



**From the SelectedWorks of Derek Bambauer**

---

August 2008

## Guiding the Censor's Scissors: A Framework to Assess Internet Filtering

Contact  
Author

Start Your Own  
SelectedWorks

Notify Me  
of New Work

---

Available at: [http://works.bepress.com/derek\\_bambauer/25](http://works.bepress.com/derek_bambauer/25)

# GUIDING THE CENSOR’S SCISSORS: A FRAMEWORK TO ASSESS INTERNET FILTERING

*Derek E. Bambauer*<sup>\*</sup>

Abstract .....	2
I. Introduction.....	3
II. The Internets .....	4
A. A Series of Filtered Tubes .....	4
B. Differing Norms: Challenges and Proposals .....	8
C. Application .....	12
III. A Method in Four Parts.....	14
A. Openness .....	14
B. Transparency .....	17
C. Narrowness.....	20
D. Accountability .....	25
IV. Implementation .....	35
A. Developing the Metrics .....	36
B. Alternatives .....	40
C. Using the Metrics .....	44
1. Corporate Decisions .....	44
2. Public Regulation .....	49
3. Third-Party Evaluation .....	61
4. Metrics As Guides .....	67
V. Challenges and Limitations .....	67
VI. Conclusion .....	71

---

<sup>\*</sup> Assistant Professor of Law, Brooklyn Law School. A.B, Harvard College; J.D., Harvard Law School. The author thanks Michael Abramowicz, Sarah Abramowicz, Tim Armstrong, Susan Cancelosi, Richard Clayton, Steve Davidoff, Ron Deibert, Jeff Engerman, Rob Faris, Terry Fisher, Lance Gable, Noah Hall, Peter Hammer, Gordon Hull, Orin Kerr, Gail Klavinger, Rebecca MacKinnon, Bill McGeeveran, Thinh Nguyen, John Palfrey, Joe Perry, C.J. Peters, Rafal Rohozinski, Colette Routel, Nart Villeneuve, Jonathan Weinberg, Aaron Williamson, Tim Wu, Peter Yu, Jonathan Zittrain, and the OpenNet Initiative. The 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>.

## ABSTRACT

*While 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 states' different value judgments about what content is unacceptable. States 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 various values-based perspectives, and have sporadically addressed key principles such as openness, transparency, narrowness, and accountability in evaluating this practice. This Article is the first to unite these principles into a coherent methodology that, by focusing on process, is applicable to a range of normative frameworks. Drawing upon scholarship in deliberative democracy, health policy, labor standards, and cyberlaw, the Article employs this new approach to clarify highly contentious policy debates about sales of censorship technology by Western companies, public law regulation of these transactions, and third-party analysis of states' Internet censorship.*

Word count: 28940

*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*

## I. INTRODUCTION

How can we make normative distinctions among Saudi Arabia's decision to censor Internet pornography, China's efforts to suppress political dissent on-line, and America's moves to filter out illegal MP3 files from the Web? Is it acceptable for Cisco to sell networking gear to China<sup>1</sup>, knowing it will be used to block dissident views on-line, or for Verizon to withdraw access to Usenet groups at the New York state attorney general's behest<sup>2</sup>? While 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 states try to make content disappear from the Web. Whether it's copyrighted songs in America or political dissent in Iran, the goal is the same – it is only the targeted material that varies. States differ not in their intent to limit access to material on-line, but in the content they target, the precision of their blocking, and the voice they offer citizens in decisionmaking. This Article offers a new method to measure the legitimacy of states' efforts, advancing debate about the balance between information sharing and control on the Internet, and about how that balance is struck.<sup>3</sup>

Scholars who have addressed Internet filtering have approached the issue from different values-based perspectives, variously discussing the importance of principles such as openness, transparency, narrowness in targeting content, and accountability when assessing a country's censorship. This Article, though, is the first to recognize that values-based analysis is unhelpful in a world of pervasive Internet censorship, and to offer an

---

<sup>1</sup> Sarah Lai Stirland, *Cisco Leak: "Great Firewall" of China Was a Chance to Sell More Routers*, WIRED, May 20, 2008, at <http://blog.wired.com/27bstroke6/2008/05/leaked-cisco-do.html>.

<sup>2</sup> Danny Hakim, *Web Providers to 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.COM, June 10, 2008, at [http://news.cnet.com/8301-13578\\_3-9964895-38.html](http://news.cnet.com/8301-13578_3-9964895-38.html) (quoting Time-Warner Cable and Verizon spokespeople that the service providers would block access to Usenet groups, but not Web sites).

<sup>3</sup> See John G. Palfrey, Jr., and Robert Rogoyski, *The Enduring Threat of "Harmful" Speech to the End-to-End Principle*, 21 WASH. U. J.L. & POL'Y 31 (2006).

integrated methodology that unites all of those factors into a coherent model for evaluating on-line information controls. This new methodology examines critically the processes of Internet censorship, to evaluate how well a state 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. Since on-line censorship is sharply on the rise world-wide – in democratic states<sup>4</sup> as well as authoritarian ones<sup>5</sup> – corporations, citizens, and governments will increasingly be forced to make difficult normative judgments about filtering practices<sup>6</sup>. The Article employs the proposed framework to help address such contentious debates as corporate decisions to sell censoring technology, public law regulation of such transactions, and third-party evaluations of a state's filtering.

## II. THE INTERNETS

### A. *A Series of Filtered Tubes*

There is no longer one Internet.<sup>7</sup> Pervasive censorship by countries worldwide means how the Net appears depends upon from where you access it.<sup>8</sup> In Beijing, one cannot reach sites criticizing the Chinese Communist Party or the country's human rights record.<sup>9</sup> In Mumbai, Internet Service Providers (ISPs) block the religious extremist Web site Hindu Unity.<sup>10</sup> A user searching Google for "stormfront" from a computer in Paris or Bonn will learn about the game designers, but not the white

<sup>4</sup> See, e.g., Danny O'Brien, *Turkish censor lacks others' subtle touch*, IRISH TIMES, Mar. 23, 2007, at 7 (noting Great Britain and the EU have expressed interest in blocking access to materials that glorify terrorism).

<sup>5</sup> Matthew Quirk, *The Web Police*, THE ATL. ONLINE, May 2006, at <http://www.theatlantic.com/doc/print/200605/chinese-internet>.

<sup>6</sup> See, e.g., Bruce Schneier, *Access Denied*, 452 NATURE 155 (2008); Christopher S. Rugaber, *Google Fights Internet Censorship*, WASH. POST, June 25, 2007, at [http://www.washingtonpost.com/wp-dyn/content/article/2007/06/25/AR2007062500364\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/06/25/AR2007062500364_pf.html); Kevin Voigt, *Internet censorship gathers steam*, CNN.COM, Apr. 18, 2007, at <http://edition.cnn.com/2007/BUSINESS/04/18/online.censorship/index.html>.

<sup>7</sup> See Jonathan Zittrain & John Palfrey, *Introduction*, in ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1, 2-4 (Ronald Deibert, John Palfrey, Rafal Rohozinski, & Jonathan Zittrain, eds., 2008) (hereinafter "ACCESS DENIED").

<sup>8</sup> See generally JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006).

<sup>9</sup> See, e.g., James Fallows, *The Connection Has Been Reset*, THE ATL. MONTHLY, Mar. 2008, available at <http://www.theatlantic.com/doc/200803/chinese-firewall>; U.S. DEPT. OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES – 2007: CHINA (2008), at <http://www.state.gov/g/drl/rls/hrrpt/2007/100518.htm>.

<sup>10</sup> OPENNET INITIATIVE, INDIA, at <http://opennet.net/research/profiles/india> (May 9, 2007); see Nart Villeneuve, *Evasion Tactics*, 36 INDEX ON CENSORSHIP 71 (2007).

supremacist group.<sup>11</sup> From Boston, someone looking for copyrighted music files may find them removed from search engines or host sites.<sup>12</sup> The decision to hold the 2008 Summer Olympic Games in the People's Republic of China has focused attention – and criticism – on China's on-line censorship practices<sup>13</sup> and, by extension, those of other states<sup>14</sup> such as Iran<sup>15</sup>, Syria<sup>16</sup>, Indonesia<sup>17</sup>, Japan<sup>18</sup>, Australia<sup>19</sup>, Brazil<sup>20</sup>, and even Paraguay<sup>21</sup>.

Increasingly, these nation-states deploy technology to block access to prohibited content – a practice known as Internet “filtering.”<sup>22</sup> The objective is to shape citizens' information environments and thereby alter

---

<sup>11</sup> See, e.g., Declan McCullagh, *Google excluding controversial sites*, CNET NEWS.COM, Oct. 23, 2002, at <http://www.news.com/2100-1023-963132.html>; OPENNET INITIATIVE, EUROPE, at <http://opennet.net/research/regions/europe> (last visited Aug. 18, 2008).

<sup>12</sup> 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 (2006); Google, *Digital Millennium Copyright Act*, at <http://www.google.com/dmca.html> (last visited Apr. 10, 2008).

<sup>13</sup> See, e.g., *I.O.C. Member Accuses Committee of Betrayal on Censorship Issue*, N.Y. TIMES, Aug. 1, 2008, at D7; Andrew Jacobs, *Beijing Games Denying Media Full Use of Web*, N.Y. TIMES, July 31, 2008, at A1; Edward Cody, *IOC Allows China To Limit Reporters' Access to Internet*, WASH. POST, July 31, 2008, at A10.

<sup>14</sup> See generally Anick Jesdanun, *Is It Censorship or Protection?*, WASH. POST, July 20, 2008, at A3.

<sup>15</sup> JOHN KELLY & BRUCE ETLING, *MAPPING IRAN'S ONLINE PUBLIC: POLITICS AND CULTURE IN THE PERSIAN BLOGOSPHERE* (2008), available at [http://cyber.law.harvard.edu/publications/2008/Mapping\\_Irans\\_Online\\_Public](http://cyber.law.harvard.edu/publications/2008/Mapping_Irans_Online_Public); *Iran launches fresh crackdown on websites: report*, AFP, May 20, 2008, at <http://uk.news.yahoo.com/afp/20080520/ttc-iran-rights-internet-0de2eff.html>.

<sup>16</sup> Zeina Karam, *Syria tightens controls on Internet use*, BOSTON GLOBE, Mar. 25, 2008, at [http://www.boston.com/business/technology/articles/2008/03/25/syria\\_tightens\\_controls\\_on\\_internet\\_use/](http://www.boston.com/business/technology/articles/2008/03/25/syria_tightens_controls_on_internet_use/).

<sup>17</sup> *Indonesia blocks access to YouTube over anti-Koran film*, CNET NEWS.COM, Apr. 8, 2008, at [http://www.news.com/Indonesia-blocks-access-to-YouTube-over-anti-Koran-film/2100-1028\\_3-6236929.html](http://www.news.com/Indonesia-blocks-access-to-YouTube-over-anti-Koran-film/2100-1028_3-6236929.html).

<sup>18</sup> See, e.g., *Government plans blocking of child porn sites*, DAILY YOMIURI ONLINE, May 2, 2008, at <http://www.yomiuri.co.jp/dy/national/20080502TDY01304.htm>; J. Mark Lytle, *Internet censorship body swings into action*, TECHRADAR UK, July 4, 2008, at <http://www.techradar.com/news/internet/web/internet-censorship-body-swings-into-action-415849> (describing filtering of Web sites accessible to minors via mobile phones).

<sup>19</sup> Andrew Colley, *Budget tackles online safety*, AUSTRALIAN IT, May 14, 2008, at <http://www.australianit.news.com.au/story/0,24897,23696923-15306,00.html>.

<sup>20</sup> *Google in deal with Brazil to fight child porn*, WASH. POST, July 2, 2008, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/02/AR2008070201988.html>.

<sup>21</sup> *State Telco does a DNS hijack prior elections*, SLASHDOT, Apr. 11, 2008, at <http://it.slashdot.org/firehose.pl?id=620098&op=view> (describing how state-run ADSL provider re-routed traffic seeking opposition political party Web site).

<sup>22</sup> See generally Zittrain & Palfrey, *supra* note 7 at 2 (defining “filtering”).

their behavior.<sup>23</sup> A persistent challenge for Internet law scholars has been to define a consistent, useful set of criteria to evaluate the legitimacy of such restrictions.<sup>24</sup> Past efforts have ranged from cyberlibertarianism<sup>25</sup> (arguing nothing should be blocked, and perhaps nothing can be blocked<sup>26</sup>) to U.S.-centric models (advocating filtering of “harmful” content based on American norms<sup>27</sup>) to idealistic but amorphous principles (seeking Internet-specific forms of democratic organization to resolve the question<sup>28</sup>). These approaches tend to suffer one of two flaws: treating restrictions as binary – all-pervasive censorship or an unlimited marketplace of ideas – or reifying one normative view of content as ideal – for example, banning hate speech is bad, but blocking copyright infringement is desirable. Searching for an evaluative methodology has particular salience given the surge in efforts to filter the Internet in the United States<sup>29</sup> -- for example, suggestions that ISPs should filter copyrighted material<sup>30</sup>, pornography should be segregated onto a separate “channel”<sup>31</sup>, ISPs should limit subscribers’ access to Web sites<sup>32</sup>

---

<sup>23</sup> Filtering is information regulation via code – computer hardware and software - rather than law, though its technical measures are frequently backed by legal mandates. *See generally* LAWRENCE LESSIG, *CODE 2.0* 24, 121-32 (2006).

<sup>24</sup> *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 are likely to reflect broader patterns of gender and social power)

<sup>25</sup> *See, e.g.*, JOHN PERRY BARLOW, *A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE* (1996), available at <http://homes.eff.org/~barlow/Declaration-Final.html>; but *see* Glenn H. Reynolds, *Does Power Grow Out of the Barrel of a Modem?*, 18 *STANFORD L. & POL’Y REV.* 432 (2007).

<sup>26</sup> Internet guru John Gilmore famously stated that “The Net interprets censorship as damage and routes around it.” Philip Elmer-Dewitt, *First Nation in Cyberspace*, *TIME*, Dec. 6, 1993, at 62.

<sup>27</sup> *See, e.g.*, Cheryl B. Preston, *Making Family-friendly Internet a Reality: The Internet Community Ports Act*, 2007 B.Y.U. L. REV. 1471 (2007).

<sup>28</sup> *See, e.g.*, David R. Johnson & David G. Post, *The Rise of Law in Cyberspace*, 48 *STAN. L. REV.* 1367 (1996).

<sup>29</sup> The FCC, though, has punished ISPs that unilaterally filter, voting to require Comcast not to block customers’ file-sharing traffic. *See, e.g.*, John Dunbar, *FCC Rules Against Comcast*, Aug. 2, 2008, *WASH. POST*, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080101205.html>.

<sup>30</sup> *See* Tim Wu, *Has AT&T Lost Its Mind?*, *SLATE*, Jan. 16, 2008, at <http://www.slate.com/id/2182152/>; E-mail from Neil Turkewitz, Executive Vice President, Recording Industry Association of America, to FN-USTRACTA (Mar. 17, 2008, 01:53PM), available at <http://www.publicknowledge.org/pdf/acta/riaa-20080317.pdf> (listing suggestions, including mandatory filtering by ISPs, from the Recording Industry Association of America to the U.S. Trade Representative for provisions in the Anti-Counterfeiting Trade Agreement).

<sup>31</sup> Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 B.Y.U. L. REV. 1417 (2007).

<sup>32</sup> Jasa Santos, *Qwest blocks access to known child porn sites*, *CASPER STAR-TRIBUNE*, July 7, 2008, at

or Usenet news groups (on topics from SCUBA diving<sup>33</sup> to radio astronomy<sup>34</sup>) to reduce distribution of child pornography<sup>35</sup>, and free wireless broadband providers should block material harmful to minors<sup>36</sup>.

This Article proposes an alternative, process-oriented framework to evaluate the legitimacy of Internet filtering. This approach draws upon scholarship in deliberative democracy, health care decisionmaking, labor and environmental law, and cyberlaw. The proposed framework then engages three contentious legal and ethical debates. First, how should companies based in countries with commitments to freedom of information decide when to sell goods or services that enable other states' censorship?<sup>37</sup> Second, how should governments decide whether to regulate these transactions using public law?<sup>38</sup> Finally, how can third parties such as other states, activists, and scholars evaluate countries' on-line information restrictions, such as when listing states as human rights violators?<sup>39</sup>

To assess legitimacy, the framework asks four questions. First, is a 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 filtering: how well does the content that is actually blocked - and not blocked - correspond to those criteria? Finally, to what degree are citizens and Internet users able to participate in decisionmaking about these restrictions, such that censors are *accountable*? Legitimate censorship is open; transparent about what is banned; effective, yet narrowly targeted; and responsive to the preferences of each state's citizens.

---

<http://www.trib.com/articles/2008/07/08/news/wyoming/8d7cbb0a6413fa718725747e007d4326.txt>.

<sup>33</sup> See *rec.scuba*, available at <http://groups.google.com/group/rec.scuba/topics> (last visited June 12, 2008).

<sup>34</sup> See *IAC Indian Astronomy Club*, available at <http://groups.google.com/group/indianastronomyclub?lnk=> (last visited June 12, 2008).

<sup>35</sup> McCullagh, *supra* note 2.

<sup>36</sup> In the Matter of Service Rules for Advanced Wireless Services in the 2155-2175 MHz Band & Service Rules for Advanced Wireless Services in the 1915-1920 MHz, 1995-2000 MHz, 2020-2025 MHz and 2175-2180 MHz Bands, ¶ 15 (adopted June 20, 2008) (proposed codification at 47 C.F.R. pt. 27.1193), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-08-158A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-158A1.pdf).

<sup>37</sup> See generally Jonathan Zittrain & John Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, in ACCESS DENIED 103, *supra* note 7; Center for Democracy & Technology, *Companies, Human Rights Groups, Investors, Academics and Technology Leaders to Address International Free Expression and Privacy Challenges*, at <http://www.cdt.org/press/20070118press-humanrights.php> (Jan. 18, 2007).

<sup>38</sup> See, e.g., Sarah Lai Stirland, *Ahead of Olympics, Congressman Pushes "Global Online Freedom Act,"* WIRED, Apr. 29, 2008, at <http://blog.wired.com/27bstroke6/2008/04/republican-hous.html>.

<sup>39</sup> See, e.g., U.S. DEPT. OF STATE, 2007 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES (2008), available at <http://www.state.gov/drl/rls/hrrpt/2007/>.

Evaluating legitimacy from a process-oriented perspective need not replace values-driven analysis that specifies what content is and is not suitable for blocking, and why. Indeed, the new framework bolsters such examinations. If a state's censorship is openly and fully described, carefully targeted, and responsive to popular demand, then objections to that country's filtering are properly aimed not at its on-line behavior, but at its larger shared 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 offensive.<sup>40</sup> The framework's goal is not to end analysis, and discussions based on values, but to spark and clarify them.

The remainder of Part II explains why a process-based methodology is optimal for assessing Internet censorship and lays out how that framework should be applied. Part III describes the framework's four components, with examples from countries that censor the Internet. Part IV explains how the methodology can improve decisions by companies selling filtering technology, governments contemplating regulation of these transactions, and third parties evaluating censoring states and corporations doing business with them. Part V candidly assesses the framework's challenges and limitations, and Part VI concludes with observations about the rise of filtering worldwide.

### *B. Differing Norms: Challenges and Proposals*

Countries increasingly agree that Internet users should be prevented from accessing certain content. There is scant agreement, though, on what material ought to be off-limits – when viewing should be blocked proactively rather than punished after the fact.<sup>41</sup> This divergence makes it hard to assess a filtering regime's legitimacy other than by evaluating whether the state blocks material one finds objectionable, and leaves other content accessible.<sup>42</sup>

But normative views on the acceptability of censorship vary widely; indeed, the limited restrictions on expression permitted by the American

---

<sup>40</sup> See generally HUMAN RIGHTS WATCH, SAUDI ARABIA (Jan. 2008), at <http://hrw.org/wr2k8/pdfs/saudiarabia.pdf>.

<sup>41</sup> Cf. Jack M. Balkin, Beth Simone Noveck, & Kermit Roosevelt, *Filtering the Internet: A Best Practices Model 7*, in PROTECTING OUR CHILDREN ON THE INTERNET: TOWARDS A NEW CULTURE OF RESPONSIBILITY (Jens Waltermann & Marcel Machill, eds.) (2000) (noting the “wide cultural and ideological diversity” that filtering must reflect).

<sup>42</sup> See generally Gordon Hull, *Overblocking Autonomy: The Case of Mandatory Library Filtering Software*, 41 CONTINENTAL PHILOSOPHY REV. (forthcoming 2008, copy on file with author) (describing library filtering of pornography as construction of space purged of “deviant” sexuality).

constitution are atypical in their narrow scope.<sup>43</sup> Many Americans would object to the United Arab Emirates' decision to block access to all sites hosted in Israel's top-level domain<sup>44</sup>; UAE citizens might well object to America's willingness to tolerate sites offering pornography or alcohol consumption<sup>45</sup>. Britain<sup>46</sup> and Canada<sup>47</sup> filter child pornography, and Australia has proposed doing so<sup>48</sup>, yet in Japan, possession of child pornography is lawful<sup>49</sup>. British defamation law, particularly on the Internet, prohibits considerably more speech than its counterpart American doctrine, despite their shared historical roots.<sup>50</sup> Anti-Semitic speech is permitted in Skokie but banned in Toronto.<sup>51</sup> U.S. standards themselves vary considerably by subject matter. American government officials criticize search engines when they help censor political speech in China<sup>52</sup>, and when they fail to censor copyrighted materials there<sup>53</sup>.

Even in democratic countries, the types of content restricted by law, and the standards for doing so, vary considerably. Analyzing comparative on-line censorship from one normative perspective is therefore unhelpful: countries with similar views on banning information will fare well, and contrary attitudes poorly. We tend to approve of like-minded thinkers. Restricting information on-line is thus a policy question about choosing

---

<sup>43</sup> See, e.g., Frederick Schauer, *The Exceptional First Amendment*, Faculty Research Working Paper Series, John F. Kennedy School of Government, July 18, 2004, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract-id=668543>; Adam Liptak, *Unlike Others, U.S. Defends Freedom to Offend in Speech*, N.Y. TIMES, June 12, 2008, at A1.

<sup>44</sup> OPENNET INITIATIVE, UNITED ARAB EMIRATES, at <http://opennet.net/research/profiles/uae> (documenting filtering of all sites in .il top-level domain) (May 9, 2007).

<sup>45</sup> *Id.*

<sup>46</sup> Martin Bright, *BT puts block on child porn sites*, THE OBSERVER, June 6, 2004, at 7.

<sup>47</sup> Cybertip.ca, *Cleanfeed*, at <http://cybertip.ca/app/en/cleanfeed> (stating Canada's Cleanfeed system blocks "access to Internet addresses specifically containing child pornography images").

<sup>48</sup> Karen Deane & Fran Foo, *Conroy wades into child porn net flood*, AUSTRALIAN IT, Jan. 8, 2008, at <http://www.australianit.news.com.au/story/0,24897,23021645-15306,00.html>.

<sup>49</sup> Jake Adelstein, *This Mob Is Big in Japan*, WASH. POST, May 11, 2008, at B2 (noting Japan's Internet Hotline Center found over 500 sites hosted in the country displaying child pornography in 2007, and that bans on producing or distributing child pornography are rarely enforced).

<sup>50</sup> See, e.g., *Demon v. Godfrey Internet Ltd.*, [2001] Q.B. 201; *Harrods Ltd. V. Dow Jones & Co.*, [2003] EWHC 1162 (QB).

<sup>51</sup> *Compare Nat'l Socialist Party of Am. v. Village of Skokie*, 432 U.S. 43 (1978), with *Can. (Human Rights Comm'n) v. Taylor*, [1990] 3 S.C.R. 892 (Can.).

<sup>52</sup> See, e.g., *Yahoo! Criticized in Case of Jailed Dissident*, N.Y. TIMES, Nov. 7, 2007, at C3.

