricultural vendors can emblazon their coffee beans, flowers, and chocolate with a Fair Trade Certified logo if they purchase from growers who meet environmental and economic standards.[366] Forest products, such as paper and wood, and the land management that produces them, can obtain certification from monitors accredited by the Forest Stewardship Council (FSC). These certifiers implement FSC's criteria and standards but employ their own methodology for evaluating compliance.[367] Certification systems provide positive incentives to engage in desired behaviors as well as negative incentives to avoid unfavorable ones. In effect, the rating entity lends its prestige to the companies it certifies. Similarly,

---

legal process for implementing selective "geolocational filtering"); MacKinnon et al., *supra* note 252, at 87 (urging the Chinese government to create a transparent process for the public to challenge censorship decisions); FREEDOM HOUSE, *supra* note 360 (evaluating a country's press freedoms based on the transparency of media ownership structures); Villeneuve, *supra* note 100 (specifically noting that the Chinese government's process for determining which material should be censored lacks both transparency and accountability); Zittrain & Palfrey, *supra* note 11, at 115–16, 238 (noting that when local authorities require Microsoft to block content, Microsoft makes efforts to make this process transparent); Joint Declaration of the OSCE Representative on Freedom of the Media & Reporters Sans Frontières on Guaranteeing Media Freedom on the Internet (June 18, 2005), http://www.rsf.org/IMG/pdf/declaration_anglais.pdf (stressing that proceedings to determine the legality of Web site content should guarantee transparency and accountability).

364. Better Bus. Bureau, BBB Online Business Program, http://www.bbb.org/us/bbb-online-business/ (last visited Oct. 23, 2009).

365. TRUSTe Homepage, http://www.truste.org/businesses/web_privacy_seal.php (last visited Oct. 23, 2009). *But see* Ben Edelman, Certifications and Site Trustworthiness (Sept. 25, 2005), http://www.benedelman.org/news/092506-1.html (finding that 5.4 percent of TRUSTe's certified Web sites are labeled untrustworthy by SiteAdvisor, versus 2.5 percent of Web sites listed overall).

366. *See* TransFair USA, Fair Trade Certification Overview, http://www.transfairusa.org/content/certification/overview.php (last visited Oct. 23, 2009).

367. Forest Stewardship Council, What Is "Certification"?, http://www.fscus.org/faqs/what_is_certification.php (last visited Oct. 23, 2009).

filtering certifications could be touted by countries in international fora (such as the Internet Governance Forum, or the U.N. Human Rights Council) or by companies when criticized.

Seals of approval for filtering countries or companies assisting them will encounter at least two objections. First, some critics will disapprove of conferring any legitimacy upon online censorship. Although it is defensible, this position runs counter to strong support in most countries for restricting access to certain material. Moreover, public support means that governments are likely to censor, and the goal of certification is to press them to do so with maximal legitimacy.

Second, there is a risk of strategic behavior. Countries and companies will probably either turn to or create friendly rating entities to award certification on easy terms. This may be particularly problematic during the early phase of evaluation, when third-party observers have not yet established sufficient recognition or credibility to counteract technological "greenwashing."[368] If observers look merely for a label, rather than its backer, this tactic can succeed.[369] This problem, however, can be mitigated. Organizations with credible reputations, such as Human Rights Watch or the Center for Democracy & Technology, should leverage existing recognition in the new zone of filtering certification. Greenwashing, or its censorship equivalent, is in itself a partial victory: it occurs when companies recognize that reputation in an area such as environmental practices motivates economic decisions by consumers.[370] It signifies a shift in expectations about acceptable behavior. Similarly, even weak certifications commit companies to the principle that legitimacy in Internet censorship is important but uncertain, and their decisions to support it are properly subject to outside review. Public scrutiny can

368. *See, e.g.*, TERRACHOICE, THE "SIX SINS OF GREENWASHING" 2–4 (2007), *available at* http://www.terrachoice.com/files/6_sins.pdf. *See generally* John M. Conley & Cynthia A. Williams, *Engage, Embed, and Embellish: Theory Versus Practice in the Corporate Social Responsibility Movement*, 31 IOWA J. CORP. L. 1, 18–20 (2005) (observing that watchdog organizations like Greenpeace must take care to "avoid complicity" in corporate efforts to conceal "environmental malfeasance").