<sup>53</sup> OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2008 SPECIAL 301 REPORT 7, available at [http://ustr.gov/assets/Document\\_Library/Reports\\_Publications/2008/2008\\_Special\\_301\\_Report/asset\\_upload\\_file553\\_14869.pdf](http://ustr.gov/assets/Document_Library/Reports_Publications/2008/2008_Special_301_Report/asset_upload_file553_14869.pdf) (criticizing Chinese search engine Baidu for "offering deep links to copyright-protected music files for unauthorized downloads").

among the multiple regulatory endpoints that are possible, and legitimate.<sup>54</sup> (Consider the American debate over whether pornography should be banned, for example.<sup>55</sup>) Thus, to assess whether a given approach to censorship is legitimate, we need an analytical tool that recognizes different possible tradeoffs while enabling comparative analysis with maximum rigor.

Rather than endorse a particular position on prohibited and permissible content, this Article offers a process-based methodology that provides rigor, focuses attention on censorship's effects, and enables application of different normative models.<sup>56</sup> The virtue of this framework is to force states to describe their reasons for censoring information (or to reveal their rationales as opaque), to evaluate the basis for their decisions, and to test how well they implement those choices. This method concentrates attention on the hard choices behind decisions to restrict access to information, forcing countries to defend their positions.

This methodology parallels proposals based on deliberative democracy models in other highly contested policy areas.<sup>57</sup> Similar process-based approaches have been deployed in other settings where multiple legitimate outcomes are possible, and even likely, such as allocating health care and regulating working conditions. Consider first a dying patient in the U.S. who wants her health care plan to pay for experimental treatment.<sup>58</sup> (Assume that the treatment may have clinical benefit, but has not been proven effective.) The plan and the patient have different, competing value sets. The plan seeks to ensure all its members have access to scarce medical resources, to discover new therapies through clinical trials, and to avoid negative public attention. The patient wants to receive therapy that may extend her life, improve its quality, or cure her disease. There is no single way to balance these competing claims; it may be reasonable to provide coverage to women with breast cancer for autologous bone marrow

---

<sup>54</sup> I thank Peter Hammer for this point.

<sup>55</sup> *Compare Erznoznik v. Jacksonville*, 422 U.S. 205 (1975) (holding unconstitutional ban on drive-in movie theaters showing films with nudity), and *Am. Booksellers Ass'n v. Hudnut*, 771 F.2d 323 (7<sup>th</sup> Cir. 1985), *aff'd mem.*, 475 U.S. 1001 (1986) (invalidating anti-pornography ordinance), with Catherine A. MacKinnon, *Pornography as Defamation and Discrimination*, 71 B.U. L. REV. 793 (1981) and Cass Sunstein, *Pornography and the First Amendment*, 1986 DUKE L.J. 589 (1986).

<sup>56</sup> Jack Balkin, Beth Noveck, and Kermit Roosevelt propose an analogous method for rating Web sites' content via application of different "templates" developed by third parties. See Balkin, Noveck, & Roosevelt, *supra* note 41, at 9.

<sup>57</sup> See generally JAMES FISHKIN, *DEMOCRACY AND DELIBERATION* (1991); *DELIBERATIVE DEMOCRACY AND HUMAN RIGHTS* (Harold Honju Koh & Ronald C. Slye, eds.) (1999).

<sup>58</sup> See Norman Daniels & James E. Sabin, *Last Chance Therapies and Managed Care*, 28 HASTINGS CENTER REPORT 27 (1998).

transplants<sup>59</sup>, but to deny access to experimental cancer drugs (which may be highly toxic)<sup>60</sup>. For the health plan, the key is to arrive at outcomes that seem legitimate to affected patients, other members, and the public.

Norman Daniels and James Sabin suggest the keys to such legitimacy are process-oriented: making decisions public; explaining how decisions reasonably address the challenge of providing benefits to a heterogeneous group of members given resource constraints; allowing appeal; and creating regulation to enforce these factors.<sup>61</sup> They 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 to allocating limited materials and services.<sup>62</sup> Patients or health plan accountants may disagree with the outcome of a particular dispute under such a process – indeed, given their differing preferences and values, one side is likely to do so – but they are more likely to accept its legitimacy if they trust how the decision was made.<sup>63</sup> As with censorship, allocating health care resources (whether through public or private choice<sup>64</sup>) 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 by stakeholders.

Similarly, setting labor standards can result in multiple legitimate outcomes – though ones that prioritize different interests and values. Under pressure from activists and other monitors, corporations have begun to adopt voluntary codes of conduct for working conditions.<sup>65</sup> These codes, while arguably oriented around principles elucidated by the International Labour Organization, differ significantly in the requirements they establish

---

<sup>59</sup> *But see* Peter D. Jacobson, Richard A. Rettig, & Wade M. Aubry, *Litigating the Science of Breast Cancer Treatment*, 32 J. HEALTH POLITICS, POLICY & LAW 785, 790 (2007) (noting randomized clinical trials showed transplants to be no more effective than standard chemotherapy).

<sup>60</sup> *Cf. Abigail Alliance for Better Access to Developmental Drugs v. Eschenbach*, 485 F.3d 695, (D.C. Cir. 2007), *cert. denied*, 128 S. Ct. 1069 (2008) (finding no constitutional right to access experimental therapies).

<sup>61</sup> Daniels & Sabin, *supra* note 58.

<sup>62</sup> Norman Daniels & James Sabin, *The Ethics of Accountability in Managed Care Reform*, 17 HEALTH AFFAIRS 50, 57 (1998).

<sup>63</sup> *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”).

<sup>64</sup> *Id.* at 61, 63.

<sup>65</sup> *See generally* Richard Locke, Thomas Kochan, Monica Romis, & Fei Qin, *Beyond corporate codes of conduct: Work organization and labour standards at Nike's suppliers*, 146 INT'L LABOR REV. 21, 22-24 (2007).

for issues such as wages, non-discrimination, and freedom of association.<sup>66</sup> Should factories pay workers (at least) the legal minimum wage in a country, or a “living” wage?<sup>67</sup> Can they discriminate in employment based on sexual orientation? (American federal employment law permits such discrimination<sup>68</sup>; French employment law bans it<sup>69</sup>.) While most participants agree that labor regulation is needed, they diverge about what content and 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 or The Gap comply with their adopted code of conduct.<sup>70</sup> Companies select both the standards by which they are measured (the code of conduct) and the evaluator (the monitoring entity). 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 for one in Vienna.<sup>71</sup> Rather than analyzing labor standards from a single value-based perspective, the RLS proposal focuses on process: self-regulation, checked by monitoring and disclosure, with feedback to refine standards and develop legitimacy.

Regulation becomes even more challenging when it is path-dependent: the rules’ value depends upon the norms that underlie them, and there are multiple sets of 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 validity through rigorous, inclusive process.

### *C. Application*

A process-driven methodology can help answer questions of legitimacy in three policy arenas related to Internet censorship: corporate transactions that supply states with filtering technology; public policy

---

<sup>66</sup> Dara O’Rourke, *Outsourcing Regulation: Analyzing Nongovernmental Systems of Labor Standards and Monitoring*, 31 POL’Y STUDIES J. 1, 7-9 (2003).

<sup>67</sup> *Id.* at 9 (comparing different codes of conduct).

<sup>68</sup> See, e.g., James E. Snyder & Reva S. Bauch, *Sexual Orientation Discrimination in the Workplace*, 20 CHI. BAR ASS’N RECORD 44, 45.

<sup>69</sup> Julie Chi-Hye Suk, *Equal by Comparison: Unsettling Assumptions of Antidiscrimination Law*, 55 AM. J. COMP. L. 295, 302-03 (2007).

<sup>70</sup> Archon Fung, Dara O’Rourke, & Charles Sabel, *Realizing Labor Standards*, 26 BOSTON REVIEW (2001), at <http://bostonreview.net/BR26.1/fung.html>; see Archon Fung, *Deliberative Democracy and International Labor Standards*, 16 GOVERNANCE 51, 54-57 (2003).

<sup>71</sup> *Id.*

choices treating those sales; and third-party analysis of those states' practices. Country ratings could aid corporations in selecting with which states to transact business, and under what terms.<sup>72</sup> Corporations increasingly find supplying dual-use technologies – or even those overtly designed for censorship – to filtering countries to be a profitable endeavor.<sup>73</sup> Yet when the same code blocks drive-by downloads and democracy sites<sup>74</sup>, how should corporations evaluate which transactions are acceptable, and how should their critics assess those choices? The metrics could serve not just to decide what deals to accept, but also to defend them publicly. Over time, governments could examine the pattern of corporate behavior to decide whether public regulation of filtering technology is necessary, or whether private decisions (cabined by public scrutiny) appropriately ration assistance to censoring countries. Similarly, activists and other commentators could employ ratings to increase the rigor and improve the utility of their analyses of state-based censorship. The new methodology will helpfully clarify multiple legal and policy questions.

Ultimately, decisions about information control on-line are important because they guide the choices we make, and the consequences that result. China's citizens demonstrate against Japan because they are offended by that country's actions in the Second World War; they typically do not know Japan has apologized repeatedly for its conduct because China's government blocks access to those facts.<sup>75</sup> We are creatures of our information environments. To influence citizens' decisions, a state need not achieve perfect control.<sup>76</sup> When a state can affect the average Internet user's typical experience, it has achieved a level of control that is powerful and that should be scrutinized.

Many states, democratic and authoritarian alike, are implementing Internet censorship. They vary not in intent, but in how forthright they are about such restrictions, how carefully they block content, and what role citizens play in policy decisions. The next section describes the four parts of this Article's new, process-based method to evaluate on-line filtering.

---

<sup>72</sup> See, e.g., David Bandurski, *Pulling the Strings of China's Internet*, 171 FAR E. ECON. REV. 18 (Dec. 2007) (describing participation of Western technology companies, including Intel, Yahoo!, and Nokia, in a trade group in China that coordinates Internet censorship).

<sup>73</sup> Derek E. Bambauer, *Cool Tools for Tyrants*, LEGAL AFF., Jan./Feb. 2006, at [http://www.legalaffairs.org/issues/January-February-2006/feature\\_bambauer\\_janfeb06.msp](http://www.legalaffairs.org/issues/January-February-2006/feature_bambauer_janfeb06.msp).

<sup>74</sup> Nart Villeneuve, *Censorship Is In the Router*, at <http://www.nartv.org/2005/06/03/censorship-is-in-the-router/> (June 3, 2005); see generally Nart Villeneuve, *The Filtering Matrix*, FIRST MONDAY, Jan. 2, 2006, at <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227>.

<sup>75</sup> Mark Magnier, *Letting Passions Burn May Backfire on China*, L.A. TIMES, Apr. 25, 2005, at A1; Jonathan Watts, *Violence flares as the Chinese rage at Japan*, THE OBSERVER, Apr. 17, 2005, at 20.

<sup>76</sup> See generally Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

### III. A METHOD IN FOUR PARTS

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

#### *A. Openness*

The first criterion for analyzing information restrictions on-line is openness: does the state admit to filtering the Internet and describe clearly its rationale for blocking? Filtering 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.

For example, compare Saudi Arabia and China. Saudi Arabia prevents users from accessing most pornographic and erotic material, along with some pages on certain sects of Islam, other minority faiths, and alcohol and illegal drugs.<sup>77</sup> The Kingdom is open about censorship; its Internet Services Unit (ISU) explains the filtering on its Web site.<sup>78</sup> The ISU justifies these practices by citing supporting materials that discuss the social harms from pornography, such as the Koran, an article on Internet pornography written by Cass Sunstein, the 1986 Attorney General's Commission on Pornography, and a study from the University of New Hampshire.<sup>79</sup> 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

---

<sup>77</sup> See OPENNET INITIATIVE, SAUDI ARABIA, at <http://opennet.net/research/profiles/saudi-arabia> (May 10, 2007).

<sup>78</sup> Internet Services Unit, King Abdulaziz City for Science & Technology, *Local Content Filtering policy*, at <http://www.isu.net.sa/saudi-internet/content-filtrng/filtrng-policy.htm> (last visited March 4, 2008).

<sup>79</sup> Internet Services Unit, King Abdulaziz City for Science & Technology, *Introduction to Content Filtering*, at <http://www.isu.net.sa/saudi-internet/content-filtrng/filtrng.htm> (last visited March 4, 2008). While the ISU does not specify which UNH study it cites, the University's Crimes Against Children Research Center has published numerous papers on Internet issues, at <http://www.unh.edu/ccrc/internet-crimes/papers.html>.

“contrary to the state or its system.”<sup>80</sup> Finally, users who attempt to reach a filtered site receive a “block page” to inform them that the disruption is deliberate.<sup>81</sup> Saudi Arabia thus discloses the existence of its on-line censorship regime and elucidates its rationales for preventing access to certain information.

China, by contrast, operates the world’s most extensive and sophisticated Internet censorship system, yet admits but rarely that the state filters information.<sup>82</sup> The Chinese filtering apparatus is multi-layered. Prohibited content can be blocked by the network backbone, ISPs, Internet café computers, e-mail servers, blog hosting services, search engines, and even personnel dedicated to detecting and removing such material as it is posted.<sup>83</sup> Users are not informed when they are prevented from reaching proscribed material; instead, their Internet connections are re-set, or their e-mail messages never reach their destinations.<sup>84</sup> Intentional censorship is difficult or impossible to distinguish from transient technical errors. Queries for sensitive terms, such as “Falun Gong” or “Taiwan,” on Chinese search engines such as Google’s or Baidu generate results that deliberately purge blocked sites.<sup>85</sup> (Google notifies users that it censors search results; interestingly, Baidu has begun notification as well, even though it is based

---

<sup>80</sup> See OPENNET INITIATIVE, *Banned Content*, in INTERNET FILTERING IN SAUDI ARABIA IN 2004 (2004), available at <http://opennet.net/studies/saudi/#toc2c>.

<sup>81</sup> See Internet@sa, *New block page*, at [http://www.internet.gov.sa/news/new-block-page/view?set\\_language=en](http://www.internet.gov.sa/news/new-block-page/view?set_language=en) (last visited March 4, 2008); see also Nart Villeneuve, *Saudi*, at [http://blockpage.com/main.php?g2\\_itemId=44](http://blockpage.com/main.php?g2_itemId=44) (last updated August 2, 2007) (displaying block page Saudi users receive when attempting to access filtered site); see generally Alfred Hermida, *Saudis block 2,000 websites*, BBC NEWS, July 31, 2002, at <http://news.bbc.co.uk/2/hi/technology/2153312.stm> (describing initial empirical testing of Saudi Arabia’s filtering and use of block pages).

<sup>82</sup> See, e.g., Declan McCullagh, *China: We don’t censor the Internet. Really*, CNET NEWS.COM, Oct. 31, 2006, at [http://news.cnet.com/China-We-dont-censor-the-Internet.-Really/2100-1028\\_3-6130970.html?hhTest=1](http://news.cnet.com/China-We-dont-censor-the-Internet.-Really/2100-1028_3-6130970.html?hhTest=1) (quoting Chinese government official that “In China, we don’t have software blocking Internet sites... We do not have restrictions at all”); Written Statement of Ronald J. Deibert, Testimony before the U.S.-China Security & Economic Review Commission, available at <http://deibert.citizenlab.org/deibertcongresstestimony.pdf> (June 18, 2008) (stating “official acknowledgement of these practices has been inconsistent at best, deceitful at worst”); see generally OPENNET INITIATIVE, CHINA, at <http://opennet.net/research/profiles/china> (May 9, 2007); Carolyn Duffy Marsan, *Chinese Internet censorship: An inside look*, NETWORK WORLD, May 12, 2008, at <http://www.networkworld.com/news/2008/051208-china-internet.html> (interviewing researcher James Fallows, who states few Chinese Internet users are aware of filtering, and the “government discourages upfront discussion of the Great Firewall’s existence”).

<sup>83</sup> OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004-2005: A COUNTRY STUDY (Apr. 2005), at <http://opennet.net/studies/china>.

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

in China.<sup>86</sup>) Even users who are aware, generally, 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 state; formally, they have no reason to be wary, since China does not usually admit to filtering.

Yet openness is easy to achieve. Nearly all filtering technology allows a state to display a block page when a user is prevented from accessing banned material.<sup>87</sup> The page, which can be customized, informs the user that her inability to retrieve a Web site is a deliberate policy choice rather than a technical error.<sup>88</sup> It is easy and inexpensive to be open about filtering. States that nonetheless obfuscate their censorship – such as Uzbekistan, which redirects users from banned sites to an innocuous third-party site – seek to conceal from users that they restrict on-line material.<sup>89</sup>

The openness criterion rests on two assumptions: first, that to act legitimately, a government must seek to advance the interests of its citizens; and second, that legitimacy requires a government to disclose to those it purports to benefit that it is so acting. At a sufficiently specific level, these assumptions may weaken – it might be counterproductive for a state to disclose it was blocking access to extremely harmful material at a specified location, thereby inviting circumvention attempts<sup>90</sup> – but generally, the more forthright a state is about its censorship, the more likely its restrictions are legitimate.

This is particularly true for restricting Internet information. Governments generally advance two reasons for censoring the Net. First, the banned content harms the community, regardless of any benefit for the individual reader. Thus, Singapore bans (at least symbolically) “material that is objectionable on the grounds of public interest, public morality, public order, public security, [and] national harmony.”<sup>91</sup> Prohibitions on hate speech function similarly – discrimination pleases the bigot, but harms his neighbors. Second, the filtered material harms the individual, who may

---

<sup>86</sup> Nart Villeneuve, *Perspectives on Transparency*, at

<http://www.nartv.org/2008/06/26/perspectives-on-transparency/> (June 26, 2008).

<sup>87</sup> See, e.g., Cisco Systems, *Cisco Security Appliance Command Line Configuration Guide, Version 7.2 – Configuring HTTP Filtering*, at

<http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/filter.html#wp1042538> (last visited June 29, 2008).

<sup>88</sup> See *Gallery*, at <http://blockpage.com/main.php> (displaying images of block pages from various countries and filtering systems) (last updated June 4, 2008).

<sup>89</sup> Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, in ACCESS DENIED 5, 13, *supra* note 7 (documenting redirection to live.com).

<sup>90</sup> See *infra* notes 417–426 and accompanying text.

<sup>91</sup> SINGAPORE MEDIA DEVELOPMENT AUTHORITY, INTERNET CODE OF PRACTICE § 4(1), available at

[http://www.mda.gov.sg/wms.file/mobj/mobj.981.internet\\_code\\_of\\_practice.pdf](http://www.mda.gov.sg/wms.file/mobj/mobj.981.internet_code_of_practice.pdf).

not realize the danger or who may find it attractive despite the risk. Vietnam, for example, claims its censorship “policy is to apply measures to prevent youngsters from unhealthy sites.”<sup>92</sup> Neither rationale is strengthened by undisclosed restrictions – rather, notice that the state blocks access reinforces the material’s harmfulness and the societal judgment that it deserves to be proscribed. In short, states confident that their censorship advances their citizens’ welfare have no cause to hide their actions. Those that disclose their restrictions are more likely to engage in legitimate controls rather than ones designed for the protection of the governing, not the governed.

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

### *B. Transparency*

The second criterion is transparency: is the censoring state clear about what material is filtered, and is it specific about the criteria that determine blocking? Transparent categories and criteria allow users to assess how the list of banned content maps to the rationales for information control advanced by that state (evaluated under openness above). A country that filters the Internet to prevent harm to minors, for example, could plausibly censor Web sites offering medication without a prescription<sup>93</sup>, violent games<sup>94</sup>, or encouragement for anorexia<sup>95</sup>. A system targeting sexually explicit material could potentially block sites ranging from pornography to lingerie catalogs to sex education. Thailand censors some pornography<sup>96</sup>; Iran blocks provocative attire sites along with pornography (with greater success than any other country)<sup>97</sup>; Saudi Arabia filters family

---

<sup>92</sup> See, e.g., *Politics a no-no but porn OK*, THE AUSTRALIAN, Aug. 15, 2006, at 33 (quoting Vietnamese Foreign Ministry spokesperson Le Dung).

<sup>93</sup> Cf. Erik Eckholm, *Abuses Are Found in Online Sales of Medication*, N.Y. TIMES, July 9, 2008, at A21 (citing study showing 85% of Internet sites selling controlled substances did not require a prescription).

<sup>94</sup> Cf. COMMISSION OF THE EUROPEAN COMMUNITIES, COMMUNICATION FROM THE COMMISSION ON THE PROTECTION OF CONSUMERS, IN PARTICULAR MINORS, IN RESPECT OF THE USE OF VIDEO GAMES, COM(2008) 207 final (Apr. 22, 2008), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0207:FIN:EN:PDF>.

<sup>95</sup> Thomas Catan, *Online anorexia sites shut down amid claims they glorify starvation*, TIMES ONLINE, Nov. 22, 2007, at [http://www.timesonline.co.uk/tol/life\\_and\\_style/health/article2916356.ece](http://www.timesonline.co.uk/tol/life_and_style/health/article2916356.ece) (documenting action by Microsoft after complaint by Spanish Internet watchdog organization); Doreen Carvajal, *France acts to outlaw anorexia Web sites*, INT’L HERALD TRIBUNE, Apr. 15, 2008, at <http://www.iht.com/articles/2008/04/15/europe/paris.php>.

<sup>96</sup> OPENNET INITIATIVE, THAILAND, at <http://opennet.net/research/profiles/thailand> (May 9, 2007).

<sup>97</sup> OPENNET INITIATIVE, IRAN, at <http://opennet.net/research/profiles/iran> (May 9, 2007).

planning sites as well<sup>98</sup>. Rationales are general. Transparency presses a state to go beyond the reasons for filtering and to explain precisely which content runs counter to its goals.

Disclosure also forces a government to go on record with the types of content it purports to block; testing (covered in the next section, under narrowness) reveals how accurate those statements are. Transparency extends the analysis begun under openness. A state could be open about filtering without being transparent: Tunisia requires ISPs to block information “likely to upset public order”<sup>99</sup> and to prohibit “information contrary to public order and good morals,”<sup>100</sup> but disguises its actual Internet censorship.<sup>101</sup> It is also possible to have some transparency without openness: China hedges about whether it filters, but some domestic search engines, such as Baidu and Soso, disclose to users when they censor query results.<sup>102</sup> Yahoo!’s Chinese search engine also engages in selective transparency: it lists sites censored for copyright violations<sup>103</sup>, but not for political or other reasons<sup>104</sup>. The openness test assesses whether a state discloses *why* it censors. The transparency prong evaluates whether it describes *what* it censors.

States can disclose what material they block either formally – such as through codification in press regulations<sup>105</sup> – or informally – such as in statements by government officials<sup>106</sup>. Formal criteria are more transparent; citizens have greater access to documented rules than to verbal utterances. Clarity in blocking disclosure varies greatly. France, for example, requires

---

<sup>98</sup> OPENNET INITIATIVE, *supra* note 77.

<sup>99</sup> 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); *see* OPENNET INITIATIVE, TUNISIA, at <http://opennet.net/research/profiles/tunisia> (May 9, 2007).

<sup>100</sup> *Id.* (citing Art. 49, DECREE OF THE MINISTRY OF TELECOMMUNICATIONS OF MARCH 22, 1997 (translated by Harvard Law School Langdell Library)).

<sup>101</sup> Tunisia displays a 404 Not Found error page (stating that the site does not exist or cannot be found) rather than the 403 Forbidden page (indicating the user has been prevented from reaching the requested site). *See* Nart Villeneuve, *Tunisia: Internet Filtering*, at <http://www.nartv.org/2005/06/07/tunisia-internet-filtering/> (June 7, 2005); OPENNET INITIATIVE, *supra* note 99.

<sup>102</sup> Villeneuve, *supra* note 86 (suggesting Western search engines such as Google have established a norm of transparency for such filtering).

<sup>103</sup> Available at [search.help.cn.yahoo.com/h3\\_9.html](http://search.help.cn.yahoo.com/h3_9.html).

<sup>104</sup> *See generally* NART VILLENEUVE, SEARCH MONITOR PROJECT: TOWARD A MEASURE OF TRANSPARENCY 5-7 (2008), available at <http://www.citizenlab.org/papers/searchmonitor.pdf>.

<sup>105</sup> Iran’s Press Law of 2000, for example, prohibits insulting Islam, attacking the Leader of the Iranian Revolution, or quoting articles from groups that oppose Islam. OPENNET INITIATIVE, *supra* note 97.

<sup>106</sup> *See supra* note 92 and accompanying text.

filtering of hate speech<sup>107</sup>, which is well-defined under its civil and criminal laws as that which targets a person or group based on their origin, belonging to, or not belonging to an ethnic group, nation, race, or religion.<sup>108</sup> China, by contrast, is vague about the material it filters, typically describing it as “unhealthy,”<sup>109</sup> “spread[ing] rumors,”<sup>110</sup> “destroy[ing] national unity,”<sup>111</sup> or even just not “wholesome.”<sup>112</sup> Moreover, China’s formal regulation of Internet content comprises a morass of statutes, regulations, and decrees from at least a dozen different government entities.<sup>113</sup> This complicates the task of a user or creator who wants to determine what content is subject to filtering. China’s opacity is deliberate: it presses on-line service providers such as Google and Sina to censor widely, as the risk of erroneously allowing access to prohibited material can include loss of an operating license or even potential criminal sanctions.<sup>114</sup> It is thus more difficult to assess what types of content are filtered, or at least subject to blocking, in China than in France. France’s censorship is more transparent.

In addition to disclosing what content is filtered, states vary in how clearly they describe the criteria for determining whether material is permitted or proscribed. More precise definitions enhance transparency. For example, blocking “child pornography,”<sup>115</sup> where that material is defined carefully in a state’s criminal code<sup>116</sup>, is more transparent than banning “nudity,”<sup>117</sup> when that content includes pornographic images, pictures of Michaelangelo’s statue of David, and photos of prisoner abuse at the Abu

---

<sup>107</sup> OPENNET INITIATIVE, EUROPE, *supra* note 11. See generally *LICRA v. Yahoo!, Inc.*, No. RG 00/05308 (T.G.I. de Paris 2000) (requiring Yahoo!’s French subsidiary to disable access to auctions of Nazi memorabilia), *available at*

<http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf>.

<sup>108</sup> Arts. 23 & 24, Law on Press Freedom, J.O., July 29, 1881, p.4202, *available at* [http://www.lexinter.net/lois/provocation\\_aux\\_crimes\\_et\\_delits.htm](http://www.lexinter.net/lois/provocation_aux_crimes_et_delits.htm) (translation by author) (copy on file with author).

<sup>109</sup> Blanchard, *supra* note 13 (quoting Technology Minister Wan Gang).

<sup>110</sup> Mark O’Neill, *Beijing closes net around Web sites*, S. CHINA MORNING POST, Oct. 4, 2000, at 10.

<sup>111</sup> *Id.*

<sup>112</sup> Marsan, *supra* note 82.

<sup>113</sup> OPENNET INITIATIVE, *supra* note 83, at <http://opennet.net/studies/china#app2>; Congressional-Executive Commission on China, *Agencies Responsible for Censorship in China*, at <http://www.cecc.gov/pages/virtualAcad/exp/expcensors.php> (last modified Apr. 5, 2006); Melinda Liu, *Big Brother Is Talking*, NEWSWEEK, Oct. 17, 2005, at 20 (estimating 38 different regulations governing the Internet in China).

<sup>114</sup> See, e.g., Clive Thompson, *Google’s China Problem (And China’s Google Problem)*, N.Y. TIMES MAGAZINE, Apr. 23, 2006, at 64.

<sup>115</sup> See, e.g., Cybertip.ca, *supra* note 47.

<sup>116</sup> CRIMINAL CODE § 163.1(1) (Ca.) (defining “child pornography”).

<sup>117</sup> See Secure Computing, *SmartFilter Database*, at <http://www.securecomputing.com/index.cfm?sk=86#categories> (defining nudity as “nonpornographic images of the bare human body”) (last visited June 10, 2008).

Ghraib facility in Iraq<sup>118</sup>. The clearer and more precise the criteria, the less discretion government officials or ISPs have to define other sites as falling within the proscribed zone. Uzbekistan's Law on Principles and Guarantees on Access to Information, for example, permits restricting information "in the name of maintaining safety and protecting the moral values of society" – a term that offers cover for governmental censorship of opposition political sites and coverage critical of the state's authoritarian regime.<sup>119</sup> 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 censorship that the state wishes to keep covert.

In sum, the transparency analysis 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 upon them. A transparent censorship regime specifies both the categories of content that can be banned and the rules for determining whether material falls within those categories. Overall, the transparency and openness prongs map the scope of a sovereign's public claims about its information control.

### *C. Narrowness*

The third criterion is narrowness: how closely does the empirical data about what a state actually blocks match that country's description of its censorship practices? This test validates the claims a state makes (if any) about its filtering through testing. Openness and transparency assess what a country claims about its censorship; narrowness examines what it does.

Narrowness considers both overinclusiveness and underinclusiveness. Most, if not all, Internet filtering systems will be overbroad (blocking content beyond that which is overtly targeted), underbroad (failing to block proscribed material), or both. Both overinclusion and underinclusion are problematic. Overbroad filtering keeps citizens from accessing material that isn't defined as harmful or forbidden. Underbroad blocking means the state fails to censor content it views as dangerous.

---

<sup>118</sup> See, e.g., Xeni Jardin, *BoingBoing banned in UAE, Qatar, elsewhere*, at <http://www.boingboing.net/2006/02/27/boingboing-banned-in.html> (Feb. 27, 2006) (describing blocking of the popular blog BoingBoing based on its classification by the filtering software SmartFilter as "nudity" even though less than one percent of posts have photos with nudity).

<sup>119</sup> Inera Safargalieva, *Uzbek Media and the Authorities – A Strange Relationship*, in OSCE REPRESENTATIVE ON FREEDOM OF THE MEDIA, CENTRAL ASIA – IN DEFENSE OF THE FUTURE 259, 263 (2003), available at [http://www.osce.org/publications/rfm/2004/02/12243\\_101\\_en.pdf](http://www.osce.org/publications/rfm/2004/02/12243_101_en.pdf).

Overinclusive censorship can be deliberate or inadvertent. Vietnam, for example, claims only to filter Web pages that are pornographic or otherwise socially harmful to minors, yet its system concentrates on ensuring that political opposition and reform sites remain inaccessible.<sup>120</sup> This is a deliberate strategy to protect the state's single-party Communist system.<sup>121</sup> Overbreadth may also represent a deliberate policy choice to tolerate false positive results (filtering innocent content) to minimize false negative results (failing to block proscribed material). Inadvertent filtering can result from classification errors, such as when Secure Computing's SmartFilter software categorized a small-town Kentucky newspaper as a pornographic site<sup>122</sup>, or from crude censorship techniques that block an entire Web site or domain containing a few suspect pages, such as when ISPs prevented access to over a million unrelated Web sites to filter 400 with child pornography, at the behest of a Pennsylvania statute<sup>123</sup>.

Underinclusive censorship occurs when users can reach content that the state seeks to block. (This differs from users who reach blocked content via circumvention techniques that deliberately evade filtering.<sup>124</sup>) Singapore operates an underinclusive filtering system by design; though all pornography is eligible for blocking, only a few sites are targeted, as a symbolic stand.<sup>125</sup>

States can have both overbroad and underbroad censorship. Vietnam's filtering system is underinclusive, as well as overinclusive: it fails to block access to any pornographic sites, though the state claims that doing so is vital to social well-being.<sup>126</sup> However, the state heavily censors political sites. Such filtering makes both types of errors, preventing access to material that is technically licit (though perhaps practically prohibited), while still permitting access to content that is theoretically damaging enough to censor.

---

<sup>120</sup> OPENNET INITIATIVE, VIETNAM, at <http://opennet.net/research/profiles/vietnam> (May 9, 2007).

<sup>121</sup> U.S. DEPARTMENT OF STATE, VIETNAM: COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES - 2007 (2008), at <http://www.state.gov/g/drl/rls/hrrpt/2007/100543.htm>.

<sup>122</sup> OPENNET INITIATIVE, INTERNET FILTERING IN THE UNITED ARAB EMIRATES IN 2004-2005: A COUNTRY STUDY n.50, available at <http://opennet.net/studies/uae/#50>.

<sup>123</sup> See, e.g., *Center for Dem. & Tech. v. Pappert*, 337 F. Supp. 2d 606, 633-34, 650-52 (E.D. Pa. 2004).

<sup>124</sup> See generally Nart Villeneuve, *Choosing Circumvention: 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](http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf); see generally Hiawatha Bray, *Beating Censorship on the Internet*, BOSTON GLOBE, Feb. 20, 2006, at A10.

<sup>125</sup> OPENNET INITIATIVE, SINGAPORE, at <http://opennet.net/research/profiles/singapore> (May 10, 2007) (finding Singapore blocks only seven high-profile pornographic sites).

<sup>126</sup> OPENNET INITIATIVE, *supra* note 120; see *supra* note 92 and accompanying text.

Commentary on filtering tends to ignore underinclusion. However, underbroad censorship causes concern for three reasons. First, assuming a state adequately justifies blocking access to harmful content, allowing users to view that material is socially undesirable. In 2006, for example, British Telecom detected 35,000 attempts per day to access child pornography.<sup>127</sup> However, until the end of 2007, only BT blocked such attempts.<sup>128</sup> If Great Britain defined child pornography as harmful enough to be censored, then allowing users to view this material because of underinclusive blocking (here, due to different practices by ISPs) is normatively problematic.<sup>129</sup> If the decision to censor material on-line is adequately justified, a state with underinclusive filtering is failing to prevent harm it formally seeks to cabin.

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 blocking of sites that threaten national security to censor the Web page of the Muslim Brotherhood, the country's major political opposition movement.<sup>130</sup> Similarly, Russia seeks to extend its controls on off-line media to the Internet – which could lead to selective enforcement of regulations against sites critical of the government.<sup>131</sup> Blocking Voice over Internet Protocol services may similarly seek to maintain an ISP's competitive position in the telephony market, particularly when the ISP is state-owned (and thus generates revenue for the country).<sup>132</sup> Censorship thus becomes a discretionary weapon in a government's arsenal, to be deployed arbitrarily rather than consistently.

---

<sup>127</sup> Tim Richardson, *Cleanfeed working overtime, says BT*, THE REGISTER, Feb. 7, 2006, at [http://www.theregister.co.uk/2006/02/07/bt\\_cleanfeed\\_iwfl](http://www.theregister.co.uk/2006/02/07/bt_cleanfeed_iwfl).

<sup>128</sup> Britain's other ISPs "voluntarily" acceded to using Cleanfeed by the end of 2007, as demanded by UK Home Office Minister Vernon Croaker. Frank Fisher, *Caught in the Web*, THE GUARDIAN, Jan. 17, 2008, at <http://www.guardian.co.uk/commentisfree/2008/jan/17/caughtintheweb>.

<sup>129</sup> *But see* Richard Clayton, *Failures in a Hybrid Content Blocking System*, in PRIVACY ENHANCING TECHNOLOGIES 78 (George Danezis & Philippe Golle, eds.) (2006) (describing technical problems with British Telecom's Cleanfeed system and demonstrating how Cleanfeed can be used to create an index of child pornography sites).

<sup>130</sup> Sarah El-Sirgany, *Al-Ahram Reverses Internet Block on Blogs*, DAILY NEWS EGYPT, Aug. 15, 2006, at <http://www.dailystaregypt.com/article.aspx?ArticleID=2615>; HUMAN RIGHTS WATCH, COUNTRY PROFILES: EGYPT (2005), at <http://www.hrw.org/reports/2005/mena1105/4.htm>.

<sup>131</sup> Anton Troianovski & Peter Finn, *Kremlin Seeks to Extend Its Reach to Cyberspace*, WASH. POST, Oct. 28, 2007, at A1; Jacqui Cheng, *New Iron Curtain may be draped over Russia's Internet*, ARS TECHNICA, Apr. 24, 2008, at <http://arstechnica.com/news.ars/post/20080424-new-iron-curtain-may-be-draped-over-russian-internet.html>.

<sup>132</sup> *See generally* Derek Bambauer, *Blocking VoIP*, at <http://blogs.law.harvard.edu/infolaw/2006/05/05/blocking-voip/> (May 5, 2006) (collecting examples of VoIP blocking).

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

One challenging aspect of assessing narrowness, particularly whether blocking is overbroad, is examining the level of filtering. At its most crude, filtering blocks users from accessing an entire domain. Pakistan, for example, sought to block access to “blasphemous” videos on YouTube in February 2008.<sup>133</sup> One Pakistani ISP, unable to selectively prevent access only to the offending videos<sup>134</sup>, filtered the entire YouTube site (and, due to a misconfiguration, briefly prevented users worldwide from reaching it)<sup>135</sup>. In 2006, Pakistan blocked the entire Blogspot blog-hosting site to prevent users from accessing controversial cartoons of Mohammed.<sup>136</sup> Ethiopia, seeking to prevent access to political dissent on Blogspot blogs, blocks the entire blogspot.com domain.<sup>137</sup> This stops Ethiopians from reading not only opposition politics material<sup>138</sup>, but also posts about women in science<sup>139</sup> or the science of the TV show *Battlestar Galactica*<sup>140</sup>. The United Arab Emirates blocks all sites in Israel's top-level .il domain, preventing users from reaching not only the Haaretz newspaper and the Knesset legislature, but also a site that sells “fun, educational toys for Israel's kids.”<sup>141</sup>

Similarly, blocking the IP address of an offending Web site often prevents access to additional, unrelated content.<sup>142</sup> When the Canadian ISP

<sup>133</sup> *Pakistan move knocked out YouTube*, CNN.COM, Feb. 25, 2008, at <http://www.cnn.com/2008/WORLD/asiapcf/02/25/pakistan.youtube/>.

<sup>134</sup> John Oates, *Pakistan blocks YouTube*, THE REGISTER, Feb. 25, 2008, at [http://www.theregister.co.uk/2008/02/25/pakistan\\_blocks\\_youtube/](http://www.theregister.co.uk/2008/02/25/pakistan_blocks_youtube/).

<sup>135</sup> Iljitsch van Beijnum, *Insecure routing redirects YouTube to Pakistan*, ARSTECHNICA, Feb. 25, 2008, at <http://arstechnica.com/news.ars/post/20080225-insecure-routing-redirects-youtube-to-pakistan.html>.

<sup>136</sup> ACCESS DENIED, *supra* note 7, at 159. On the cartoons, see generally Michael Kimmelman, *Outrage at Cartoons Still Tests the Danes*, N.Y. TIMES, Mar. 20, 2008, at E1.

<sup>137</sup> Ethan Zuckerman, *Blogspot still blocked. Newspapers still silent*, My Heart's in Accra, June 13, 2006, at <http://www.ethanzuckerman.com/blog/2006/06/14/blogspot-still-blocked-newspapers-still-silent/>. I thank Nart Villeneuve for this example.

<sup>138</sup> See, e.g., ethiopundit, at <http://ethiopundit.blogspot.com/> (displaying logo stating “This Blog is Blocked in Ethiopia”).

<sup>139</sup> Women in Science, at <http://sciencewomen.blogspot.com/> (last visited June 11, 2008).

<sup>140</sup> The Science of Battlestar Galactica, at <http://thescienceofbattlestargalactica.blogspot.com/> (last visited June 11, 2008).

<sup>141</sup> OPENNET INITIATIVE, *supra* note 122 at n.47 (describing ToyStore.co.il).

<sup>142</sup> Nart Villeneuve, *Why Block by IP Address?*, at <http://www.nartv.org/2005/02/14/why-block-by-ip-address/> (Feb. 14, 2005).

Telus blocked a Web site about a labor dispute with a union by filtering its IP address, it also prevented access to over 700 other sites.<sup>143</sup>

Even a Web page with objectionable material may have primarily unoffensive content – BoingBoing is classified by the SmartFilter software as containing nudity, although the popular blog has only a tiny amount of nude images among its posts.<sup>144</sup> It is a difficult, subjective decision to determine the right granularity for filtering: how much acceptable material should be blocked to prevent access to prohibited content?

Assessing whether a state's censorship is underbroad, overbroad, or both, requires careful empirical testing. This is challenging; the number of Web pages 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 generally 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 targeted for blocking.<sup>145</sup> Second, they check sites on topics known to be sensitive to a given country, such as pages about the Falun Gong spiritual movement in China.<sup>146</sup> For countries that employ commercial filtering software, one can test sites with known categories to establish which types of content that state wants to block.<sup>147</sup> This can also help uncover overinclusive filtering; commercial filtering programs have well-established errors, such as when the Websense software briefly classified Microsoft's downloads page as marijuana-related.<sup>148</sup>

To assess narrowness, testing should include a range of sites in zones of content a state has vowed (or is believed) to restrict, in areas it is suspected of covertly filtering (if any), and in categories that other states

---

<sup>143</sup> *Telus cuts subscriber access to pro-union website*, CBC NEWS, July 24, 2005, at <http://www.cbc.ca/story/canada/national/2005/07/24/telus-sites050724.html>; OPENNET INITIATIVE, TELUS BLOCKS CONSUMER ACCESS TO LABOUR UNION WEB SITE AND FILTERS AN ADDITIONAL 766 UNRELATED SITES, at <http://opennet.net/bulletins/010> (Aug. 2, 2005).

<sup>144</sup> Jardin, *supra* note 118; Tom Zeller Jr., *Popular Web Site Falls Victim to a Content Filter*, N.Y. TIMES, Mar. 6, 2006, at C3.

<sup>145</sup> See, e.g., OPENNET INITIATIVE, INTERNET FILTERING IN VIETNAM IN 2005-2006: A COUNTRY STUDY (2006), at <http://opennet.net/studies/vietnam/#app2> (displaying which sites on ONI's "global list" were blocked in Vietnam); see also *id.* at <http://opennet.net/studies/vietnam/#toc3a> (describing the global list and ONI's testing methodology).

<sup>146</sup> See, e.g., HUMAN RIGHTS WATCH, CHINA: WORLD REPORT 2007 (2007), at <http://hrw.org/englishwr2k7/docs/2007/01/11/china14867.htm>; Reporters Sans Frontières, *Internet Enemies: Syria*, at [http://www.rsf.org/article/php3?id\\_article=26156&Valider=OK](http://www.rsf.org/article/php3?id_article=26156&Valider=OK); Paul Wiseman, *In China, a battle over Web censorship*, USA TODAY, Apr. 23, 2008, at 1A.

<sup>147</sup> See *infra* note 353 and accompanying text.

<sup>148</sup> John Leyden, *Websense makes hash of MS classification*, THE REGISTER, Nov. 4, 2005, at [http://www.theregister.co.uk/2005/11/04/ms\\_websense\\_hash/](http://www.theregister.co.uk/2005/11/04/ms_websense_hash/).

block. The first set of sites checks how effective a country's blocking is. The second and third sets evaluate whether the state is forthright about the material it restricts.

Testing results show what types of sites a state filters (though not a comprehensive list of which sites are blocked). This empirical data also demonstrates how good the filtering system is at blocking prohibited material (evaluating underbreadth); what other sites, if any, it censors (evaluating overbreadth); and how broad (in the number of categories of material filtered) and deep (the percentage or number of sites per category) overblocking is.<sup>149</sup> This enables comparison of a state's actions and its rhetoric.

One normative challenge in the narrowness evaluation is deciding whether a site – blocked or unblocked – falls within the parameters of what a state claims to filter. (If the state makes no such public claim, this difficulty mitigates, but mapping the range of topics filtered is still trying.) The more vague or unclear a state's criteria for blocking, the more likely a site will fall within the ambit of prohibited content, or at least its penumbra. This uncertainty may in itself be useful: it can reveal innocent content that is swept up for blocking. Some material is inherently susceptible to classification in multiple ways: a dating site for the gay / lesbian community may be blocked because the state objects to dating services<sup>150</sup>, to public discussion of gay and lesbian issues<sup>151</sup>, or both<sup>152</sup>. Categorizing content involves subjective decisions; a state's censors may be lax, strict, or simply wrong in their blocking choices. 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 state is in revealing its reasons and actions for censorship; transparency maps the content the state purports to restrict; and narrowness checks how successful the state's actions are – and whether it suppresses different matter than it claims.

#### *D. Accountability*

The fourth criterion is accountability: to what degree can citizens influence policymaking on what is censored? What measures or structures

---

<sup>149</sup> See Faris & Villeneuve, *supra* note 89, at 11, 18-20.

<sup>150</sup> See OPENNET INITIATIVE, *supra* note 44.

<sup>151</sup> See, e.g., OPENNET INITIATIVE, YEMEN, at <http://opennet.net/research/profiles/yemen> (documenting Yemen's filtering of some gay and lesbian content) (May 9, 2007).

<sup>152</sup> See OPENNET INITIATIVE, *supra* note 97 (analyzing Iran's filtering).

push officials to respond to their constituents? What recourse is available to content owners who contend they have been blocked erroneously?

The purpose of this factor is to assess how closely a state's censorship aligns with the goals and views of its citizens. It also considers how responsive blocking practices are to changes in those views. Accountability here has four major aspects: participation in censorship decisions, specification of authority, opportunity to challenge filtering, and counter-majoritarian constraints.

Participation looks to whether citizens and users drive both the decision to block access to Internet material at all and subsequent selection of sites to filter. The most obvious method is policy adopted by a representative government after public debate. Though it has faced significant criticism<sup>153</sup>, the Digital Millennium Copyright Act enacted by the United States in 1998<sup>154</sup> is a good example: it moved through public hearings and was widely supported in the U.S. Congress<sup>155</sup>. Under the DMCA, ISPs must filter access to allegedly copyright-infringing materials<sup>156</sup> – either on their servers or in the search results they provide – to avail themselves of a “safe harbor” exemption from secondary liability<sup>157</sup>. Filtering thus emerged from an established, participatory public regulation process.

There are also examples of citizens participating in filtering policy both indirectly, by electing a government that implements on-line restrictions through informal or private arrangements, and directly, by suggesting or “tagging” sites for addition to a block list. For example, France's Interior Minister announced that French ISPs had agreed, after negotiations with the government, to filter sites with child pornography, terrorism, or hate speech.<sup>158</sup> French users can alert the state to sites believed to fall into those categories; the government will then decide whether to

---

<sup>153</sup> 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, *Why the Anti-Circumvention Regulations Need To Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); but see Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J. LAW & TECH. 49 (2006) (proposing to use the digital rights systems protected by the DMCA to enable fair use under copyright law).

<sup>154</sup> Pub. L. No. 105-304, 112 Stat. 2860, 2877-86 (1998).

<sup>155</sup> The final version of the DMCA passed unanimously in both houses of Congress. Urban & Quilter, *supra* note 12, at 635.

<sup>156</sup> See, e.g., Chris Sherman, *Google Makes Scientology Infringement Demand Public*, SEARCH ENGINE WATCH, Apr. 15, 2002, at <http://searchenginewatch.com/showPage.html?page=2159691>; *Google Asked to Delist Scientology Critics (#1)*, CHILLING EFFECTS CLEARINGHOUSE, Mar. 8, 2002, at <http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=232>.

<sup>157</sup> 17 U.S.C. §§ 512(c), (d).

<sup>158</sup> *France blocks online child porn, terrorism, racism*, ASSOC. PRESS, June 10, 2008, available at [http://www.usatoday.com/tech/world/2008-06-10-france-online-porn\\_N.htm](http://www.usatoday.com/tech/world/2008-06-10-france-online-porn_N.htm).

include “flagged” sites on the list blocked by ISPs.<sup>159</sup> (This approach is similar to open source efforts that involve users in categorizing content, such as the Open Directory Project<sup>160</sup> and OpenDNS<sup>161</sup>; OpenDNS also runs an Internet filtering service<sup>162</sup>.) Thus, French citizens guide both the general censorship approach (such as the ban on racist speech<sup>163</sup>) and specific filtering decisions.