369. *But see* Eric Pfanner, *Cooling Off on Dubious Eco-Friendly Claims*, N.Y. TIMES, July 18, 2008, at C3 (noting that consumers have become skeptical of misleading claims of environmental friendliness).

370. *See generally* Joshua A. Newberg, *Corporate Codes of Ethics, Mandatory Disclosure, and the Market for Ethical Conduct*, 29 VT. L. REV. 253, 287–94 (2005) (arguing that firms "actively compete on the basis of ethical commitments" when their conduct is made transparent).

help convert these rhetorical commitments to action, even if it is limited.

The Framework improves third-party analysis of Internet censorship by making it more consistent, rigorous, and readily comparable. Outside groups should use the Framework's results to offer rewards that balance their critiques.

* * *

Metrics based on the Framework can help address three challenging problems: (1) how corporations decide whether to help a state censor the Internet; (2) whether a country should use public law to regulate those companies' decisions; and (3) how third parties should evaluate filtering in a defensible, rigorous, reproducible, and comparable way. The Framework is not a panacea, but it is a useful tool for tackling each challenge.

IV. CHALLENGES AND LIMITATIONS

There are three important challenges that complicate application of the Framework and metrics, namely, circumvention, interdependence, and China. Circumvention—often portrayed uncritically as an antidote to censorship—is more appropriately assessed under the Framework's rubric as well. The term covers a panoply of technological methods that bypass online censorship.[371] With a tool such as Anonymizer, an Internet user can reach material that is otherwise blocked.[372] Circumvention includes using proxy servers to fetch prohibited material on one's behalf,[373] routing requests through specialized unfiltered network nodes such as Tor,[374] and accessing blocked pages from a search engine's cache.[375] Falun Gong practitioners have developed sophisticated software tools to

371. *See generally* CITIZEN LAB, EVERYONE'S GUIDE TO BY-PASSING INTERNET CENSORSHIP (2007), *available at* http://citizenlab.org/CL-circGuide-online.pdf (describing several circumvention technologies such as Web tunneling software and anonymous communication systems, as well as explaining their use).

372. *See* Anonymizer, Frequently Asked Questions, http://www.anonymizer.com/company/about/anonymizer-faq.html (last visited Oct. 23, 2009).

373. *See, e.g.*, Psiphon Homepage, http://psiphon.ca (last visited Oct. 23, 2009).

374. *See, e.g.*, Tor: Anonymity Online, http://www.torproject.org (last visited Oct. 23, 2009).

375. *See, e.g.*, OpenNet Initiative, Google Search & Cache Filtering Behind China's Great Firewall (Sep. 3, 2004), http://opennet.net/bulletins/006.

enable Chinese users to breach the country's censorship, motivated partly by China's heavy filtering of Falun Gong content.[376]

Circumvention is typically praised as online civil disobedience—technological resistance to unjustified limits on information.[377] Circumvention's legitimacy, however, depends upon the filtering it subverts. Empowering Internet users to share information about democracy is inspiring; enabling users to trade child pornography is disturbing.[378] Circumvention, like filtering, cuts both ways: it permits users to bypass all content restrictions.

Like corporations offering technology to filter Internet content, entities distributing circumvention tools should evaluate a country's censorship regime before helping citizens bypass it. If a country's decision to block access to certain material is legitimate, then helping its users evade restrictions should be criticized, not celebrated. If the United States passes legislation to block children's access to sites selling controlled substances without a prescription, helping children bypass that filtering would likely be illegitimate.[379] (This assumes that the legislation is sufficiently transparent and narrow.) Thus, the Framework can serve another purpose: to guide circumvention designers and anticensorship activists as well as their opponents.

The second challenge is that the Framework's four criteria are interdependent. Accountability, for example, requires a level of free information exchange that filtering impedes. It is difficult to assess a country's censorship from within—or to criticize it—if dissenting views are blocked. In Russia, allies of the government have moved to purchase existing media outlets and create new ones,[380] enhancing

376. *See, e.g.*, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, *supra* note 214, at 15–16 (statement of Shiyu Zhou, Ph.D.), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7187 (describing FreeGate and UltraSurf programs); OPENNET INITIATIVE, supra note 13.

377. *See, e.g.*, Wiseman, *supra* note 129; Tom Zeller, Jr., *How to Outwit the World's Internet Censors*, N.Y. TIMES, Jan. 29, 2006, at C2.

378. *See* Robert Lemos, *Tor Hack Proposed to Catch Criminals*, SECURITYFOCUS, Mar. 8, 2007, http://www.securityfocus.com/news/11447.

379. *See, e.g.*, *Keep Internet Neighborhoods Safe: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 10–14 (2007) (statement of Philip Heymann, Professor, Harvard University Law School), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=2755&wit_id=6468. The author of this Article acted as a technical advisor to the Internet Drugs Expert Working Group that developed the proposal outlined by Heymann. *See* Drug Strategies, Internet Drugs: Internet Expert Panel, http://www.drugstrategies.com/internetdrugs/iep.html#1 (last visited Oct. 23, 2009).

380. Anton Troianovski & Peter Finn, *Kremlin Seeks to Extend Its Reach to Cyberspace*, WASH. POST, Oct. 28, 2007, at A1.

progovernment viewpoints, and prosecutors have begun to apply existing laws more stringently and frequently to bloggers and online critics.[381] A filtering system—even an imperfect one—can sufficiently alter the information environment such that, although censorship appears popular, accountability is significantly diminished. Narrowness also affects the other factors. Overbroad filtering could indicate incompetence, but probably means that a country is less than forthright about what material it targets, reducing transparency and openness. Thus, the four factors are not always separable; shifts in one of the factors can (and perhaps should) alter the others.

Finally, the critical test case for evaluating Internet filtering's legitimacy is almost certainly China, which poses considerable difficulties. First, Chinese citizens are divided over their government's proper role in shaping online content and the actions of American technology companies.[382] Anecdotal evidence suggests that many users hate Yahoo! and (perhaps grudgingly) like Microsoft;[383] empirical evidence from market share suggests that both play a far smaller role in China's online environment than domestic entities such as Baidu.[384] Any conclusion about how technology firms should behave in China will be contested by Chinese users, among others.

Second, companies—and perhaps even governments—have economic motivation to resolve doubts in favor of participating in China's burgeoning market. Although statistics are not entirely clear, China appears to have the most Internet users and bloggers[385] of any country—an attractive target for technology providers. Companies such as IBM have rushed to set up research labs there to tap its technological talent and to build relationships that can lead to future sales.[386] Moreover, China's censorship apparatus is itself a sales

381. *See, e.g.*, Alex Rodriguez, *Trial in Russia Sends Message to Bloggers*, CHI. TRIB., Mar. 31, 2008, at C8.

382. Fallows, *supra* note 172.

383. Thompson, *supra* note 110.

384. *See Baidu Leads China Web Search Market in Q4*, REUTERS, Jan. 25, 2008, http://www.reuters.com/article/internetNews/idUSSHA11273420080125 (listing Baidu at 60.1 percent market share, Google at 25.9 percent, and Yahoo! China at 9.6 percent).

385. Press Release, China Internet Network Info. Ctr., CNNIC Releases 2007 Survey Report on China Weblog Market (Dec. 27, 2007), *available at* http://www.cnnic.cn/html/Dir/2007/12/27/4954.htm (claiming that China has nearly 73 million blogs and 47 million bloggers).

386. *See* IBM, China Research Laboratory, http://www.research.ibm.com/beijing (last visited Oct. 23, 2009).

opportunity, as Cisco and Nortel Networks have realized.[387] Technology companies may be willing to forgo sales to Burma or Sudan for ethical reasons, but China may be too lucrative to pass up. Applying the framework to China's Internet censorship will likely produce a range of outcomes (though probably not wholehearted approval). Firms will seize on any seemingly favorable—or even neutral—assessments as justification for continued sales.