Democratic government, though, does not guarantee participation in policy choices on censorship. Thailand generally functions as a democracy (albeit with intermittent military coups<sup>164</sup>), but operates a censorship regime with minimal citizen participation<sup>165</sup>. While the Thai government must theoretically obtain a court order to force ISPs to block a Web site, a government minister in May 2008 unilaterally ordered the filtering of a prominent independent news portal and a social criticism site, both with popular discussion boards, allegedly on instructions from senior Thai officials.<sup>166</sup> Many sites earlier blocked by the military government contain content critical of the 2006 military coup and of the Thai military's involvement in politics.<sup>167</sup>

In addition, it is increasingly difficult to assess whether a state is “democratic,” and the ability to use a state's formal structures of government as a reliable indicator of accountability is weakening.<sup>168</sup> A country may have the outward indicators of democratic governance – multiple independent government branches, elections based on universal suffrage, a formalized constitution, and so forth – yet may subvert them via tactics such as voter intimidation, arbitrary arrest, media control, and state

<sup>159</sup> U.S., *France move to block online child pornography*, CBC NEWS, June 10, 2008, at <http://www.cbc.ca/technology/story/2008/06/10/isps-porn-block.html>.

<sup>160</sup> *dmoz – Open Directory Project*, at <http://www.dmoz.org/> (last visited June 11, 2008).

<sup>161</sup> *OpenDNS*, at <http://www.opendns.com/> (last visited June 11, 2008).

<sup>162</sup> *OpenDNS, Content Filtering*, at [http://www.opendns.com/features/content\\_filtering/](http://www.opendns.com/features/content_filtering/) (last visited June 11, 2008).

<sup>163</sup> *See, e.g., Bardot fined over racial hatred*, BBC NEWS, June 3, 2008, at <http://news.bbc.co.uk/2/hi/entertainment/7434193.stm>; *see generally supra* note 108.

<sup>164</sup> *See, e.g., Seth Mydans, Ousted Premier Is Set to Return to Thailand, Officials Say*, N.Y. TIMES, Feb. 27, 2008, at A4.

<sup>165</sup> OPENNET INITIATIVE, THAILAND, *supra* note 96.

<sup>166</sup> C.J. Hinke, *Censoring Free Speech in Thailand*, at <http://advocacy.globalvoicesonline.org/2008/05/17/censoring-free-speech-in-thailand/> (May 17, 2008). It is not clear whether the Thai government has legal authority to censor the Internet at all. ACCESS DENIED, *supra* note 7, at 158-59.

<sup>167</sup> *Thailand: Military-Backed Government Censors Internet*, HUMAN RIGHTS NEWS, at <http://www.hrw.org/english/docs/2007/05/23/thaila15996.htm> (May 24, 2007); *see generally* GLOBAL INTEGRITY REPORT, THAILAND (2007), at <http://report.globalintegrity.org/Thailand/2007>.

<sup>168</sup> *See generally* Andreas Schedler, *The menu of manipulation*, 13 J. DEMOCRACY 36 (2002).

ownership of key information outlets. Russia<sup>169</sup>, Venezuela<sup>170</sup>, and Zimbabwe<sup>171</sup> are examples of states where the appearance of democracy is increasingly at odds with the reality of governance, and where accountability is diminishing.

Even U.S. efforts can generate accountability problems. In June 2008, New York's attorney general pressed three major ISPs to withdraw access to a wide range of Usenet news groups – only 88 of which had been demonstrated to contain illicit material – to reduce on-line distribution of child pornography<sup>172</sup>; by July, AT&T and AOL had agreed to do so as well<sup>173</sup>. Beyond the obvious narrowness concerns, the agreement between New York and the ISPs will limit Usenet access for all of the providers' customers, not just those in New York.<sup>174</sup> While child pornography is unlawful under U.S. federal statutes<sup>175</sup>, in addition to New York ones<sup>176</sup>, regulators in other states (or the federal government) might have sought a different solution to the problem of its distribution. They might have included other major U.S. providers (such as Comcast<sup>177</sup>), narrowed the scope of Usenet restrictions (perhaps to the 88 groups with unlawful images), or broadened blocking to include Web sites with child pornography (as initial reports indicated New York had required<sup>178</sup>). Other states have begun to echo New York's demands on ISPs, increasing the likelihood of fragmented regulation.<sup>179</sup>

<sup>169</sup> See, e.g., Human Rights Watch, *Russia Goes to the Polls*, at <http://hrw.org/english/docs/2007/11/29/russia17440.htm> (Nov. 29, 2007); Clifford J. Levy, *Putin Aide Secures His Assured Victory in Russian Vote*, N.Y. TIMES, Mar. 3, 2008, at A3.

<sup>170</sup> See, e.g., Fabiola Sanchez, *Venezuela's Chavez pushes through 26 decrees*, WASH. POST, Aug. 5, 2008, at [http://www.washingtonpost.com/wp-dyn/content/article/2008/08/04/AR2008080402684\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/08/04/AR2008080402684_pf.html).

<sup>171</sup> See, e.g., Celia W. Dugger & Barry Bearak, *Mugabe Rival Quits Zimbabwe Runoff, Citing Attacks*, N.Y. TIMES, June 23, 2008, available at <http://www.nytimes.com/2008/06/23/world/africa/23zimbabwe.html?pagewanted=all>; HUMAN RIGHTS WATCH, ALL OVER AGAIN: HUMAN RIGHTS ABUSES AND FLAWED ELECTORAL CONDITIONS IN ZIMBABWE'S COMING GENERAL ELECTIONS (2008), available at <http://hrw.org/reports/2008/zimbabwe0308/>.

<sup>172</sup> McCullagh, *supra* note 2.

<sup>173</sup> See, e.g., Linda Rosencrance, *ISPs Join to Block Child Porn*, PCWORLD, July 13, 2008, at [http://www.pcworld.com/article/148295/isps\\_join\\_to\\_block\\_child\\_porn.html](http://www.pcworld.com/article/148295/isps_join_to_block_child_porn.html).

<sup>174</sup> *Id.*

<sup>175</sup> See, e.g., 18 U.S.C. §§ 2252, 2252A (2008).

<sup>176</sup> N.Y. PENAL LAW § 263.00 et seq. (Consol. 2008).

<sup>177</sup> Comcast was the second-largest U.S. ISP for the fourth quarter of 2007. Alex Goldman, *Top 25 U.S. ISPs by Subscriber: Q4 2007*, ISP-PLANET, Apr. 10, 2008, at <http://www.isp-planet.com/research/rankings/usa.html>.

<sup>178</sup> Hakim, *supra* note 2; Peter Grier, *ISPs Take Major Step in Curbing Child Porn*, THE CHRISTIAN SCIENCE MONITOR, June 11, 2008, at <http://www.csmonitor.com/2008/0611/p01s09-usgn.html?page=2>.

<sup>179</sup> Marguerite Reardon, *California pols ask ISPs to block child porn*, CNET NEWS.COM, June 20, 2008, at [http://news.cnet.com/8301-10784\\_3-9973966-7.html](http://news.cnet.com/8301-10784_3-9973966-7.html).

Conversely, participation is possible even in states without democratic government. Saudi Arabia, for example, permits only limited political participation by its citizens<sup>180</sup>, but invites users to suggest sites that should be blocked, or to challenge a decision to censor material. The acting general manager of the kingdom's Internet gateway claimed that all such requests were reviewed within 24 hours, and that requests for censorship were rejected if they were not within the guidelines established by a governmental committee.<sup>181</sup> The Saudi censors receive hundreds of requests each day to censor additional material, but only a few to unblock sites.<sup>182</sup> Historically, participation has had at least some effect: in 2001, a Saudi official reported that 30% of requests to block additional sites resulted in additions to the kingdom's "block list," and 3% of requests to unblock material were granted.<sup>183</sup> Users' satisfaction is mixed, but indicates that Saudi filtering may be a compromise: a 1999 survey revealed that 41% of users were satisfied with the level of censorship, while 45% found it too onerous and 14% sought even more restrictions.<sup>184</sup> Even if citizens have limited participation in governance, they may have some ability to shape their country's Internet censorship.

Accountability also includes the ability to hold government censors to task – a process eased considerably when the basis for censorship is specified formally in statute or rule. Codification of censorship criteria not only puts citizens on notice regarding permitted and prohibited content, it also constrains blocking decisions. Even if challenging a censor's decision is not possible, filtering that is at odds with a state's rules detracts from the legitimacy of those restrictions. Where one can contest censorship choices, any such contradictions will weaken the basis for upholding denials of access.

---

<sup>180</sup> See, e.g., FREEDOM HOUSE, SAUDI ARABIA: 2007 (2007), at <http://www.freedomhouse.org/template.cfm?page=22&year=2007&country=7265> (noting "Saudis do not enjoy freedoms of assembly and association... Saudi Arabia does not have political parties, and the only semblance of organized political opposition exists outside the country").

<sup>181</sup> See, e.g., Raid Qusti, *Most of Kingdom's Internet Users Aim for the Forbidden*, ARAB NEWS, Oct. 2, 2005, at <http://www.arabnews.com/?page=1&section=0&article=71012&d=2&m=10&y=2005> (noting the filtering body "had ignored requests from many people to block all religious sites except for Islamic ones").

<sup>182</sup> Robin Miller, *Meet Saudi Arabia's most famous computer expert*, NEWSFORGE, Jan. 14, 2004, at <http://internet.newsforge.com/article.pl?sid=04/01/12/2147220>.

<sup>183</sup> ABDULAZIZ HAMAD AL-ZOMAN, THE INTERNET IN SAUDI ARABIA (TECHNICAL VIEW), at <http://www.isu.net.sa/library/CETEM2001-Zoman.pdf> (Apr. 30, 2001).

<sup>184</sup> INTERNET SERVICES UNIT, THE OLD USER SURVEY RESULTS (JULY – SEPT. 1999), at <http://www.isu.net.sa/surveys-&-statistics/user-survey.htm>. Note, though, that the sample size is small – only 260 users.

Italy, for example, passed legislation in 2005<sup>185</sup> allowing an agency of the Ministry of Economy and Finances to specify gambling sites that must be blocked by Italian ISPs (namely, sites that did not register with the agency, the Autonomous Administration of State Monopolies, or AAMS).<sup>186</sup> AAMS created a list of sites in February 2006 and published it.<sup>187</sup> On-line gambling enterprises thus knew whether they had been filtered, and why – indeed, the Malta-based bookmaker Astrabet successfully challenged the ban in court in Italy.<sup>188</sup> Specifying the criteria for filtering, and the sites to be blocked, limited the government's discretion in banning on-line content and enabled affected sites to contest their blacklisting.

Formalizing censorship standards, though, may not sufficiently constrain state 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<sup>189</sup> and Broadcasting Act<sup>190</sup>), regulation (class licenses for broadcasting<sup>191</sup>), and formal ISP industry policy documents (the Media Development Authority's Internet Code of Practice<sup>192</sup>). However, definitions of prohibited content are broad – such as “objectionable on the grounds of public interest, public morality, public order, [or] public security” – and provide discretion to government censors.<sup>193</sup> While the putative focus for filtering is pornography and religious extremism, the state has employed these elastic guidelines to block popular gay and lesbian sites.<sup>194</sup> The ability to argue that the government has exceeded its mandate is limited by paired legal obstacles: the broad regulatory language defining banned content, and the opportunity for government officials to wield Singapore's harsh defamation laws to

---

<sup>185</sup> Italian Fin. Law 266/2005 (Dec. 23, 2005), *available at* <http://www.gazzettaufficiale.it/guri/attocompleto?dataGazzetta=2005-12-29&redazione=005G0293&service=0&ConNote=2>.

<sup>186</sup> Andrea Glorioso, *Betting Websites Are Blocked in Italy*, EDRI, June 21, 2006, *at* <http://www.edri.org/edrigram/number4.12/italybetting>.

<sup>187</sup> AAMS, *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*, *at*

<http://www.aams.it/site.php?page=20060213093814964&op=download>.

<sup>188</sup> Glorioso, *supra* note 186.

<sup>189</sup> Available at <http://www.mda.gov.sg/wms.www/devnpolicies.aspx?sid=153>.

<sup>190</sup> *Id.*

<sup>191</sup> BROADCASTING (CLASS LICENCE) NOTIFICATION, § 9, ch. 28, Broadcasting Act, July 15, 1996, *available at* <http://www.mda.gov.sg/wms.file/mobj/mobj.487.ClassLicence.pdf>.

<sup>192</sup> Singapore Media Development Authority, *supra* note 91.

<sup>193</sup> *Id.*

<sup>194</sup> *See, e.g., Singapore bans gay website*, SYDNEY MORNING HERALD, Oct. 28, 2005, *at* <http://www.smh.com.au/news/breaking/singapore-bans-gay-website/2005/10/28/1130400335787.html>.

silence critics.<sup>195</sup> Even a state that specifies its filtering criteria in formal regulations may not be particularly accountable.

Censors make mistakes. Moreover, content owners may want to challenge even decisions that correctly classify their Web sites by attacking the underlying rationale for a ban. One aspect of accountability is whether a state provides means to contest censorship. This interacts with governance – democratic institutions generally provide some opportunity for redress, whether via legislatures or courts – and also with specificity – the more concrete the guidelines for filtering, the easier it is to show whether a particular ban contravenes them. Challenges to censorship enhance legitimacy by forcing the state to justify its decisions, pressing censors to align their decisions with relevant criteria, and allowing content creators to argue for the legality of their material in the face of adverse government contentions.

China, for example, fares poorly on this front. The state implements its filtering policies – when it admits to them overtly<sup>196</sup> – via a congeries of statutes, agency regulations, and informal measures<sup>197</sup>. Censorship occurs through a mix of formal legal restrictions and tacit cooperation by Internet companies, including American firms such as Yahoo! and Google.<sup>198</sup> It is difficult to determine how to contest censorship, and whom to hold responsible. Even citizens bold enough to challenge restrictions – such as a dog owner's lawsuit over the removal of his post criticizing Beijing's animal size limits – face legal hurdles (the court rejected his case) and

---

<sup>195</sup> See, e.g., Seth Mydans, *Power and Tenacity Collide in a Singapore Courtroom*, N.Y. TIMES, May 30, 2008, at <http://www.nytimes.com/2008/05/30/world/asia/30singapore.html> (describing defamation suits that bankrupted opposition political leader Chee Soon Juan).

<sup>196</sup> See Patrick Di Justo, *Does the End Justify the Means?*, WIRED, Mar. 18, 2003, at <http://www.wired.com/politics/law/news/2003/03/58082> (quoting Larry Wu, second secretary for Science and Technology at China's embassy in Washington, as stating “We don't have censorship of the Internet... Generally, the Chinese government is for the full exchange of information”).

<sup>197</sup> See, e.g., State Administration of Radio, Film, and Television, *Provisions on the Administration of Internet Video and Audio Programming Services*, available at <http://www.chinasarft.gov.cn/articles/2007/12/29/20071229134709730745.html> (Dec. 20, 2007); Ministry of Information Industry (MII), *Measures for the Administration of Internet Information Services*, at <http://tradeinservices.mofcom.gov.cn/en/b/2000-09-25/18565.shtml> (Sept. 25, 2000); MII & General Administration of Press and Publication, *Interim Provisions on the Administration of Internet Publication*, available at <http://www.lawinfochina.com/law/displayModeTwo.asp?id=2393> (June 27, 2002); Internet Society of China, *Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry*, at <http://www.isc.org.cn/20020417/ca102762.htm> (last revised July 19, 2002); see generally Liu, *supra* note 113.

<sup>198</sup> *Id.*; see generally LOKMAN TSUI, INTERNET IN CHINA: BIG MAMA IS WATCHING YOU (July 2001), available at <http://www.lokman.nu/thesis/010717-thesis.pdf>; 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 (2007).

informal pressures, such as harassment from government agents.<sup>199</sup> Chinese citizens – many of whom endorse a role for the government in regulating Internet content<sup>200</sup> – evidently view formal challenges as futile; only two such lawsuits have ever been filed<sup>201</sup>.

Unsurprisingly, states with independent judicial systems are most likely to enable challenges to filtering decisions. Astrabet sued in Italian court to overturn state-mandated blocking of its site; the company won, and an appellate court upheld the verdict and ordered the removal of the site from the block list.<sup>202</sup> In the United States, the Center for Democracy & Technology successfully sued to overturn a Pennsylvania state law that mandated blocking of Internet child pornography but that also caused ISPs to filter over one million unrelated Web sites.<sup>203</sup> While there is likely a strong correlation between the ability to challenge meaningfully a censorship decision and a state's overall form of governance, contesting filtering is possible even in non-democratic states. Saudi Arabia allows users or content owners to ask for sites to be unblocked, and decisions to overturn filtering, while uncommon, do occur.<sup>204</sup> Efforts by civic actors in Tajikistan and Azerbaijan have led those states to reverse decisions to block political opposition sites.<sup>205</sup> While less robust than the Italian or American methods for challenging censorship, these examples prove that there is a continuum of means to contest filtering, and that a state's form of governance is not a perfect proxy for this variable.

A final challenge for measuring accountability is the proper role for countermajoritarian constraints. Even under democratic government, a state may disadvantage or discriminate against minority groups, whose limited numbers impede their ability to counteract majoritarian rule. Australia's treatment of its indigenous Aborigine peoples serves as one example<sup>206</sup>, as

---

<sup>199</sup> Edward Cody, *Man Sues After Government Removes Posting Critical of Canine Height Restriction*, WASH. POST, Dec. 26, 2007, at A18.

<sup>200</sup> Deborah Fallows, *Few in China Complain About Internet Controls*, PEW INTERNET & AMERICAN LIFE PROJECT, Mar. 27, 2008, at <http://pewresearch.org/pubs/776/china-internet> (reporting on public opinion polls showing 80% of respondents support Internet regulation, and 85% believe the government should undertake it).

<sup>201</sup> Cody, *supra* note 199.

<sup>202</sup> Francesco Portolano & Yan Pecoraro, *Italy: Italian Courts on Betting Sites Black-List*, MONDAQ, Apr. 25, 2006, at <http://www.mondaq.com/article.asp?articleid=39326>.

<sup>203</sup> *Pappert*, 337 F. Supp. 2d 606.

<sup>204</sup> See AL-ZOMAN, *supra* note 183.

<sup>205</sup> OPENNET INITIATIVE, COMMONWEALTH OF INDEPENDENT STATES, at <http://opennet.net/research/regions/cis> (last visited Aug. 18, 2008).

<sup>206</sup> See, e.g., Andrew Bonnell & Martin Crotty, *Australia's History under Howard: 1996-2007*, 617 ANNALS OF THE ACADEMY OF POLIT. & SOC. SCI. 149, 155-59 (2008) (discussing Australia's treatment of its indigenous population).

does Canadian treatment of its Indian, Inuit, and Metis population<sup>207</sup>. Discrimination, unfortunately, may be popular.

Censorship of minority-interest Web content is common. 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).<sup>208</sup> Oman blocks gay and lesbian sites, including dating sites.<sup>209</sup> Saudi Arabia, with a predominantly Sunni population, prevents access to some material about the Bahai faith or about non-Sunni Muslim views.<sup>210</sup> Pakistan blocks sites advocating independence for its Balochistan and Sindh provinces.<sup>211</sup> Burma filters material about the minority Karen people.<sup>212</sup>

Filtering poses a difficult normative problem: a minority of citizens wants access to certain material on-line, while the majority of their compatriots wants to prevent it. When should the minority's objections to a decision that commands majoritarian support be upheld? Ultimately, this is a question of system design – 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 struggled to describe the proper set of constraints on majoritarian decisionmaking and to defend the rationale for such limits in a representative democracy. Alexander Bickel first coined the term “counter-majoritarian check,” noting that having an independent judiciary review (and, potentially, disallow) democratic decisions could cause legislatures to rely overly on courts to save them from illegitimate or unlawful actions.<sup>213</sup> Bickel concluded, though, that judicial training, and focus upon the specific facts of a contested case, usefully enabled reconsideration of controversial regulation.<sup>214</sup> 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, for example, saw the courts, and constitutional interpretation more broadly, as focused primarily upon ensuring procedural

---

<sup>207</sup> DeNeeen L. Brown, *Canadian Government Apologizes For Abuse of Indigenous People*, WASH. POST, June 12, 2008, at A1.

<sup>208</sup> OPENNET INITIATIVE, *supra* note 120; *see generally* Human Rights Watch, *Vietnam: Montagnards Face Religious, Political Persecution*, June 14, 2006, at <http://hrw.org/english/docs/2006/06/14/vietna13542.htm>.

<sup>209</sup> OPENNET INITIATIVE, OMAN, at <http://opennet.net/research/profiles/oman> (May 10, 2007).

<sup>210</sup> OPENNET INITIATIVE, *supra* note 80, at <http://opennet.net/studies/saudi#toc4b>.

<sup>211</sup> OPENNET INITIATIVE, PAKISTAN, at <http://opennet.net/research/profiles/pakistan> (May 10, 2007).

<sup>212</sup> OPENNET INITIATIVE, INTERNET FILTERING IN BURMA IN 2005 (2005), at <http://opennet.net/studies/burma>.

<sup>213</sup> ALEXANDER BICKEL, THE LEAST DANGEROUS BRANCH 16-18 (1962).

<sup>214</sup> *Id.* at 131-32.

protections, while deferring normative judgments to government's representative branches.<sup>215</sup> 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.<sup>216</sup> In short, whether, and to what degree, popular will should be limited – to protect certain shared values<sup>217</sup> or to prevent discrimination against weaker minority groups<sup>218</sup> – is highly contested, and beyond this Article's scope (and its author's expertise).

However, Internet censorship may make countermajoritarian constraints particularly necessary, for two reasons. First, filtering is not always transparent: it can be difficult to detect what content one has been prevented from accessing, or what sites are most relevant in response to a search engine query.<sup>219</sup> (Contrast this with the ease of detecting censorship in physical media, as when copies of *National Geographic* in China were found with pages on disputed borders or ethnic minorities glued together.<sup>220</sup>) Filtering is easy to hide and hard to evaluate for legitimacy or scope. It risks altering not the systemic structures of a state, but the information its citizens use to arrive at decisions. Russian citizens may not know about political opposition to the current government, or its grounds for complaint, if contrary views are made to disappear from mass media such as television and the Internet.<sup>221</sup> Censorship raises Ely's concerns about skewing process, though it does so more subtly than overt changes such as alterations in the franchise might.

Second, censorship prevents access to material that might influence popular views regarding its necessity. Political opponents or critics are more

---

<sup>215</sup> JOHN HART ELY, *DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW* 73-77 (1980).

<sup>216</sup> Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 *YALE L.J.* 1346 (2006).

<sup>217</sup> See, e.g., Laurence H. Tribe, *The Puzzling Persistence of Process-Based Constitutional Theories*, 59 *YALE L.J.* 1063 (1980).

<sup>218</sup> See, e.g., *U.S. v. Carolene Prods. Co.*, 304 U.S. 144, 152-53 n.4 (discussing possibility that “prejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities”).

<sup>219</sup> See, e.g., Nart Villeneuve, *Degrading Transparency: Comparing Google, Yahoo! and Microsoft*, at <http://www.nartv.org/2008/01/25/degrading-transparency-comparing-google-yahoo-and-microsoft/> (Jan. 25, 2008).

<sup>220</sup> Geoffrey A. Fowler, *Glued Geographic*, *WALL STREET J.*, June 4, 2008, at <http://blogs.wsj.com/chinajournal/2008/06/04/glued-geographic/>.

<sup>221</sup> See, e.g., Clifford J. Levy, *It Isn't Magic: Putin Opponents Vanish From TV*, *N.Y. TIMES*, June 3, 2008, at <http://www.nytimes.com/2008/06/03/world/europe/03russia.html>.

readily mocked or demonized when their views are unavailable.<sup>222</sup> Subjective preferences are not independent or static; they evolve in response to available information.<sup>223</sup> As Oliver Wendell Holmes noted, today's minority viewpoint may be tomorrow's accepted wisdom.<sup>224</sup> It may seem acceptable to sacrifice access to information under one set of circumstances, but this makes it difficult to regain access in the future, when the data may be more useful, since it becomes hard to assess the relevance of unavailable data. Thus, on-line censorship may present a more acute need for checks on majoritarian decisionmaking.

Accountability may, ironically, require limiting censorship's responsiveness to popular sentiment. This could include both regulatory inertia – dampening or delaying shifts in practices to accord with changes in social views – and also countermajoritarian protections for minority expression. At minimum, accountability analysis should include assessing how a state addresses minority concerns and the potential risks of majoritarian control.

Accountability, the final factor in the framework for analyzing filtering's legitimacy, complements the previous three by measuring how responsive censorship practices are to the people they are supposed to protect. This prong evaluates how fully citizens can participate in the decision to filter the Internet and in what content to target for blocking; how the state formalizes and specifies its criteria for censorship; to what degree filtering decisions can be contested; and what protection exists for minority viewpoints.

With the overview of the four-part evaluative framework complete, the next question is how to translate this approach into concrete tools for assessing a given state's practices.

#### IV. IMPLEMENTATION

The analytical model described in Part III is only as useful as its implementation. The best way to apply the framework is for multiple entities, public and private, to construct quantitative metrics that measure how a state fares on each of the four criteria. As these metrics are used, they will inevitably compete, and that competition will refine and improve their measurements. The metrics can, and should, guide corporate decisions,

---

<sup>222</sup> *Id.*

<sup>223</sup> See generally RICHARD H. THALER & CASS R. SUNSTEIN, *NUDGE* (2008); Derek E. Bambauer, *Shopping Badly: Cognitive Biases, Communications, and the Fallacy of the Marketplace of Ideas*, 77 *COLO. L. REV.* 649 (2006).

<sup>224</sup> *Abrams v. U.S.*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (noting “time has upset many fighting faiths”).

government regulation, and third-party assessments regarding Internet censorship.

#### *A. Developing the Metrics*

The purpose of the four-part framework is to enable more rigorous assessments of the legitimacy of a state's Internet censorship. Implicit in this goal is comparison: it is useful to evaluate whether China's Internet filtering is more legitimate than Iran's, or whether that blocking has become more legitimate over time. However, comparison based upon general principles is difficult – it is challenging to establish on what basis, for example, a particular state is more transparent than another without a means of measuring that quality.

Metrics provide that means. For Internet filtering, a metric would establish numeric criteria to rate a state on each of the four factors. The metric's test would be applied to each censoring country. Since all states would be evaluated under the same rules, one could compare their scores to determine relative position. For example, a metric could test a state's openness by awarding points for methods of 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 and spokespeople to discuss filtering in the media, and so forth. Freedom House uses an analogous method to assess a country's political environment as it affects press freedom, asking (among other questions) whether media regulatory bodies can operate freely and independently (scored from 0 to 2 points); whether a state's constitution or other basic laws protect freedoms of the press and expression, and whether those provisions are enforced (0-6 points); and whether there are penalties for libeling state officials, and the degree to which they are enforced (0-3 points).<sup>225</sup> In analyzing narrowness, a metric could check how effective a state is in blocking material that it seeks to censor (with 100% efficacy the goal); how many other categories of material are blocked, and how heavily (using, for example, the classification system of the Open Directory Project<sup>226</sup>, or the OpenNet Initiative's categories<sup>227</sup> or global list<sup>228</sup>); and perhaps how precise the method of filtering used is (with less credit awarded for crude methods such as IP address blocking). The OpenNet Initiative uses a similar approach,

---

<sup>225</sup> FREEDOM HOUSE, SURVEY METHODOLOGY 3-4 (2008), *available at* <http://www.freedomhouse.org/uploads/fop08/Methodology2008.pdf>

<sup>226</sup> *See supra* note 160.

<sup>227</sup> *See* FARIS & VILLENEUVE, *supra* note 89, at 7.

<sup>228</sup> *See, e.g.*, OPENNET INITIATIVE, *supra* note 120, at

<http://opennet.net/studies/vietnam#toc4b> (describing results of global list testing).

rating countries on a scale of 1 to 4 for the level of filtering of political sites, social sites, conflict and security material, and Internet tools, while also grading states on how consistent their censorship is.<sup>229</sup>

Metrics – quantitative rankings or grades – have been helpfully employed for other contested issues, including corruption<sup>230</sup>, press freedom<sup>231</sup>, economic freedom<sup>232</sup>, labor<sup>233</sup>, environmental friendliness<sup>234</sup>, and ICT (information and communication technology) readiness<sup>235</sup>. These measurements serve at least four useful purposes. First, they translate abstract goals or standards into more 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, the metrics direct critical attention back to the standards that they seek to implement. Implementation challenges can highlight criteria that are insufficiently precise or too difficult to measure accurately.<sup>236</sup>

Designing a metric involves challenging, subjective choices. The most obvious is deciding how to measure a principle such as accountability. What considerations should be included? How should one measure each

---

<sup>229</sup> FARIS & VILLENEUVE, *supra* note 89, at 17-19.

<sup>230</sup> See, e.g., TRANSPARENCY INTERNATIONAL, CORRUPTION PERCEPTIONS INDEX 2007, at [http://www.transparency.org/policy\\_research/surveys\\_indices/cpi/2007](http://www.transparency.org/policy_research/surveys_indices/cpi/2007); TRANSPARENCY INTERNATIONAL, BRIBE PAYERS INDEX 2006, at [http://www.transparency.org/content/download/9757/71853/version/1/file/BPI\\_2006\\_Analysis\\_Report\\_270906\\_FINAL.pdf](http://www.transparency.org/content/download/9757/71853/version/1/file/BPI_2006_Analysis_Report_270906_FINAL.pdf).

<sup>231</sup> FREEDOM HOUSE, *supra* note 225.

<sup>232</sup> See, e.g., THE HERITAGE FOUNDATION & THE WALL STREET JOURNAL, INDEX OF ECONOMIC FREEDOM 2008, at <http://www.heritage.org/research/features/index/index.cfm>; JAMES GWARTNEY & ROBERT LAWSON, ECONOMIC FREEDOM OF THE WORLD: 2007 ANNUAL REPORT (2007), at <http://www.freetheworld.com/2007/EFW2007BOOK2.pdf>.

<sup>233</sup> See, e.g., Nike, *Audit Tools*, available at [http://www.nikebiz.com/nikeresponsibility/#workers-factories/audit\\_tools](http://www.nikebiz.com/nikeresponsibility/#workers-factories/audit_tools) (providing tools and measures Nike uses to determine factory compliance with its labor standards); Richard M. Locke, Fei Qin, & Alberto Brause, *Does Monitoring Improve Labor Standards? Lessons From Nike*, 61 INDUS. & LABOR RELATIONS REV. 3 (2007).

<sup>234</sup> See, e.g., Global Reporting Initiative, *Reporting Framework Overview*, at <http://www.globalreporting.org/ReportingFramework/ReportingFrameworkOverview/> (last visited July 20, 2008); ADVANCE, *About the Survey*, at <http://www.advance-project.org/survey/aboutthesurvey/index.html> (last visited July 20, 2008).

<sup>235</sup> See, e.g., INFODEV, E-READY FOR WHAT? (May 2005), available at <http://www.infodev.org/en/Publication.3.html>; BRIDGES.ORG, E-READINESS ASSESSMENT TOOLS COMPARISON (Feb. 28, 2005), at [http://www.bridges.org/files/active/0/ereadiness\\_tools\\_bridges\\_10Mar05.pdf](http://www.bridges.org/files/active/0/ereadiness_tools_bridges_10Mar05.pdf).

<sup>236</sup> See, e.g., Robert M. Stern, *Labor Standards and Trade*, in NEW DIRECTIONS IN INTERNATIONAL ECONOMIC LAW (Marco Bronckers & Reinhard Quick, eds.) (2000); working paper available at <http://www.fordschool.umich.edu/research/papers/PDFfiles/00-008.pdf>.

component? How should the components be weighed relative to one another? How should a metric account for a state's internal inconsistencies, such as when different ISPs filter to varying degrees<sup>237</sup>, or government officials waver on admitting to censorship<sup>238</sup>? The next normative choice involves comparing factors. Should openness count more than narrowness? In assessing environmental sustainability, ADVANCE, for example, distinguishes between the absolute amount of sustainable value companies create, based on their environmental practices, and the efficiency with which those companies use resources (since larger companies tend to generate more value than smaller ones, but also use more resources).<sup>239</sup> Finally, the metric must select at what level countries can be compared. Can scores for the four principles be aggregated into a composite score for a state, or does that obscure more than it reveals about a country's censorship? Is it too difficult to comprehend factor-by-factor comparisons of states? Transparency International, for example, standardizes the data inputs to its corruption index and creates an overall measure of how corrupt a country is perceived to be.<sup>240</sup> These are all hard decisions. There is no obvious correct choice. As with filtering itself, there are likely multiple defensible answers.

Thus, it would be optimal to generate multiple metrics, reflecting a range of decisions on these value-driven questions.<sup>241</sup> Different experts and interested parties could create and apply metrics that measure how states comply with the framework's four criteria. 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 OpenNet Initiative) would be preferable. Different analysts will measure compliance along each factor differently – and will weigh the relative importance of those factors variously (or not at all). Each metric should make clear both how it resolves these questions and why. This not

---

<sup>237</sup> Yemen's two ISPs, for example, filter varying levels of content. Y.Net consistently blocks sites, while YemenNet does so sporadically due to the concurrent user limits of the software license for its BlueCoat filtering technology. OPENNET INITIATIVE, *supra* note 151.

<sup>238</sup> Compare McCullagh, *supra* note 82 (government official denies Internet filtering exists in China), with Andrew Jacobs, *China Angered by U.S. Lobbying on Rights*, N.Y. TIMES, Aug. 1, 2008, available at <http://www.nytimes.com/2008/08/01/sports/olympics/01dissidents.html> (spokesman for Beijing Olympics organizing committee admits China bans sites).

<sup>239</sup> ADVANCE, *Ranking*, at <http://www.advance-project.org/results/ranking/index.html> (last visited July 20, 2008).

<sup>240</sup> JOHANN GRAF LAMBSDORFF, THE METHODOLOGY OF THE CORRUPTION PERCEPTIONS INDEX 2007 2-8 (2007), at <http://www.transparency.org/content/download/23965/358196>.

<sup>241</sup> Cf. ROBERTA ROMANO, THE ADVANTAGE OF COMPETITIVE FEDERALISM FOR SECURITIES REGULATION (2003) (making a similar argument for competition in securities regulation).

only illuminates how censoring states fare when the focus of scrutiny for each factor changes, but also reveals the value sets each rating entity prioritizes.<sup>242</sup>

This is an unusual proposal: achieving greater insight, and comparison among censoring states, by using more than one metric to rate them.<sup>243</sup> There are, though, several key benefits to having multiple, competing metrics. First, quantifying the four principles involves subjective judgments. Analysts will differ, reasonably, on such choices. By making explicit these decisions, metrics can offer a means to assess a state under different tests and, perhaps, to arrive at a consensus view of its practices. Second, competition will press creators to refine and develop their measurements. Demand from non-governmental organizations, state actors, and companies will help elucidate the benefits and shortcomings in each metric. This should cause a winnowing process: as some metrics are widely used, and others ignored, the set of plausible tools for future use will decrease. In addition, the organizations that develop the metrics will be able to re-assess their choices, and how they implement them, by examining those of other entities. It is likely that the World Bank<sup>244</sup> and Freedom House<sup>245</sup> will address issues related to political accountability from which other entities can learn, and that OpenNet Initiative's narrowness criteria will have refinements to offer to other metrics<sup>246</sup>. The metrics should get better, and fewer, over time. This increases the ability to compare results under these different tests.

Finally, adopting an open methodology for measuring filtering is consistent with the framework's focus on process rather than on specifying substantive decisions. Both the framework, and the criteria that rate countries based upon it, are process-based. The framework looks not at the content a country censors, but rather at how it arrives at the decision to filter that material. Similarly, the metrics do not reflect a single view of how to measure accountability or openness, but rely on interaction and competition

---

<sup>242</sup> Cf. Balkin, Noveck, & Roosevelt, *supra* note 41, at 9-10 (discussing how templates that rate Web content reveal preferences).

<sup>243</sup> 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 context).

<sup>244</sup> See, e.g., Daniel Kaufmann, Aart Kraay, & Massimo Mastruzzi, *Governance Matters VII: Aggregate and Individual Governance Indicators 1996-2007* 7-11, 28, 37 (2008), World Bank Policy Research Working Paper No. 4654, available at <http://ssrn.com/abstract=1148386>.

<sup>245</sup> See Freedom House, *Countries at the Crossroads 2007: Survey Methodology*, at <http://www.freedomhouse.org/template.cfm?page=140&edition=8&ccrpage=38> (last visited July 20, 2008).

<sup>246</sup> See, e.g., FARIS & VILLENEUVE, *supra* note 89, at 7-9, 18-22.

to arrive at workable models. This is not the only way to build metrics to measure filtering, but it appears to be the best one.

### *B. Alternatives*

There are paths other than proliferation and competition to produce metrics to measure Internet filtering – most notably, a cooperative effort among stakeholders to produce a consensus tool, or a top-down approach. However, the proposed competitive process appears the most effective: cooperation has proven inadequate thus far, and no one entity has sufficient power to force adoption of its criteria.

A metric produced through collaboration among affected parties and experts on Internet censorship is intuitively appealing: such a tool would be more likely to be broadly accepted, and could reduce or eliminate the time necessary for competing models to coalesce and adapt.<sup>247</sup> It could draw upon the expertise of each party and thus move towards a metric that reflected best practices and avoided past errors. Collaboration, though, suffers two key theoretical shortcomings: selection problems and risk of gridlock. Moreover, current collaborative attempts have dragged on for years, producing only frustration<sup>248</sup> and press releases<sup>249</sup>.

Who would choose the participants in a collaborative effort? Selection reflects subjective values about who is, and is not, appropriate, relevant, and useful. For example, a consensus approach would almost certainly include companies whose financial results might be affected by the metrics they would help develop, such as Microsoft and Google.<sup>250</sup> If China's filtering were to be rated as illegitimate under the new metric, and transactions by technology companies that enable China's censorship attracted heightened scrutiny, Microsoft and Google might be pressured to reduce such business, and hence lose revenue.<sup>251</sup> Indeed, the companies

---

<sup>247</sup> Cf. Fung, *supra* note 70, at 53-54 (describing a “grand consensus” approach to labor standards).

<sup>248</sup> See Arvind Ganesan, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, Testimony to the U.S. Senate Judiciary Committee, Subcommittee on Human Rights and the Law, May 20, 2008, 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”).

<sup>249</sup> Center for Democracy & Technology, *supra* note 37.

<sup>250</sup> See Section IV.C *infra*.

<sup>251</sup> Cf. Nate Anderson, *Rights group, search firms to ink code of conduct for China*, ARS TECHNICA, Mar. 18, 2008, at <http://arstechnica.com/news.ars/post/20080318-rights-group-search-firms-to-ink-code-of-conduct-for-china.html>.

with the most insight to contribute would be those with the greatest conflicts of interest: filtering software companies such as Secure Computing (which supplies Tunisia's censorship system) and Fortinet (which supplies Burma's). Excluding these technology firms would detract from the effort to include all stakeholders; including them would harm its perceived credibility.

A consensus effort could also easily splinter. Those not selected might become disaffected, opting not to recognize or employ the metric, or even developing their own measurement. Moreover, stakeholders dissatisfied with the metric's development could threaten to withdraw as a negotiating tactic or, if sufficiently aggrieved, could depart and launch their own project. (Thus, competition can enter even a collaborative approach.) It might be possible to launch a truly participatory, "open source" project to measure the four criteria, but Internet censorship is a controversial topic, and open source projects often struggle to accommodate divergent views on contested issues.<sup>252</sup> Open source software programs frequently split, or "fork," into multiple, competing versions when these differences prove impossible to reconcile.<sup>253</sup> Consensus can thus dissolve readily.

Even a collaborative effort that does not fork may falter due to gridlock. Members may be unable to choose effective measures or resolve differences of opinion. Some may delay due to strategic behavior – it may be beneficial to appear to work on a tool for evaluating Internet censorship without risking unfavorable analysis based on the final product. The broader the range of participants, the more likely a disagreement is to occur – technology companies, governments, and human rights monitors have divergent goals and normative approaches.

Current efforts to define a code of conduct for technology businesses confronted with freedom of expression and privacy issues suggest these concerns are well-grounded. The consortium working to produce principles has been meeting since 2006 and includes industry

---

<sup>252</sup> Wikipedia, for example, has frequently limited edits to its entry on George W. Bush for this reason. See Stacy Schiff, *Know It All*, NEW YORKER, July 31, 2006, at [http://www.newyorker.com/archive/2006/07/31/060731fa\\_fact](http://www.newyorker.com/archive/2006/07/31/060731fa_fact); Ulrik Brandes & Jürgen Lerner, *Visual analysis of controversy in user-generated encyclopedias*, 7 INFORMATION VISUALIZATION 34 (2008) (noting this page is the most frequently revised in the English-language Wikipedia), available at <http://www.palgrave-journals.com/ivs/journal/v7/n1/full/9500171a.html>.

<sup>253</sup> See, e.g., Paul Adams, *In Response to User Demand, Pidgin Forks*, WIRED, Apr. 22, 2008, at <http://blog.wired.com/monkeybites/2008/04/in-response-to.html> (Pidgin instant-messaging software); Dana Blankenhorn, *Proprietary forks undermine open source purpose*, ZDNET, Jan. 23, 2008, at <http://blogs.zdnet.com/open-source/?p=1923> (DTrace code analysis tool); cf. Jill Coffin, *Analysis of open source principles in diverse collaborative communities*, 11 FIRST MONDAY (June 2006), at [http://www.firstmonday.org/issues/issue11\\_6/coffin/index.html](http://www.firstmonday.org/issues/issue11_6/coffin/index.html) (Burning Man community).

leaders Google, Microsoft, and Yahoo!, but thus far has generated only a press release and criticism from a Senate subcommittee for its glacial progress.<sup>254</sup> According to a participant, the initiative has foundered largely on resistance from some technology companies to independent monitoring of their compliance. This suggests that for some firms, the move to draft consensus standards is intended to deflect attention and criticism rather than to guide behavior.<sup>255</sup> Even assuming good faith participation by members of the working group, the effort to codify principles for dealing with Internet censorship has been slow to develop. Metrics for measuring actual compliance with principles would likely be even more challenging.

Beyond the challenge of convincing reluctant companies to agree to meaningful auditing of their implementation of principles, there are at least two other problems that jeopardize a consensus-driven solution. First, firms face strong pressures to resolve doubts in favor of consummating deals. Corporate governance – at least for companies organized in the U.S. – centers on producing value and profit for shareholders.<sup>256</sup> Companies will accordingly tend to pursue sales where the consensus standards do not clearly forbid them. Second, abstaining from questionable but uncertain deals becomes more difficult in a competitive environment. Another company may resolve its doubts in favor of the sale, reaping the benefit and placing its more virtuous competitor at a disadvantage.<sup>257</sup> This is particularly likely if some companies do not sign on to the proposed standards. Cisco, for example, has not joined the consortium's effort, perhaps because it sees China's filtering as a business opportunity.<sup>258</sup> Western technology companies also face the risk of displacement by domestic producers in some markets, particularly China. That state has

---

<sup>254</sup> See Leslie Harris, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, Statement for the Record Before the Senate Judiciary Committee, Subcommittee on Human Rights and the Law, May 20, 2008, at <http://cdt.org/testimony/20080520harris.pdf>; Martyn Williams, *Chinese internet censorship code of conduct in the works*, WASH. POST, Mar. 18, 2008, at <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/18/AR2008031800978.html>; Frank Davies, *Senators grill tech companies on aiding Chinese censorship*, MERCURY NEWS, May 20, 2008, at [http://www.siliconvalley.com/news/ci\\_9322546?nclick\\_check=1](http://www.siliconvalley.com/news/ci_9322546?nclick_check=1) (quoting Senator Richard Durbin's criticism of the "intolerably slow" process).

<sup>255</sup> See Ganesan, *supra* note 248 (stating a "fundamental problem" with the effort for a code of conduct is "that some companies continue to be very resistant to the idea of independent monitoring... the preferred option for companies is a system in which they will decide who the monitors are and what they will see, while companies implement those standards at a pace convenient to them").

<sup>256</sup> See, e.g., Stephen M. Bainbridge, *Director Primacy: The Means and Ends of Corporate Governance*, 97 NW. U.L. REV. 547, 548-49 (2003).

<sup>257</sup> See, e.g., Zittrain & Palfrey, *supra* note 37, at 119.

<sup>258</sup> See *infra* notes 272–273 and accompanying text.

already moved to develop its own censorship technologies.<sup>259</sup> Market pressures, in short, are likely to drive companies to dilute metrics to enable more transactions to take place or to push them out of the process altogether.

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 would require a sufficiently powerful stakeholder to press for its adoption and use. Using one metric would also facilitate comparison among studies. However, the prerequisite for a single, mandatory filtering metric is lacking: there is no entity with the ability to impose its preferences on other stakeholders. This may be beneficial: any state or organization sufficiently powerful to require use of its criteria for measuring Internet censorship would be strongly tempted to codify its normative preferences regarding filtering into that metric. Measurements propagated by the U.S. government would likely include, even if only implicitly, American views about free expression that would be at odds with Turkish<sup>260</sup> and Thai<sup>261</sup> norms – not to mention Chinese ones.

In the absence of a plenipotentiary power able to dictate a metric, attempts to force a single measurement for filtering legitimacy will probably founder: dissenters can, and will, produce their own criteria. Thus, the two major alternative models 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.

Finally, using competing alternatives to evaluate censorship fits well with the Internet's ethos. Google<sup>262</sup>, TCP/IP<sup>263</sup>, iTunes Music Store<sup>264</sup>, MySpace<sup>265</sup> – each of these leaders or standards emerged from a welter of

---

<sup>259</sup> See, e.g., Nart Villeneuve, *6/4 & Censorware*, at <http://www.nartv.org/2004/06/04/64-censorware/> (June 4, 2004) (describing Filter King and Net Police 110 products).

<sup>260</sup> See, e.g., Thomas Crampton, *Turkey: YouTube Blocked Over Content Found Offensive*, N.Y. TIMES, Mar. 8, 2007, at C7; *Turkey blocks Web site over insults to country's founder*, REUTERS, Mar. 25, 2008, available at [http://www.news.com/2102-1028\\_3-6235481.html](http://www.news.com/2102-1028_3-6235481.html).

<sup>261</sup> See, e.g., *Thai government threatens to shut down 29 websites*, AFP, May 20, 2008, at <http://uk.news.yahoo.com/afp/20080520/ttc-thailand-royals-internet-censor-0de2eff.html>; Seth Mydans, *Agreeing to Block Some Videos, YouTube Returns to Thailand*, N.Y. TIMES, Sept. 1, 2007, at A7.

<sup>262</sup> See Jefferson Graham, *The search engine that could*, USA TODAY, Aug. 26, 2003, at [http://www.usatoday.com/tech/news/2003-08-25-google\\_x.htm](http://www.usatoday.com/tech/news/2003-08-25-google_x.htm).

<sup>263</sup> See Laura Chappell, *Migrating to IP*, NETWORK WORLD, Oct. 18, 1999, at <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).

<sup>264</sup> See Tom Spring, *Digital Music: Worth Buying Yet?*, PC WORLD, Jan. 18, 2002, at <http://www.pcworld.com/article/id,80564-page,1/article.html>.

<sup>265</sup> See Steve Rosenbush, *Hey, Come To This Site Often?*, BUSINESS WEEK, June 13, 2005, at [http://www.businessweek.com/magazine/content/05\\_24/b3937077\\_mz063.htm](http://www.businessweek.com/magazine/content/05_24/b3937077_mz063.htm).

competitors. Even the protocols that form the Net's lingua franca are framed as consensual standards<sup>266</sup>, where usage is voluntary and replacement is commonplace<sup>267</sup>. The Internet itself could be a valuable tool for creating, promulgating, and developing metrics.<sup>268</sup>

While there are plausible alternatives to an open, competitive process for producing metrics to measure filtering, the multilateral approach best fits the Internet's norms and allows the application of multiple approaches to evaluating compliance.

### C. Using the Metrics

Why would metrics to measure filtering's legitimacy be useful, and worth developing?

The metrics' criteria, and the concomitant analyses of various countries' filtering practices, can guide corporate decisions on whether to sell censorship-enabling technology to a given state; government deliberations on regulating such choices through public law; and normative evaluations by private entities and non-governmental organizations. This section explores each issue where the metrics could usefully be applied.