Lastly, China is probably the country where withdrawal of Western technology firms would make the least difference to filtering's success. China is developing domestic censorship technology for media from blogs to text messaging to cybercafé computers.[388] Its citizens already prefer Chinese technology providers.[389] Western firms will use this possibility to bolster their case for remaining engaged in China, even if its filtering program is deemed illegitimate. Leaving, they will argue, will at best make no difference to China's Internet users, and at worst will deprive them of services offered by companies more resistant to state demands than locally based companies.[390]

China poses difficult questions for the Framework and technology companies alike. Though most commentators have been critical of China's filtering, conclusions should flow from analysis under the Framework.[391] (Tellingly, companies such as Google and Microsoft do not defend China's actions; instead, they claim that their presence will mitigate filtering's ill effects.[392]) Even if firms decide to support China's practices despite negative assessments, that does not destroy the methodology's value. Indeed, the contrast between corporate choices and an objective, process-based evaluation would

---

387. *See* GREG WALTON, CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA 8, 14 (2001).

388. *See* OPENNET INITIATIVE, *supra* note 13; Villeneuve, *supra* note 261.

389. *See, e.g.*, *supra* note 384 and accompanying text.

390. *Cf.* Villeneuve, *supra* note 100, at 2 (noting that Google, Microsoft, and Yahoo! have all pledged to increase transparency regarding their censorship decisions but that the industry's overall transparency has declined).

391. *See, e.g.*, *Access to Information and Media Control in the People's Republic of China*, *supra* note 78; Viktor Mayer-Schonberger & Malte Ziewetz, *Jefferson Rebuffed: The United States and the Future of Internet Governance*, 8 COLUM. SCI. & TECH. L. REV. 188, 204 (2007); Palfrey & Rogoyski, *supra* note 5, at 53–65.

392. *See, e.g.*, *Gates Defends China's Internet Restrictions*, TIMES ONLINE, Jan. 27, 2006, http://technology.timesonline.co.uk/tol/news/tech_and_web/article721120.ece; McLaughlin, *supra* note 291.

provide critics with powerful ammunition. Finally, refusing to sell Western hardware, software, and services to China might diminish only slightly its censorship prowess, but inevitability does not erase agency. The question is whether it is appropriate for firms to assist China's filtering, not whether they can prevent it. Substitution is not acceptable in other contexts: North Korea will torture political dissidents with or without Western assistance, but few firms would consider it legitimate to sell its government thumbscrews.[393]

Circumvention, interdependence, and China complicate the application of the Framework, but do not diminish its utility. The Framework opens a window onto a complex problem, and it can clarify censorship's challenges.

CONCLUSION

If Internet filtering were a stock, one would be well-advised to buy it: online censorship is on the march, in democratic states as well as in authoritarian ones. In the mid-1990s, a handful of countries used technology to censor the Internet. By 2006–2007, over three dozen tested by the OpenNet Initiative did so.[394] Canada, Britain, France, and Finland already filter; Australia, Japan, and America (among others) are moving to do so. A country's mode of governance is no longer an accurate proxy for the legitimacy of its Internet restrictions. Filtering is not limited to bad actors and repressive regimes. Cybersieves are becoming commonplace.

This Article offers a new approach to evaluating Internet filtering's legitimacy by focusing on the process by which censorship decisions are made. It proposes rating countries on the openness, transparency, narrowness, and accountability of their practices. This Framework seeks to engage a range of stakeholders—from governments to activists to corporations—in assessing filtering through quantitative metrics based on its four principles. The Framework also seeks to utilize these measurements in public and private decisionmaking. Consistent, rigorous analysis that is applied

393. *See generally* U.S. DEP'T OF COMMERCE, *supra* note 311, at 9–19 (noting that the United States "has a policy of denial for any license application to export specially designed implements of torture and thumbscrews"); Press Release, U.N. Office in Belarus, Commission Adopts Measures on Situations in Cuba, Belarus, Turkmenistan, and Democratic People's Republic of Korea and Approves Special Rapporteurs for Belarus and Democratic People's Republic of Korea (Apr. 15, 2004), *available at* http://un.by/en/hr/releases/21-04-04-4.html.

394. Zittrain & Palfrey, *supra* note 11, at 2.

to all censoring countries, and that illuminates comparisons among them, will improve the quality and perception of such decisions. Filtering is increasingly normal, but it should not be seen as natural. Instead, legal scholars should examine carefully, skeptically, and thoughtfully calls to restrict access to information online.