#### 1. Corporate Decisions

Western corporations have stirred controversy over Internet censorship by supplying technology to states that enables them to filter, and by engaging in filtering themselves for services they offer within such states.<sup>269</sup> California-based firm Fortinet sold firewall technology to Burma / Myanmar that lets that country's military dictatorship limit citizens' access to on-line material about human rights, political dissent, and ethnic minority groups.<sup>270</sup> The hardware / software combination also prevents Burmese users from using e-mail services such as Hotmail and Yahoo! Mail – and gives the government the ability to monitor e-mail messages they send from

---

<sup>266</sup> See S. Bradner, *The Internet Standards Process – Revision 3* (Oct. 1996), at <ftp://ftp.rfc-editor.org/in-notes/bcp/bcp9.txt> (noting that the Internet “supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards”).

<sup>267</sup> See, e.g., P. Mockapetris, *Domain Names – Concepts and Facilities [RFC 1034]* (Nov. 1987), at <http://www.ietf.org/rfc/rfc1034.txt?number=1034> (replacing RFC 973, “Domain System Changes and Observations”).

<sup>268</sup> See generally Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369 (2002); Jonathan Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1987-96 (2006).

<sup>269</sup> See Bandurski, *supra* note 72.

<sup>270</sup> OPENNET INITIATIVE, *supra* note 212; Nart Villeneuve, *Fortinet for Who?*, at <http://www.nartv.org/2005/10/13/fortinet-for-who/> (Oct. 13, 2005).

approved accounts.<sup>271</sup> Cisco's routers form a key component of China's censorship system (known colloquially as the "Great Firewall of China").<sup>272</sup> Internal documents reveal not only that Cisco knows China uses its products to censor the Web, but that the company views this practice as a business opportunity.<sup>273</sup> Secure Computing sells its Web filtering software and content classification database to Saudi Arabia, Tunisia<sup>274</sup>, Sudan<sup>275</sup> and Oman<sup>276</sup>; Websense provides its version to Yemen; SurfControl supplies Singapore's Singnet ISP.<sup>277</sup> Google, Yahoo!, and Microsoft operate search engines in China that remove results linking to sites blocked by the Great Firewall.<sup>278</sup> Google's localized French, German, and Canadian search engines similarly de-list hate speech sites.<sup>279</sup> Microsoft's Chinese MSN Spaces blog site prevents users from posting content with certain sensitive keywords, including "democracy" and "demonstration."<sup>280</sup>

While 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 in favor of doing business with South Africa under apartheid.<sup>281</sup> The U.S. Congress has held numerous hearings on corporate participation in state-based Internet censorship<sup>282</sup>, and members such as Representative Christopher Smith have introduced

---

<sup>271</sup> *Id.*

<sup>272</sup> ETHAN GUTMANN, LOSING THE NEW CHINA 130-32, 158-60 (2004).

<sup>273</sup> Glenn Kessler, *Cisco File Raises Censorship Concerns*, WASH. POST, May 20, 2008, at D1; CISCO SYSTEMS, OVERVIEW OF THE PUBLIC SECURITY SECTOR 57-58 (2002) (describing government goals of "Combat[ing] 'Falun Gong' evil religion and other hostiles" and concomitant Cisco business opportunities in technical training, security, and operational maintenance) (copy on file with author).

<sup>274</sup> Ben Arnoldy, *When US-made "censorware" ends up in iron fists*, THE CHRISTIAN SCIENCE MONITOR, Oct. 10, 2007, at <http://www.csmonitor.com/2007/1010/p01s01-ussc.html> (describing Saudi Arabian and Tunisian use).

<sup>275</sup> OPENNET INITIATIVE, SUDAN, at <http://opennet.net/research/profiles/sudan> (May 10, 2007).

<sup>276</sup> OPENNET INITIATIVE, OMAN, at <http://opennet.net/research/profiles/oman> (May 10, 2007).

<sup>277</sup> Xení Jardin, *Exporting Censorship*, N.Y. TIMES, Mar. 9, 2006, at A23.

<sup>278</sup> VILLENEUVE, *supra* note 104.

<sup>279</sup> McCullagh, *supra* note 11; OPENNET INITIATIVE, *supra* note 11; Testimony of Nicole Wong, Deputy General Counsel, Google, Inc., before the U.S. Senate Judiciary Committee Subcommittee on Human Rights and the Law, May 20, 2008, at [http://judiciary.senate.gov/testimony.cfm?id=3369&wit\\_id=7183](http://judiciary.senate.gov/testimony.cfm?id=3369&wit_id=7183).

<sup>280</sup> See, e.g., *Microsoft censors Chinese blogs*, BBC NEWS, at <http://news.bbc.co.uk/1/hi/technology/4088702.stm> (June 14, 2005).

<sup>281</sup> Nate Anderson, *Sen.: Iron Curtain swapped for Virtual Curtain of censorship*, ARS TECHNICA, May 20, 2008, at <http://arstechnica.com/news.ars/post/20080520-sen-iron-curtain-swapped-for-virtual-curtain-of-censorship.html>.

<sup>282</sup> See, e.g., Anne Broache, *Politicos attack tech firms over China*, CNET NEWS.COM, Feb. 1, 2006, at [http://news.cnet.com/2100-1028\\_3-6033976.html](http://news.cnet.com/2100-1028_3-6033976.html).

legislation that would ban such sales<sup>283</sup>. Non-governmental organizations such as Human Rights Watch, Amnesty International, and Reporters Without Borders<sup>284</sup> have attacked sales to censoring countries. Owners of Web sites targeted for blocking have protested, and even offered guides to bypassing censorship.<sup>285</sup> While corporations concede the need for some constraints, they prefer to emphasize self-regulation through voluntary codes of conduct, and inter-governmental efforts to press for openness<sup>286</sup> and to treat filtering as a trade barrier<sup>287</sup>.

Operating in, or trading with, a state that censors on-line content creates conflict: companies have a duty to shareholders to pursue profitable transactions<sup>288</sup>, but their corporate values – and the values of the countries in which they are based – may counsel against such transactions<sup>289</sup>. For example, Microsoft has opted not to locate its Chinese-language Hotmail servers (which provide free e-mail accounts) within China to avoid the risk that the state would demand private user data<sup>290</sup>, even though doing so would lessen the technical problems that occasionally plague Hotmail there<sup>291</sup>. Yahoo!, in contrast, placed the servers for its free e-mail service inside China, making it easier for China's security services to get the company to disclose such information – which has been used to convict and imprison at least four dissidents.<sup>292</sup> The conflict is clear: offering Web services from outside China reduces their performance and hence attractiveness (some Chinese users switched from Hotmail to Google's

---

<sup>283</sup> Global Online Freedom Act of 2007, H.R. 275, 110<sup>th</sup> Congress (2007).

<sup>284</sup> See, e.g., Verena Dobnik, *13 nations denounced for Web censorship*, ASSOC. PRESS, Nov. 8, 2006, available at

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/15955567.htm>.

<sup>285</sup> See, e.g., Jardin, *supra* note 277; *BoingBoing's Guide to Defeating Censorware*, at <http://www.boingboing.net/censorroute.html> (last visited June 12, 2008).

<sup>286</sup> See, e.g., *Tech firms urge Washington to confront China on Net censorship*, SILICONVALLEY.COM, Jan. 30, 2007, at

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/16582624>.

<sup>287</sup> Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J. INT'L LAW 263 (2006).

<sup>288</sup> See, e.g., *Dodge v. Ford Motor Co.*, 170 N.W. 668 (Mich. 1919) (holding corporations are organized for the purpose of shareholder profit, and that directors must pursue this goal).

<sup>289</sup> See *infra* note 295.

<sup>290</sup> Rebecca MacKinnon, *America's Online Censors*, THE NATION, Feb. 24, 2006, at <http://www.thenation.com/doc/20060313/mackinnon>.

<sup>291</sup> Sumner Lemon, *Microsoft restores Hotmail service in China*, INFOWORLD, May 22, 2006, at [http://www.infoworld.com/article/06/05/22/78548\\_HNhotmailchina\\_1.html](http://www.infoworld.com/article/06/05/22/78548_HNhotmailchina_1.html).

<sup>292</sup> HUMAN RIGHTS WATCH, "RACE TO THE BOTTOM": CORPORATE COMPLICITY IN CHINESE INTERNET CENSORSHIP – HOW MULTINATIONAL INTERNET COMPANIES ASSIST GOVERNMENT CENSORSHIP IN CHINA (2006), at <http://www.hrw.org/reports/2006/china0806/5.htm>; *Yahoo! Criticized in Case of Jailed Dissident*, N.Y. TIMES, Nov. 7, 2007, at C3.

Gmail due to outages<sup>293</sup>), but increases the risk that a technology company may assist in political repression.

This tension becomes particularly acute when the filtering state represents an important market (China boasts the greatest number of Internet users of any nation<sup>294</sup>) or when ethical behavior is particularly important to a company (Google's philosophy includes the statement "You can make money without doing evil"<sup>295</sup>). Many information technology companies have a core business function of making information easier to access or locate; 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," the company censors results on the Chinese version of its search engine; indeed, the company on average filters out more results than either Google or Microsoft do for their Chinese sites.<sup>296</sup> How a company behaves, and how it reconciles those choices with its corporate values, is up to each firm. Those decisions, however, will be challenged by observers ranging from activists to government officials. Employing a rigorous, defensible, public methodology will improve a company's ability to justify its actions.

Even the self-regulation method espoused by companies such as Microsoft, Google, and Yahoo! implies that corporations must assess internally whether to sell filtering technology to a given state – and that there are some countries that are not suitable customers. Thus far, firms have not been forthcoming about the standards they employ for these evaluations. (Indeed, the delay in promulgating a set of "best practices" for such questions may represent a tactical move to forestall American legislation on the question.<sup>297</sup>) The four-part analysis this Article proposes, and the metrics that implement it, are well-suited to this assessment.

External pressures may also factor into a company's decisions about restricting information (or aiding a state to do so). Freedom of expression groups have begun to use market pressures to push technology firms to consider such transactions more carefully, including by adopting codes of

---

<sup>293</sup> Sumner Lemon, *Microsoft's Hotmail problems persist in China*, COMPUTERWORLD, May 18, 2006, at [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000605&source=rss\\_topic62](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000605&source=rss_topic62).

<sup>294</sup> See, e.g., Calum MacLeod, *China vaults past USA in Internet users*, USA TODAY, Apr. 20, 2008, at [http://www.usatoday.com/tech/world/2008-04-20-Internetusers\\_N.htm](http://www.usatoday.com/tech/world/2008-04-20-Internetusers_N.htm).

<sup>295</sup> Google, *Corporate Information – Our Philosophy*, at <http://www.google.com/corporate/tenthings.html> (last visited June 22, 2008).

<sup>296</sup> Yahoo! Inc., *Yahoo!: Our Beliefs as a Global Internet Company*, at <http://yhoo.client.shareholder.com/press/ReleaseDetail.cfm?ReleaseID=187401> (last visited June 22, 2008); VILLENEUVE, *supra* note 278 (finding Yahoo! blocked 20.8% of sites tested on average, while Google filtered 15.2% and Microsoft 15.7%).

<sup>297</sup> See generally Ganesan, *supra* note 248.

conduct<sup>298</sup>, factoring human rights explicitly into decisions<sup>299</sup>, and even to forswear censorship altogether<sup>300</sup>. The pressures combine financial incentives (for example, including evaluation of filtering transactions in decisions on whether to invest in a company's stock<sup>301</sup>) with corporate governance measures (such as attempting to mandate consideration of human rights via committees empowered to review a firm's policies<sup>302</sup>) and public relations efforts (such as seeking to embarrass a firm's directors and officers<sup>303</sup>).

There are two risks inherent in using metrics to guide corporate actions: that companies will use this procedure for analyzing transactions as a cover rather than a genuine component of the decision, and that firms will select (or even create) metrics designed to legitimize most if not all potential clients. While real, these concerns can be mitigated. First, using the principles / metrics commits companies to their merit as criteria. It forces firms to defend the content of the metrics used, having conceded the framework's applicability and the desirability of assessing such actions. Some measurement constrains better than none.

Second, outside entities such as watchdog groups can check and challenge corporate conclusions both from an internal perspective (is the transaction justified under the measurements the company used?) and an external one (is that particular metric defensible?). Other companies' decisions, and justifications, will also act as reference points. Finally, there is value in framing the supply of Internet-restricting technology as a

---

<sup>298</sup> See, e.g., Reporters Without Borders, *Joint investor statement on freedom of expression and the Internet*, at <http://www.rsf.org/fonds-investissement-en.php3> (last visited June 25, 2008) (listing 35 investments firms signing a statement of principles that "Call[s] on Internet businesses to adopt and make public ethical codes stressing their commitment to freedom of expression and defining their obligations to uphold these freedoms").

<sup>299</sup> See, e.g., BOSTON COMMON ASSET MANAGEMENT LLC, HUMAN RIGHTS AND INTERNET FRAGMENTATION PROPOSAL RECEIVES RECORD SHAREHOLDER SUPPORT, at <http://www.bostoncommonasset.com/news/cisco-agm-111506.html> (Nov. 15, 2006).

<sup>300</sup> See, e.g., GOOGLE, DEFINITIVE PROXY STATEMENT (SCHEDULE 14A INFORMATION), Proposal Number 4, at [http://sec.gov/Archives/edgar/data/1288776/000119312508064574/ddef14a.htm#rom98719\\_66](http://sec.gov/Archives/edgar/data/1288776/000119312508064574/ddef14a.htm#rom98719_66) (Mar. 25, 2008) (listing shareholder proposal calling on Google "not [to] engage in pro-active censorship").

<sup>301</sup> See, e.g., Calvert, *Issue Brief: Human Rights*, at [http://www.calvertgroup.com/sri\\_IBHumanRights.html](http://www.calvertgroup.com/sri_IBHumanRights.html) (January 2007) (describing Calvert's approach to technology companies involved with China); Reporters Without Borders, *supra* note 298.

<sup>302</sup> *Id.*; see, e.g., GOOGLE, DEFINITIVE PROXY STATEMENT (SCHEDULE 14-A), *Proposal Number 5: Stockholder Proposal*, at <http://sec.gov/Archives/edgar/data/1288776/000119312508064574/ddef14a.htm> (Apr. 6, 2007).

<sup>303</sup> See, e.g., *Chinese Activists Protest Yahoo!*, CNET NEWS.COM, Oct. 19, 2005, at [http://news.cnet.com/2300-1028\\_3-5902094-1.html?part=rss&tag=5902094&subj=news](http://news.cnet.com/2300-1028_3-5902094-1.html?part=rss&tag=5902094&subj=news).

decision requiring analysis, disclosure, and justification. Currently, technology companies are opaque, or even misleading, about their relationships with filtering states.<sup>304</sup> The framework can improve corporate decisions about enabling censorship.

## 2. Public Regulation

Companies have generally resolved debates about supplying filtering technology to censoring states in favor of these transactions, generating controversial calls for governmental regulation to constrain such sales.<sup>305</sup> Firms have variously supported and opposed legal rules governing their behavior.<sup>306</sup> Companies favor legislation as a negotiating tool with foreign states (to the degree they wish to resist pressure to support filtering), but are reluctant to accede to regulation that may bar them from certain markets.<sup>307</sup> Non-governmental organizations and experts line up on both sides of the regulatory question, with some seeing legislation as necessary given the failure of private ordering<sup>308</sup> and others viewing law as too blunt a tool to be useful in this technological context<sup>309</sup>. Similarly, scholars have varying receptivity to legislation regarding Internet censorship, though most

---

<sup>304</sup> See, e.g., Arnoldy, *supra* note 274 (noting Secure Computing refused to confirm transactions with Tunisia, Saudi Arabia, and the United Arab Emirates, and that Fortinet misled researchers about sales to Burma).

<sup>305</sup> See, e.g., Declan McCullagh, *Proposed law targets tech-China cooperation*, CNET NEWS.COM, Feb. 16, 2006, at [http://news.cnet.com/Proposed-law-targets-tech-China-cooperation/2100-1028\\_3-6040303.html](http://news.cnet.com/Proposed-law-targets-tech-China-cooperation/2100-1028_3-6040303.html).

<sup>306</sup> See, e.g., Declan McCullagh, *"Internet freedom" bill targeting China cooperation faces rough road*, CNET NEWS.COM, May 28, 2008, at [http://news.cnet.com/8301-13578\\_3-9952815-38.html](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).

<sup>307</sup> See generally Anne Broache, *Web giants ask for feds' help on censorship*, CNET NEWS.COM, Jan. 30, 2007, at [http://news.cnet.com/Web-giants-ask-for-feds-help-on-censorship/2100-1028\\_3-6154930.html](http://news.cnet.com/Web-giants-ask-for-feds-help-on-censorship/2100-1028_3-6154930.html).

<sup>308</sup> See, e.g., HUMAN RIGHTS WATCH, *supra* note 292, at [http://www.hrw.org/reports/2006/china0806/6.htm#\\_Toc142395831](http://www.hrw.org/reports/2006/china0806/6.htm#_Toc142395831); Amnesty International et al., *NGO Joint Statement in Support of H.R. 275*, at [http://www.amnestyusa.org/Internet\\_Censorship/HR\\_275\\_Support/page.do?id=1081016&n1=3&n2=26&n3=1035](http://www.amnestyusa.org/Internet_Censorship/HR_275_Support/page.do?id=1081016&n1=3&n2=26&n3=1035) (Oct. 19, 2007).

<sup>309</sup> See, e.g., John Palfrey, *Leaked Cisco Document: Chinese Censorship Among "Opportunities,"* at <http://blogs.law.harvard.edu/palfrey/2008/05/22/leaked-cisco-document-chinese-censorship-among-opportunities/> (May 22, 2008) (stating that "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"); Center for Democracy & Technology, *Analysis of the Global Online Freedom Act of 2008 [H.R. 275]*, at <http://www.cdt.org/international/censorship/20080505gofa.pdf> (May 2, 2008); Jonathan Zittrain, *Global Online Freedom Act: Governments Can't Protect Freedom by Themselves*, at <http://futureoftheinternet.org/global-online-freedom-act-governments-cant-protect-freedom-by-themselves> (July 24, 2008).

see private corporate efforts to address the issue as inadequate.<sup>310</sup> In short, whether regulation via public law is desirable at all is contested, let alone the particular provisions of legislation.

Public regulation of technology exports varies, and is particularly challenging for dual-use items. America typically imposes only limited regulation of technology transactions abroad. The country bans most trade to countries seen as state sponsors of terrorism, such as Iran<sup>311</sup>, or as hostile to U.S. interests, such as Cuba<sup>312</sup>, and enforces purpose-specific embargoes on nations such as China<sup>313</sup>. Even these limits have exceptions and uncertainties. Cisco, for example, sells policing 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.<sup>314</sup>

There have been serious proposals for U.S. legislation to regulate how technology companies interact with states that filter the Internet, though none has come close to enactment. Some technology companies favor formal limits on their behavior, albeit weakly<sup>315</sup>, but many companies<sup>316</sup> and commentators<sup>317</sup> (as well as the Bush administration) oppose such steps. The Global Online Freedom Act of 2007, for example, would seek to develop minimum voluntary corporate standards related to Internet freedom; identify Internet-restricting states; prohibit U.S. companies from storing personally identifiable information in those states

---

<sup>310</sup> See, e.g., Surya Deva, *Corporate Complicity in Internet Censorship in China*, 39 GEO. WASH. INT'L L. REV. 255, 309- (2007) (arguing legislation is legitimate to enforce human rights objectives, but that the Global Online Freedom Act is flawed); Mark D. Nawyn, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China*, 2007 COLUM. BUS. L. REV. 505, 544-55 (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 (2006) (describing risks of targeting Internet intermediaries via regulation)

<sup>311</sup> See 31 C.F.R. 560.101 et seq. (2008).

<sup>312</sup> See 31 C.F.R. 515.201-208, 501-577 (2008).

<sup>313</sup> See § 902(a)(4), Foreign Relations Authorization Act for FY 1990-1991, Pub. L. No. 101-246 (suspending export licenses for crime control and detection equipment to China after the Tiananmen Square repression of 1989).

<sup>314</sup> Bambauer, *supra* note 73; Written Testimony of Mark Chandler, Senior Vice President Legal Services, General Counsel and Secretary, Cisco Systems, Inc., before the U.S. Senate Committee on the Judiciary, Subcommittee on Human Rights and the Law, at [http://judiciary.senate.gov/pdf/08-05-20Mark\\_Chandler\\_Testimony.pdf](http://judiciary.senate.gov/pdf/08-05-20Mark_Chandler_Testimony.pdf) (May 20, 2008).

<sup>315</sup> See, e.g., Wong, *supra* note 279 (representing Google).

<sup>316</sup> See, e.g., Anne Broache, *Politicos OK limits for U.S. firms in Net-censoring countries*, CNET NEWS.COM, Oct. 23, 2007, at [http://news.cnet.com/8301-10784\\_3-9802616-7.html](http://news.cnet.com/8301-10784_3-9802616-7.html) (discussing Microsoft and the Computer & Communications Industry Association).

<sup>317</sup> See, e.g., Written statement of John G. Palfrey, Jr. & Colin Maclay, Berkman Center for Internet & Society, Harvard Law School, at <http://blogs.law.harvard.edu/palfrey/2008/05/20/testimony-on-internetfiltering-and-surveillance/> (May 20, 2008).

or from providing such information to Internet-restricting governments; require American-owned search engines to provide the State Department with terms and parameters used to alter search results in these countries; mandate that U.S. companies provide the State Department with URLs filtered in these nations; and ban blocking of U.S. government or government-funded Web content.<sup>318</sup> These constraints would be enforced by substantial civil fines and, for willful violations, criminal penalties. The Act also contemplates expanding the Export Administration Regulations to cover Internet-restricting countries and calls for a feasibility study of this change.<sup>319</sup>

Objections to the Global Online Freedom Act exemplify the challenges of public regulation in this space. The U.S. Department of State argued that the bill's requirements would place American firms at a competitive disadvantage.<sup>320</sup> The Department of Justice raised several concerns: limiting storage of personally identifiable information could cause other countries to exclude U.S. businesses; requiring ISPs to carry information could implicate American free speech protections; defining "Internet-restricting country" as the bill does would likely include states in Western Europe that ban hate speech; prohibiting release of personally identifiable information could trap technology companies between the Act's dictates and foreign state laws requiring information sharing; and, finally, raising the possibility that the U.S. would object if a foreign state sought to regulate the storage of personally identifiable information by companies based in its jurisdiction.<sup>321</sup> These concerns effectively destroy the Act's chances to become law in this Congressional session.<sup>322</sup>

Efforts to limit transactions between Western technology firms and censoring states, like the Global Online Freedom Act, generally encounter resistance along one or more of four fronts. First, argue the companies, information technology is virtually always dual-use: it can be used to further ends both fair and foul.<sup>323</sup> The feature in Cisco's router that lets network administrators block viruses and worms will also prevent access to

---

<sup>318</sup> Global Online Freedom Act of 2007, H.R. 275 (110<sup>th</sup> Congress). See 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).

<sup>319</sup> *Id.* at § 301.

<sup>320</sup> McCullagh, *supra* note 306.

<sup>321</sup> Letter from Brian A. Benzckowski, Principal Deputy Assistant Attorney General, U.S. Dept. of Justice, to The Honorable Howard L. Berman, Acting Chairman, Committee on Foreign Affairs, U.S. House of Representatives, *available at* <http://politechbot.com/docs/doj.letter.gofa.052708.pdf> (May 19, 2008).

<sup>322</sup> Declan McCullagh, *White House opposition likely dooms anti-China Internet bill*, CNET NEWS.COM, May 30, 2008, *at* [http://news.cnet.com/8301-13578\\_3-9956124-38.html](http://news.cnet.com/8301-13578_3-9956124-38.html).

<sup>323</sup> See Bambauer, *supra* note 73.

the BBC or Wikipedia.<sup>324</sup> The SmartFilter software blocks pornography, political sites, and sites that “offer different interpretations of significant historical facts” with equal ease.<sup>325</sup> Thus, companies contend, responsibility is more properly placed upon the user rather than the manufacturer. Second, even if companies participate directly in censorship, they argue that having a limited platform for expression and information exchange is preferable to having no participation at all.<sup>326</sup> Third, firms point to their obligation to conform to local laws: much as U.S. intellectual property law pushes Google to remove search results pointing to sites that infringe copyright, China requires the company to de-list certain opposition political content. This axis of attack carries a hint of a charge of hypocrisy – why should the U.S. complain about censorship when the country engages in its own content restrictions? Finally, companies worry about displacement. If Cisco can’t sell filtering routers to China, the argument goes, then Huawei will rapidly displace them from one of the world’s most lucrative and promising technology markets.

The four-part framework, and the metrics it hopes to generate, can help evaluate two of these four arguments, and by extension the merits of their claims that export regulation should be minimized or prevented. (The other two contentions are beyond the framework’s reach. Whether a state 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% more Web content on controversial topics due to the presence of Google, Microsoft, and Yahoo!<sup>327</sup>) For dual-use, the framework and metrics can predict how a given state will use the technology it procures. Technology firms generally evade the issue of how a state is likely to employ its new capabilities – precisely what the

---

<sup>324</sup> Chandler, *supra* note 314.

<sup>325</sup> See Secure Computing, *SmartFilter Database*, at <http://www.securecomputing.com/index.cfm?skey=86#categories> (last visited June 24, 2008) (describing Pornography, Politics/Opinion, and Historical Revisionism content categories).

<sup>326</sup> See, e.g., Nate Anderson, *Yahoo on China: We’re doing some good*, ARS TECHNICA, May 12, 2006, at <http://arstechnica.com/news.ars/post/20060512-6823.html> (quoting then-Yahoo! CEO Terry Semel); Andrew McLaughlin, *Google in China*, at <http://googleblog.blogspot.com/2006/01/google-in-china.html> (Jan. 27, 2006) (outlining Google’s rationale); Alison Maitland, *Skype says texts are censored in China*, FINANCIAL TIMES, Apr. 18, 2006, at <http://www.ft.com/cms/s/2/875630d4-cef9-11da-925d-0000779e2340.html> (describing Skype CEO’s justification for implementing filter in its Chinese text messaging client).

<sup>327</sup> VILLENEUVE, *supra* note 278 at 2, 16.

framework helps uncover.<sup>328</sup> This predictive approach is used in regulating other dual-use technologies. U.S. law prevents sales of handguns to felons, but not fearful homeowners.<sup>329</sup> Technology companies are liable for products intended or designed to infringe copyrights<sup>330</sup>, but not for those capable of substantial non-infringing uses<sup>331</sup>.

The legitimacy of a sale of dual-use technology can be assessed by examining two factors. First, how is the filtering state likely to employ the new gear? Cisco, for example, had to know that its Policenet system would be used by China not just for crime control, but for political control.<sup>332</sup> The company is not only aware that China uses its routers to censor the Internet, it trumpeted this fact to its internal sales team as a selling point.<sup>333</sup> Second, will the new technology expand the state's capabilities, allowing it to broaden censorship? And is the state inclined to do so? Yemen's filtering goals currently exceed its capacity – one of the state's ISPs uses a Blue Coat WebFilter system but lacks enough concurrent user licenses to block access consistently.<sup>334</sup> Ethiopia blocks some content critical of its government on political or human rights grounds, and would clearly prefer to expand its filtering, but the state-owned ISP lacks the sophistication to do so.<sup>335</sup> Selling a comprehensive filtering solution to Ethiopia would likely mean that the country's evaluation under the four-part framework would worsen. The framework can help evaluate the desirability of sales of dual-use technology without solving the puzzle of whether ultimate responsibility lies with the user or the producer.

Technology companies often reiterate the need to comply with local laws and regulations of the states in which they operate.<sup>336</sup> This position is

---

<sup>328</sup> 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 73; 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).

<sup>329</sup> 18 U.S.C. § 922(d)(1) (2008).

<sup>330</sup> See, e.g., *A&M Records v. Napster*, 239 F.3d 1004 (9<sup>th</sup> Cir. 2001); *Grokster*, 545 U.S. 913.

<sup>331</sup> See, e.g., *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417, 442 (1984).

<sup>332</sup> See, e.g., Rebecca MacKinnon, *More on Cisco in China*, at [http://rconversation.blogs.com/rconversation/2005/06/more\\_on\\_cisco\\_i.html](http://rconversation.blogs.com/rconversation/2005/06/more_on_cisco_i.html) (June 30, 2005); GUTMANN, *supra* note 272, at 167-71.

<sup>333</sup> See *supra* note 273.

<sup>334</sup> OPENNET INITIATIVE, *supra* note 151.

<sup>335</sup> OPENNET INITIATIVE, ETHIOPIA, at <http://opennet.net/research/profiles/ethiopia> (May 9, 2007); see Andrew Heavens, *You block Blogspot, I block Boing Boing*, at [http://www.meskelsquare.com/archives/2007/10/ethiopia\\_blocks.html](http://www.meskelsquare.com/archives/2007/10/ethiopia_blocks.html) (Oct. 8, 2007).

<sup>336</sup> See, e.g., Testimony of Michael Samway, Vice President & Deputy General Counsel, Yahoo! Inc., before the U.S. Senate Judiciary Committee Subcommittee on Human Rights and the Law, at [http://judiciary.senate.gov/testimony.cfm?id=3369&wit\\_id=7182](http://judiciary.senate.gov/testimony.cfm?id=3369&wit_id=7182) (May 20, 2008) (Yahoo!); Matt Marshall, *Microsoft and Bokee mired in Chinese free-speech*

both 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 as much as it frees: it requires that a firm's actions comport with explicit laws or regulations, not merely governmental whim or preference. Companies are often highly responsive to informal government pressures on filtering, not only in China, but also in states such as Britain<sup>337</sup>, Denmark<sup>338</sup>, Sweden<sup>339</sup>, and the U.S.<sup>340</sup> Accountability, openness, and transparency measure the degree to which a state discloses and specifies the grounds for its censorship and the criteria for blocking material. The more clear-cut the basis and standards for filtering, the more readily outside analysts can evaluate whether tech companies are simply following the rules, or whether they are currying favor with potential clients by blocking sensitive content while hiding behind legalistic justifications. Thus, the framework assesses a country's local laws and regulations, and the testing undertaken for the narrowness prong checks how carefully it follows them.

Unilateral limits on American technology firms could merely lead a filtering state to substitute products or services from companies in a country with more lax regulation. Companies might also seek to evade the restrictions through clever restructuring; Yahoo!, for example, runs its operations in China through Alibaba, a Chinese corporation in which Yahoo! owns 40% of the equity.<sup>341</sup> This enables Yahoo! to comply with China's censorship demands while shifting responsibility to Alibaba (which cooperates enthusiastically).<sup>342</sup> In addition, the Justice Department's objection picks up on a potential inconsistency in the U.S. approach: it seeks to hamper Internet censorship by other countries without examining

---

*controversy*, THE MERCURY NEWS, Jan. 4, 2006, at [http://www.siliconbeat.com/entries/2006/01/04/microsoft\\_and\\_bokee\\_mired\\_in\\_chinese\\_freespeech\\_controversy.html](http://www.siliconbeat.com/entries/2006/01/04/microsoft_and_bokee_mired_in_chinese_freespeech_controversy.html) (Microsoft); *Google to censor itself in China*, CNN.COM, Jan. 26, 2006, at <http://www.cnn.com/2006/BUSINESS/01/25/google.china/> (Google); Frank Davies, *Senators grill tech companies on aiding Chinese censorship*, SAN JOSE MERCURY NEWS, May 21, 2008, at [http://origin.mercurynews.com/nationworld/ci\\_9331283](http://origin.mercurynews.com/nationworld/ci_9331283) (Baynote, AeA trade association).

<sup>337</sup> See *supra* notes 127-129 and accompanying text.

<sup>338</sup> *Filter blocks Danes from accessing child pornography*, FINANCIAL MIRROR, Nov. 28, 2005, at [http://www.financialmirror.com/more\\_news.php?id=2574](http://www.financialmirror.com/more_news.php?id=2574).

<sup>339</sup> Telenor, *Telenor and Swedish National Criminal Investigation Department to introduce Internet child porn filter*, at [http://press.telenor.com/PR/200505/994781\\_5.html](http://press.telenor.com/PR/200505/994781_5.html) (May 17, 2005).

<sup>340</sup> See *supra* notes 172 - 178 and accompanying text.

<sup>341</sup> Tom Zeller Jr., *Internet Firms Facing Questions About Censoring Online Searches in China*, N.Y. TIMES, Feb. 15, 2006, at C3.

<sup>342</sup> Stuart Biggs, *Under oath and under pressure*, SOUTH CHINA MORNING POST, Feb. 21, 2006, at 1 (quoting Alibaba's chief executive as saying "We are very co-operative with the authorities").

relevant American practices.<sup>343</sup> Finally, American companies have been able to comply with “local laws” mandating censorship because the applicable legal regimes are tilted towards filtering: blocking material is either required or optional, but there are no affirmative requirements to make information available. The Global Online Freedom Act would change that equilibrium in an interesting but problematic direction by prohibiting American firms from censoring U.S. government materials. Public regulation of censorship could easily confront technology firms with conflicting legal mandates; for example, the United Arab Emirates could extend its blocking of Israel’s top-level domain from a technical constraint to a legal one, and Israel could respond with legislation forbidding companies conducting business in the country from censoring its content.<sup>344</sup> “Must carry” requirements, though still nascent, could pose difficult challenges for tech firms.

Public law regulation of technology companies’ transactions can target the seller, the buyer, or both. Constraining the seller’s behavior limits what one can send abroad – for example, American companies must obtain permission before exporting strong encryption technologies.<sup>345</sup> Limiting buyers prevents firms from transacting with parties in certain states. American law prevents U.S. companies from exporting nearly all goods or services to Cuba without a license from the Department of Commerce (which customarily denies applications),<sup>346</sup> and penalizes foreign firms that do business there if the transaction involves property confiscated by Cuba’s government<sup>347</sup>. The Global Online Freedom Act targets both sides: it dictates how U.S. companies must act (prohibiting filtering of certain sites, and requiring disclosure of lists of blocked sites to the State Department), and limits the states for which these rules apply (regulating practices only in Internet-restricting states).

The objections by the Departments of Justice and State to the Act demonstrate that targeting sellers is much more challenging for regulators. Deciding which states should be eligible to purchase censorship technologies is difficult, but it is easier than dictating what those products and services should be able to do, for three reasons. First, regulating dual-use technology is hard; Cisco is quick to remind critics that its routers

---

<sup>343</sup> Cf. 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 predecessor “hypocritical and arrogant” for this reason).

<sup>344</sup> OpenNet Initiative, *supra* note 44.

<sup>345</sup> 15 C.F.R. § 742.15(b)(2) (2008).

<sup>346</sup> 15 C.F.R. § 742.6 (2008); *see* U.S. DEPARTMENT OF COMMERCE, *Embargoed Countries and Persons*, in FOREIGN POLICY REPORT 2005 (2005), at [http://www.bis.doc.gov/policiesandregulations/05forpolcontrols/chap5\\_embargo.htm](http://www.bis.doc.gov/policiesandregulations/05forpolcontrols/chap5_embargo.htm).

<sup>347</sup> 22 U.S.C. § 6021 et seq.; *see, e.g.*, Adam Liptak, *A Wave of the Watch List, and Speech Disappears*, N.Y. TIMES, Mar. 4, 2008, at A16.

safeguard children from pornography as readily as they censor political speech.<sup>348</sup> Second, such restrictions run counter to the goals of the states that are potential customers, who may pressure companies to evade the regulation or opt for non-U.S. providers. Finally, Internet censorship is relatively dynamic, and public law regulation is relatively static. Even well-crafted laws may rapidly become irrelevant. Regulations designed for Web pages and blogs may struggle with new issues specific to user-generated video (consider YouTube) or text messaging (think Twitter).<sup>349</sup> While this last objection is not fatal, it highlights the difficulty of writing cogent legislation, particularly when it seeks to shape a rapidly shifting technological space.

Regulating buyers makes more sense. Here, the proposed framework can help. The framework's goal is to evaluate how legitimate a state's on-line censorship practices are. The more legitimate the restrictions, the fewer concerns public regulators should have about private firms supporting those activities. Conversely, companies should not enable repressive governments with broad censorship regimes to better control their citizens' information environment. The benefit of the framework is that it provides a yardstick to assess both state and corporate behavior. With a range of metrics, and the concomitant diversity of resulting analysis, regulators such as Congress will have more information to evaluate the extent of the problem (suspect sales, such as Fortinet's to Burma, may be unusual) and, if necessary, to craft a legislative response. Moreover, the framework should help simplify any regulation that develops and, possibly, provide an additional tool to shape censorship practices. For example, it is easier to specify that firms cannot sell filtering technology to Uzbekistan than to define what personally identifiable information they may store in that country.<sup>350</sup> Such restraints may also press countries to engage in more legitimate restrictions.

Buyer-targeted regulation may also offer ancillary benefits such as lower administrative and enforcement costs. For example, American companies cannot lawfully sell software to Iran.<sup>351</sup> Secure Computing has

---

<sup>348</sup> See, e.g., Darren Waters, *Microsoft considers China policy*, BBC NEWS, Nov. 1, 2006, at <http://news.bbc.co.uk/2/hi/technology/6102180.stm> (quoting Cisco senior director Art Reilly).

<sup>349</sup> See generally Ethan Zuckerman, *The Cute Cat Theory Talk at ETech*, at <http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech/> (Mar. 8, 2008) (discussing states' censorship of emerging Web 2.0 technologies and describing a Tunisian video mash-up of Apple's famous "1984" ad used to criticize President Ben Ali); Ryan Singel, *Seeking Tighter Censorship, Repressive States Target Web 2.0 Apps*, WIRED, Mar. 4, 2008, at <http://blog.wired.com/business/2008/03/etech-what-happ.html>.

<sup>350</sup> Cf. Jeffrey Gadmin, *Reporting Among Gangsters*, WASH. POST, July 2, 2008, at A15 (describing media repression in Uzbekistan).

<sup>351</sup> 31 C.F.R. § 560.204 (2008); see, e.g., Sun Microsystems, *Embargoed Countries*, at <http://www.sun.com/sales/its/countries/Embargoed.html> (last visited July 4, 2008).

stated that the SmartFilter software used by Iranian ISPs such as ParsOnline is unauthorized.<sup>352</sup> If the company had sold the product to ParsOnline, the violation would be clear, and relatively inexpensive to detect. (In addition to SmartFilter's characteristic block page, technical experts can "fingerprint" a filtering system to reveal which product it uses.<sup>353</sup>) In contrast, the legality of technology sales to China depends upon the characteristics of the products involved.<sup>354</sup> Whether Cisco's Policenet runs afoul of U.S. export restrictions depends in part on whether Cisco developed the database used by the system, and in part on interpreting whether Policenet is an "identification" system.<sup>355</sup> This determination is not only unclear prospectively, it is a complex question that would be relatively costly to adjudicate. Focusing regulation on the legitimacy of the prospective buyer's censorship is easier for companies to comply with, and cheaper to enforce.

Two additional refinements would bolster the framework approach. First, if Congress (or other public regulators) consider seriously regulating technology sales to filtering states, they should begin by gathering data that would improve policymaking via mandatory, limited disclosure of corporate transactions. For regulators to assess whether public law is necessary, they need sufficient (and sufficiently accurate) information to evaluate the scope of activity they seek to influence. Corporations, though, are loath to provide specifics about sales of filtering technology.<sup>356</sup> Determining this data from public filings, such as those with the Securities and Exchange Commission, or from public statements by company officials can be difficult if not impossible.<sup>357</sup> Thus, it would be beneficial to implement a confidential reporting system.

Crafting the contours of the disclosure system would require care, to avoid collecting irrelevant data (exposing companies to unnecessary cost)

---

<sup>352</sup> OPENNET INITIATIVE, INTERNET FILTERING IN IRAN IN 2004-2005 n.1 (2005), at <http://opennet.net/studies/iran#1>.

<sup>353</sup> See, e.g., OPENNET INITIATIVE, *supra* note 122, at § 4.C.2.c.

<sup>354</sup> See generally Keith Bradsher, *At Trade Show, China's Police Shop for the West's Latest*, N.Y. TIMES, Apr. 26, 2008, available at <http://www.nytimes.com/2008/04/26/business/worldbusiness/26security.html>.

<sup>355</sup> 15 C.F.R. § 742.7(a)(1) (2008) (defining crime control technology subject to regulation); Supp. No. 1 to 15 C.F.R. § 774 (2008) (defining Export Control Classification Number EA981, "automated fingerprint and identification retrieval systems"); see Bambauer, *supra* note 73; MacKinnon, *supra* note 332; see generally 15 C.F.R. § 738.2 (2008).

<sup>356</sup> See, e.g., Arnoldy, *supra* note 274; Bambauer, *supra* note 73 (noting Cisco does not disclose sales figures for China).

<sup>357</sup> Secure Computing, for example, discloses only that 36% of its 2007 revenues came from international sales, and that major foreign markets include China, the Pacific Rim, and the Middle East. SECURE COMPUTING CORPORATION, FORM 10-K, available at [http://edgar.sec.gov/Archives/edgar/data/1001916/000119312508047834/d10k.htm#tx34847\\_8](http://edgar.sec.gov/Archives/edgar/data/1001916/000119312508047834/d10k.htm#tx34847_8) (Mar. 5, 2008).

and to avoid missing relevant transactions (depriving regulators of useful information). Limiting the countries for which sales would have to be reported would be useful. Studying transactions with Mexico, which does not censor the Internet, would not help; capturing data about those with Vietnam would.<sup>358</sup> The reporting system could use one of a number of methodologies to choose which countries to target. Assuming that analysts start to use this Article's framework to assess states' filtering, the system could select countries where on-line restraints fall below certain minima of legitimacy. Alternatively, the State Department could select the countries based on its annual Human Rights Reports<sup>359</sup>, or the system could target states identified as repressing Internet content (for example, by Reporters Without Borders<sup>360</sup>) or with documented instances of Internet filtering (for example, by the OpenNet Initiative<sup>361</sup>).

Some technology is irrelevant to Internet filtering – laptop computers, for example, or Apple's iPhone – and should be excluded from reporting. Defining these technological boundaries could be tricky, especially with “dual use” items. Regulators could either attempt to delineate the characteristics of items or services that must be reported (a dicey task), or could again focus on the buyer. A simple, though admittedly imperfect, rule would mandate submitting data about sales to government agencies or service providers in a state, or about transactions where the reporting entity was itself acting as a service provider.<sup>362</sup> To avoid evasion through cleverly constructed sales channels, as Yahoo!<sup>363</sup> and Fortinet<sup>364</sup> have sought to do, providers could be required to obtain, and report, this data from their distributors or subsidiaries as well.

A disclosure requirement – however limited – is likely to be opposed by technology companies. (For example, past attempts to require disclosure of transactions with “terrorist-sponsoring states,”<sup>365</sup> or of

---

<sup>358</sup> OPENNET INITIATIVE, LATIN AMERICA, at <http://opennet.net/research/regions/la> (last visited July 2, 2008).

<sup>359</sup> U.S. Department of State, *Human Rights*, at <http://www.state.gov/g/drl/rls/hrrpt/> (last visited June 21, 2008).

<sup>360</sup> Reporters Without Borders, *Internet Enemies*, at [http://www.rsf.org/article.php3?id\\_article=26082](http://www.rsf.org/article.php3?id_article=26082) (last visited July 2, 2008) (listing countries that are “Internet Enemies” or are “Under Surveillance” for suspect practices).

<sup>361</sup> OpenNet Initiative, *Research*, at <http://opennet.net/research>; ACCESS DENIED, *supra* note 7.

<sup>362</sup> Regulation could incorporate the definition of “service provider” from the Digital Millennium Copyright Act. See 17 U.S.C. § 512(k)(1) (2008).

<sup>363</sup> See *supra* note 342 and accompanying text.

<sup>364</sup> See Villeneuve, *supra* note 270; Arnoldy, *supra* note 274.

<sup>365</sup> See, e.g., Floyd Norris, *S.E.C. Rethinks Lists Linking Companies and Terrorist States*, N.Y. TIMES, July 21, 2007, at C2.

potential environmental liabilities<sup>366</sup>, elicited substantial corporate opposition, and a current petition before the U.S. Securities and Exchange Commission to mandate inclusion of climate change risks in corporate filings has met mixed reaction from companies and investment firms.<sup>367</sup>) There are analogous programs, though, designed to improve public regulation that suggest this reporting system need not be onerous or risky for firms. For example, the National Practitioner Data Bank (NPDB) collects information about civil judgments – including settlements – and criminal convictions against physicians and health care providers for malpractice.<sup>368</sup> Insurers and other payers must report settlement data to the NPDB.<sup>369</sup> The general public cannot access these records, but regulators such as state licensing boards, professional societies, and federal agencies can.<sup>370</sup> Federal agencies have used this data to analyze such regulatory questions as the role of malpractice insurance premiums in the rise in health care costs<sup>371</sup>, and legislators have evaluated NPDB information in considering limits on damages in medical malpractice lawsuits<sup>372</sup>. Despite ongoing pressure from lawyers and activists<sup>373</sup>, NPDB records remain off-limits to the public<sup>374</sup>. Thus, regulators gain access to data otherwise

---

<sup>366</sup> See, e.g., Barnaby J. Feder, *New Battles Over Disclosure*, N.Y. TIMES, June 24, 1990, available at <http://query.nytimes.com/gst/fullpage.html?res=9C0CE3D6123CF937A15755C0A966958260>; William Baue, *SEC Urged to Strengthen Rules Governing Corporate Disclosure of Environmental Risks*, at <http://www.socialfunds.com/news/article.cgi/911.html> (Aug. 21, 2002).

<sup>367</sup> See Request for Interpretive Guidance on Climate Risk Disclosure (File No. 4-547), available at <http://www.sec.gov/rules/petitions/2007/petn4-547.pdf> (Sept. 18, 2007); U.S. Securities and Exchange Comm'n, *Comments on Rulemaking Petition: Request for Interpretive Guidance on Climate Risk Disclosure*, at <http://www.sec.gov/comments/4-547/4-547.shtml> (last modified June 12, 2008); Steven Mufson, *SEC Pressed to Require Climate-Risk Disclosures*, WASH. POST, Sept. 18, 2007, at D1.

<sup>368</sup> Health Care Quality Improvement Act of 1986, Title IV, Pub. L. 99-660, 100 Stat. 3784 (codified as amended at 42 U.S.C. § 11101 et seq.); see U.S. Dept. of Health & Human Services, *National Practitioner Data Bank*, at <http://www.npdb-hipdb.hrsa.gov/npdb.html> (last visited July 2, 2008).

<sup>369</sup> 42 U.S.C. § 11131 (2008).

<sup>370</sup> 42 U.S.C. § 11137 (2008).

<sup>371</sup> U.S. GENERAL ACCOUNTING OFFICE, *MEDICAL MALPRACTICE: IMPLICATIONS OF RISING PREMIUMS ON ACCESS TO HEALTH CARE* (Aug. 2003), available at <http://www.gao.gov/new.items/d03836.pdf>.

<sup>372</sup> See, e.g., Richard A. Opiel, Jr., *Bush Enters Fray Over Malpractice*, N.Y. TIMES, Jan. 17, 2003, at A24 (citing NPDB data on average malpractice judgment awards).

<sup>373</sup> See, e.g., Sidney M. Wolfe, *Bad Doctors Get a Free Ride*, N.Y. TIMES, Mar. 4, 2003, at A25.

<sup>374</sup> See, e.g., DEPT. OF HEALTH & HUMAN SERVICES, *NATIONAL PRACTITIONER DATA BANK / HEALTHCARE INTEGRITY AND PROTECTION DATA BANK: FACT SHEET FOR THE GENERAL PUBLIC* (May 2008), available at [http://www.npdb-hipdb.hrsa.gov/pubs/fs/Fact\\_Sheet-General\\_Public.pdf](http://www.npdb-hipdb.hrsa.gov/pubs/fs/Fact_Sheet-General_Public.pdf).

unavailable (settlement agreements are typically confidential), while participants (who may have settled a suit for economic reasons rather than because of fault) remain shielded from public scrutiny. There are similar systems for reporting storage of toxic chemicals<sup>375</sup> and “near miss” aviation safety incidents<sup>376</sup>. Disclosure of transactions involving censorship technology or services with states that filter the Internet would improve regulators’ ability to determine the extent to which such sales are problematic, and to construct appropriate legislation should it be necessary. Confidentiality would protect companies from reputational harm or civil suits, reducing their opposition and making the project more viable politically.

Second, there may be edge cases where a state’s censorship practices are either on the borderline of what regulators consider acceptable or, while generally unoffensive, seem specifically problematic in some aspect. In this instance, it might be beneficial to also regulate the selling company’s behavior, though at the cost of expanded legislation or rules tailored to individual countries. One example might be Singapore. The country’s Web filtering regime is relatively minimal and focused; it bans only a few, symbolic pornography sites under its “light touch” approach, though the state claims the authority to block more.<sup>377</sup> However, the state’s principal tool to quash political dissent is legal: defamation lawsuits. Bloggers are frequent targets<sup>378</sup>, and can suffer substantial monetary penalties<sup>379</sup>, as well as the loss of freedom to travel<sup>380</sup>. The U.S. government likely would not worry about companies selling filtering technology to Singapore’s government or ISPs, but would probably be concerned about firms offering blog hosting, with data identifying individual bloggers

---

<sup>375</sup> 42 U.S.C. § 11023 (2008); 40 C.F.R. § 372.1 et seq. (2008); *see generally* U.S. Environmental Protection Agency, *What is the Toxics Release Inventory (TRI) Program*, at <http://www.epa.gov/tri/triprogram/whatis.htm> (last updated Mar. 31, 2008). Toxics data is publicly available, though. *See generally* MARY GRAHAM, *DEMOCRACY BY DISCLOSURE* 21-61 (2002).

<sup>376</sup> Nat’l Aeronautics & Space Administration (NASA), *ASRS – Aviation Safety Reporting System*, at <http://asrs.arc.nasa.gov/overview/summary.html> (last visited July 2, 2008). While incident reports to the ASRS are voluntary, they are confidential, and policymakers employ them in crafting regulations. NASA, *ASRS: THE CASE FOR CONFIDENTIAL INCIDENT REPORTING SYSTEMS* (2001), at [http://asrs.arc.nasa.gov/docs/rs/60\\_Case\\_for\\_Confidential\\_Incident\\_Reporting.pdf](http://asrs.arc.nasa.gov/docs/rs/60_Case_for_Confidential_Incident_Reporting.pdf).

<sup>377</sup> OPENNET INITIATIVE, *supra* note 125.

<sup>378</sup> *See, e.g.*, Melissa Lwee, *Singapore: Blogger says, Sorry again A\*Star*, STRAITS TIMES, May 10, 2005, available at <http://www.asiamedia.ucla.edu/article.asp?parentid=24127>; REPORTERS WITHOUT BORDERS, *SINGAPORE – ANNUAL REPORT 2007* (2007), at [http://www.rsf.org/country-50.php3?id\\_mot=265&Valider=OK](http://www.rsf.org/country-50.php3?id_mot=265&Valider=OK).

<sup>379</sup> Mydans, *supra* note 195.

<sup>380</sup> Patrick May, *Fremont blogger held in Singapore*, MERCURY NEWS, June 24, 2008, at [http://www.siliconvalley.com/news/ci\\_9681300?nclick\\_check=1](http://www.siliconvalley.com/news/ci_9681300?nclick_check=1).

physically stored on servers in Singapore. Here, it might be appropriate to regulate firms in addition to identifying the target country – perhaps offering a choice between storing data outside Singapore or requiring minimization of information retained about blog authors and readers.

Regulating information technology is challenging both politically and as a matter of legislative drafting. This Article's four-part framework can help regulators determine whether public law constraints on corporate transactions with censoring states are necessary. It also suggests that focusing on states as buyers – by evaluating their filtering practices – can helpfully avoid some of the drafting challenges encountered in existing legislation such as the Global Online Freedom Act. Again, whether to regulate corporate behavior is a normative choice: regulators could seek to block all transactions with censoring states, or only those where Western technology is critical to the filtering regime's functionality, or permit unfettered trade. The framework seeks to improve the process of regulatory deliberation and to refine its end product, not to define a normative endpoint for that process.

### 3. Third-Party Evaluation

Filtering opens a state to external critiques of its practices – from Slashdot discussions<sup>381</sup> to State Department reports<sup>382</sup> to press freedom analysis<sup>383</sup> to United Nations evaluations<sup>384</sup>. Internet censorship has received increased attention in recent years from entities such as the U.S. Department of State.<sup>385</sup> These third-party assessments are of varying quality and employ different methodologies – from legal probes of the bases for a country's censorship<sup>386</sup> to limited quantitative analysis<sup>387</sup> to careful

---

<sup>381</sup> See, e.g., kdawson, *Three ISPs Agree to Block Child Porn*, SLASHDOT, June 10, 2008, at <http://yro.slashdot.org/article.pl?sid=08/06/10/1819200>.

<sup>382</sup> See U.S. Department of State, *supra* note 359.

<sup>383</sup> See, e.g., REPORTERS WITHOUT BORDERS, ANNUAL REPORT 2007: DICTATORSHIPS GET TO GRIPS WITH WEB 2.0, at [http://www.rsf.org/article.php3?id\\_article=20844](http://www.rsf.org/article.php3?id_article=20844) (last visited June 21, 2008).

<sup>384</sup> See, e.g., UNITED NATIONS HUMAN RIGHTS COUNCIL, REPORT OF THE WORKING GROUP ON THE UNIVERSAL PERIODIC REVIEW – TUNISIA 10, 12 (2008) (discussing Tunisia's Internet controls).

<sup>385</sup> Bradley Graham, *Violence Said to Slow Rights Effort in Iraq: Report Lauds Steps Toward Democracy*, WASH. POST, Mar. 9, 2006, at A15 (quoting assistant secretary for human rights on “growing attention to government censorship of the Internet” in State Department evaluations).

<sup>386</sup> See, e.g., Human Rights Watch, *Human Rights and the 2008 Olympics in Beijing: Media and Internet Censorship*, at <http://www.hrw.org/campaigns/china/beijing08/censorship.htm> (last visited July 9, 2008) (analyzing Chinese laws used to regulate journalism and Internet posts).

empirical testing<sup>388</sup>. While this diversity can paint a more fulsome picture of an individual state, it makes cross-country comparison challenging. (Indeed, it can complicate assessing any single state, as different groups emphasize various factors: Venezuela does not filter, but its overall media restrictions<sup>389</sup> and informal pressures on independent journalists<sup>390</sup> limit freedom of expression on the Net there<sup>391</sup>.) By using a process-oriented methodology, third parties can take different normative positions on filtering, and on how a given country implements it; simultaneously, such an approach increases the rigor of their assessments and improves the ability to compare, for example, Saudi Arabia's system to that of Iran. With a consistent approach that looks at the behavior of the filtering state, third parties can also adduce stronger reasons for supporting or criticizing corporate choices in supplying censorship technology.

External evaluations of a state's censorship practices face at least two challenges. First, the state may simply (and, perhaps, plausibly) claim that its filtering serves to prevent social harms and is thereby justified.<sup>392</sup> Second, the country may critique its critics, seeking to show that they too engage in the practices described and consequently are hypocritical.<sup>393</sup> China, for example, 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 and to America's surveillance of international communications.<sup>394</sup> Such responses can achieve two ends: mitigating the force of negative analysis by showing that questionable practices are widespread, and reducing a critic's credibility by showing it has also engaged in suspect activities.<sup>395</sup> In the filtering context, countries such as

<sup>387</sup> See, e.g., Reporters Without Borders, *Test of filtering by Sohu and Sina search engines following upgrade*, at [http://www.rsf.org/article.php3?id\\_article=18015](http://www.rsf.org/article.php3?id_article=18015) (June 22, 2006); but see VILLENEUVE, *supra* note 278, at 21 (describing problems with the study's methodology).

<sup>388</sup> See, e.g., OPENNET INITIATIVE, *supra* note 120.

<sup>389</sup> See, e.g., Human Rights Watch, *Venezuela: TV Shutdown Harms Free Expression*, at <http://hrw.org/english/docs/2007/05/22/venezu15986.htm> (May 22, 2007).

<sup>390</sup> 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.

<sup>391</sup> OPENNET INITIATIVE, VENEZUELA, at <http://opennet.net/research/profiles/venezuela> (May 9, 2007).

<sup>392</sup> See *supra* note 92 (documenting Vietnamese claims regarding censorship).

<sup>393</sup> Cf. David J. Rothkopf, *Values Conundrum: Will the U.S. and China Play by the Same Rules?*, WASH. POST, July 11, 2005, at A15 (comparing controversies over U.S. technology companies' activities in China with U.S. resistance to Unocal's sale to a Chinese firm).

<sup>394</sup> See, e.g., Calum MacLeod, *China: U.S. criticism of human rights record is "hypocrisy"*, USA TODAY, Mar. 10, 2006, at 9A.

<sup>395</sup> 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 American criticism of Pakistan, Egypt, and Syria for methods the U.S. has employed when interrogating captives).

China frequently advert to other states' practices of preventing access to on-line material and portray their efforts as similar.<sup>396</sup>

The framework can avoid these issues by offering a consistent method to rate states' practices. This would improve the coherence of third-party analysis. There are a number of 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, the U.N. Human Rights Council, the International Council on Human Rights Policy, Freedom Watch, the Committee to Protect Journalists, and others. They approach Internet censorship with a range of methodologies, from evaluating it as part of a holistic picture of human rights (for example, the U.S. State Department's annual Human Rights Reports) to a specific focus on the subject (for example, Reporters Without Borders' annual Internet Enemies list and OpenNet Initiative's ongoing studies of filtering). Employing the framework would augment these organizations' existing approaches while improving the ability to compare their analyses or to aggregate them.

For example, Reporters Without Borders (RSF<sup>397</sup>) classifies states it regards as violating freedom of expression or the press on-line as either Internet Enemies or Under Surveillance.<sup>398</sup> At the extremes, it is difficult to quarrel with RSF's sorting: North Korea's Internet censorship trumps that of Jordan. But the organization's methodology is less clear in the middle range. What makes Egypt's on-line controls<sup>399</sup> (Internet Enemy) worse than those of Tajikistan<sup>400</sup> (Under Surveillance)? (In contrast, OpenNet Initiative finds that Egypt does not filter, although bloggers and on-line journalists have been imprisoned or harassed by government officials<sup>401</sup>; Tajikistan engages in selective political filtering, with moderate transparency but low

---

<sup>396</sup> See, e.g., Joseph Kahn, *China defends Internet censorship*, INT'L HERALD TRIBUNE, Feb. 15, 2006, at <http://www.iht.com/articles/2006/02/14/business/net.php> (quoting a Chinese official in the Information Office of the Chinese State Council that "If you study the main international practices in this regard, you will find that China is basically in compliance with the international norm").

<sup>397</sup> Reporters Without Borders is better known as Reporters Sans Frontières (RSF); the organization is based in France.

<sup>398</sup> Reporters Without Borders, *Internet*, at [http://www.rsf.org/rubrique.php?id\\_rubrique=273](http://www.rsf.org/rubrique.php?id_rubrique=273) (last visited Aug. 14, 2008).

<sup>399</sup> Reporters Without Borders, *Internet Enemies – Egypt*, at [http://www.rsf.org/rubrique.php?id\\_rubrique=273](http://www.rsf.org/rubrique.php?id_rubrique=273) (last visited July 4, 2008).

<sup>400</sup> Reporters Without Borders, *Countries Under Surveillance – Tajikistan*, at [http://www.rsf.org/article.php?id\\_article=26127&Valider=OK](http://www.rsf.org/article.php?id_article=26127&Valider=OK) (last visited July 4, 2008).

<sup>401</sup> OPENNET INITIATIVE, EGYPT, at <http://opennet.net/research/profiles/egypt> (May 9, 2007).

consistency<sup>402</sup>.) RSF's assessments of Internet content control would be improved by a consistent methodology that does not depend on what material is restricted and that reveals how RSF classifies countries. (RSF includes other factors, such as the ability of journalists to conduct their craft, in its evaluations<sup>403</sup>; this Article's methodology applies only to its analysis of on-line content restrictions.) The framework is well-positioned to perform this task.

Finally, if third-party analysts moved towards convergent criteria for measuring Internet censorship (even if they differed in how they assessed these criteria, or weighted them relative to one another), it would be easier to compare – and critique – their evaluations. Freedom House and OpenNet Initiative both describe how they rate states (Freedom House, for press freedom generally<sup>404</sup>; ONI, for Internet filtering<sup>405</sup>). Thus, one can compare Freedom House's relatively negative evaluation of Oman (ranking it as Not Free, and placing it 165<sup>th</sup> of 195 countries) with ONI's relatively positive one (finding Oman has highly transparent and consistent filtering).<sup>406</sup> It is possible to reconstruct these conclusions based on each organization's methodology, and to see how the differences result from the varying analytical focus. Oman suppresses little speech technologically (ONI), but much expression via legal, economic, and informal pressures (Freedom House).

One criticism of this suggestion is that it assumes away the problem: it would obviously improve the ability to compare third-party reports if they shared a methodology, but the difficulty lies in convincing organizations with different goals and values to adopt the same system. This is partly correct: some evaluators might not be concerned with accountability, for example, or might ground their analysis on different principles entirely. There are two reasons for optimism, though. First, because it is process-focused, this Article's framework is compatible with a wide range of views on content restrictions – it tries to clarify what restraints exist, and how they are determined, without taking a position on the limits themselves. Second, analysts and commentators frequently advert to the criteria used in the framework.<sup>407</sup> Openness, transparency, narrowness, and accountability

---

<sup>402</sup> OPENNET INITIATIVE, TAJIKISTAN, at <http://opennet.net/research/profiles/tajikistan> (May 9, 2007).

<sup>403</sup> See, e.g., Reporters Without Borders, *supra* note 399, at n.\*\* (describing methodology).

<sup>404</sup> FREEDOM HOUSE, FREEDOM OF THE PRESS – 2007 EDITION: METHODOLOGY (2007), at [http://www.freedomhouse.org/template.cfm?page=350&ana\\_page=339&year=2007](http://www.freedomhouse.org/template.cfm?page=350&ana_page=339&year=2007).

<sup>405</sup> Faris & Villeneuve, *supra* note 89, at 5-27.

<sup>406</sup> Compare FREEDOM HOUSE, OMAN (2007), at <http://www.freedomhouse.org/template.cfm?page=251&country=7246&year=2007> with OPENNET INITIATIVE, *supra* note 209.

<sup>407</sup> See, e.g., VILLENEUVE, *supra* note 278 (transparency, accountability); Joint Declaration of the OSCE Representative on Freedom of the Media & Reporters Sans Frontières on

capture the most commonly expressed criteria, principles, or values used as reference points in analyzing Internet content restrictions. This increases the likelihood that the framework will be broadly acceptable to those who assess filtering.

Finally, this section on third-party evaluation has assumed to this point that outside groups play the role of critics: they assess a state's filtering and critique it, or the companies that contribute to it. There is an alternative, though. Organizations could create a set of minimum standards or best practices for filtering and then confer recognition – their “seal of approval” – on states that meet these requirements, and on technology companies that engage in transactions only with such states. This approval or certification approach has many analogues in other areas of regulation. Web sites can obtain certification from groups such as the Better Business Bureau<sup>408</sup> and Truste<sup>409</sup> 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 certain environmental and economic requirements.<sup>410</sup> Energy-efficient products, such as computers<sup>411</sup> and new homes<sup>412</sup>, can earn an Energy Star from the U.S. Department of Energy and the U.S. Environmental Protection Agency to display to consumers. Forest products, such as paper and wood, and the

Guaranteeing Media Freedom on the Internet, *at*

[http://www.rsf.org/IMG/pdf/declaration\\_anglais.pdf](http://www.rsf.org/IMG/pdf/declaration_anglais.pdf) (June 18, 2005) (accountability);

Human Rights Watch, *supra* note 292, *at*

[http://www.hrw.org/reports/2006/china0806/7.htm#\\_Toc142395835](http://www.hrw.org/reports/2006/china0806/7.htm#_Toc142395835) (transparency);

FREEDOM HOUSE, *id.* (accountability, openness); OPENNET INITIATIVE, ASIA, *at*

<http://opennet.net/research/regions/asia> (last visited Aug. 18, 2008) (openness,

narrowness); U.S. DEPT. OF STATE, *supra* note 39, *at*

<http://www.state.gov/g/drl/rls/hrrpt/2007/100464.htm> (accountability, openness); ACCESS

DENIED, *supra* note 7, at 115-16, 238 (accountability, narrowness, transparency); Balkin,

Noveck, & Roosevelt, *supra* note 41, at 4-9 (transparency, accountability).

<sup>408</sup> Better Business Bureau, *BBBOnline*, *at*

<http://us.bbb.org/WWWRoot/SitePage.aspx?site=113&id=12e4909f-f815-49a4-ab22-a9f55813c3cd> (last visited July 14, 2008).

<sup>409</sup> TRUSTe, *Make Privacy Your Choice*, *at*

[http://www.truste.org/businesses/web\\_privacy\\_seal.php](http://www.truste.org/businesses/web_privacy_seal.php) (last visited July 14, 2008); *but see*

Ben Edelman, *Certifications and Site Trustworthiness*, *at*

<http://www.benedelman.org/news/092506-1.html> (Sept. 25, 2006) (finding 5.4% of

TRUSTe's certified sites are labeled untrustworthy by SiteAdvisor, versus 2.5% of sites listed overall).

<sup>410</sup> See TransFair USA, *Fair Trade Certification Overview*, *at*

<http://www.transfairusa.org/content/certification/overview.php> (last updated Jan. 29, 2008).

<sup>411</sup> Energy Star, *Computer Specification*, *at*

[http://www.energystar.gov/index.cfm?c=revisions.computer\\_spec](http://www.energystar.gov/index.cfm?c=revisions.computer_spec) (last visited July 14, 2008).

<sup>412</sup> Energy Star, *ENERGY STAR Qualified Homes*, *at*

[http://www.energystar.gov/index.cfm?c=bldrs\\_lenders\\_raters.pt\\_bldr](http://www.energystar.gov/index.cfm?c=bldrs_lenders_raters.pt_bldr) (last visited July 14, 2008).

land management that produces them, can obtain certification from monitors accredited by the Forest Stewardship Council; these certifiers implement the FSC's criteria and standards, but employ their own methodology for evaluating compliance.<sup>413</sup> The goal is to provide positive incentives for companies to engage in desired behaviors, as well as negative incentives to avoid unfavorable ones. If consumers seek to purchase from companies that are demonstrably environmentally-friendly or privacy-conscious, certifications or labels from trusted third parties help them locate such vendors and differentiate them from competitors.<sup>414</sup> In effect, the rating entity lends its prestige to the company it certifies. Similarly, filtering certifications could be touted by states in international fora (such as the Internet Governance Forum) or by companies when criticized by activists.

Seals of approval for filtering states, or companies assisting them, will likely encounter at least two objections. First, some commentators will disapprove of conferring legitimacy upon on-line censorship. This position, while defensible, runs counter to strong support in many countries for restricting access to certain material. Moreover, that public support means states are likely to engage in censorship; the goal of certification is to press them to do so with maximal legitimacy.

Second, states and companies will probably turn to – or create – friendly rating entities to award them certification on easy terms. This may be particularly problematic during the early phase of evaluation, when third-party observers may have not yet established sufficient recognition or credibility to counteract this technological “greenwashing.”<sup>415</sup> If consumers or other observers look merely for a label, rather than its backer, this tactic can succeed.<sup>416</sup> However, this problem can be mitigated. Organizations with credible reputations, such as Human Rights Watch or the Center for Democracy & Technology, can leverage existing recognition in the new zone of filtering classification. 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.<sup>417</sup> It signifies a shift in expectations about

---

<sup>413</sup> The Forest Stewardship Council, *What is “certification”?*, at [http://www.fscus.org/faqs/what\\_is\\_certification.php](http://www.fscus.org/faqs/what_is_certification.php) (last visited Aug. 8, 2008).

<sup>414</sup> See Eric Pfanner, *Cooling Off on Dubious Eco-Friendly Claims*, N.Y. TIMES, July 18, 2008, at C3 (noting consumers have become skeptical of misleading claims of environmental friendliness).

<sup>415</sup> See, e.g., TerraChoice, *The “Six Sins of Greenwashing,”* at [http://www.terrachoice.com/files/6\\_sins.pdf](http://www.terrachoice.com/files/6_sins.pdf) (Nov. 2007); 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).

<sup>416</sup> But see Pfanner, *supra* note 414.

<sup>417</sup> 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).

acceptable behavior. Similarly, even weak certifications commit companies to the principle that legitimacy in censorship is uncertain, and that their decisions to support it are properly subject to outside review.

#### 4. Metrics As Guides

Metrics based on this Article's framework can help with three challenging problems: how corporations decide whether to help a state censor the Internet; whether a country with a strong technology sector should use public law to regulate those decisions; and how third parties should evaluate a state's filtering in a defensible, rigorous, reproducible, and comparable way. While not a panacea, the framework is a useful tool to tackle each challenge.

### V. CHALLENGES AND LIMITATIONS

There are three important challenges that complicate application of the framework and its metrics: circumvention, interdependence, and the China quandary.

First is circumvention. Circumvention covers a panoply of technological methods that bypass on-line censorship.<sup>418</sup> With a tool such as Anonymizer, an Internet user can reach material that would otherwise be blocked.<sup>419</sup> Circumvention includes using proxy servers to fetch prohibited material on one's behalf<sup>420</sup>, routing requests through specialized unfiltered network nodes such as Tor<sup>421</sup>, and accessing blocked pages from a search engine's cache<sup>422</sup>. Falun Gong practitioners, for example, have developed sophisticated software tools to enable Chinese users to breach the Great Firewall, motivated partly by China's heavy filtering of Falun Gong content.<sup>423</sup> Circumvention is typically praised as on-line civil disobedience – technological resistance to unjustified limits on information.<sup>424</sup>

<sup>418</sup> See generally CITIZEN LAB, EVERYONE'S GUIDE TO BY-PASSING INTERNET CENSORSHIP (Sept. 2007), at <http://citizenlab.org/CL-circGuide-online.pdf>.

<sup>419</sup> See generally *id.*; Anonymizer, *Frequently Asked Questions*, at <http://www.anonymizer.com/company/about/anonymizer-faq.html> (last visited Aug. 14, 2008).

<sup>420</sup> See, e.g., *Psiphon*, available at <http://psiphon.civisec.org/>.

<sup>421</sup> *Tor: anonymity online*, at <http://www.torproject.org/>.

<sup>422</sup> See, e.g., OPENNET INITIATIVE, GOOGLE SEARCH & CACHE FILTERING BEHIND CHINA'S GREAT FIREWALL (Aug. 30, 2004), at <http://opennet.net/bulletins/006>.

<sup>423</sup> See *Testimony of Shiyu Zhou, Ph.D.*, before the Senate Committee on the Judiciary, Subcommittee on Human Rights and the Law, May 20, 2008, at [http://judiciary.senate.gov/testimony.cfm?id=3369&wit\\_id=7187](http://judiciary.senate.gov/testimony.cfm?id=3369&wit_id=7187) (describing FreeGate and UltraSurf programs); OPENNET INITIATIVE, *supra* note 82 (documenting filtering).

<sup>424</sup> See, e.g., Wiseman, *supra* note 146; Tom Zeller, Jr., *How to Outwit the World's Internet Censors*, N.Y. TIMES, Jan. 29, 2006, at 2.

Circumvention's legitimacy, though, depends upon one's assessment of the filtering it subverts. Empowering Internet users to share information about democracy seems inspiring; enabling users to trade child pornography seems disturbing.<sup>425</sup> Circumvention, like filtering, cuts both ways: it permits users to bypass all content restrictions. (Attempts to limit circumvention to facilitate access only to favored content have failed, sometimes embarrassingly. The U.S. offered Iranian and Chinese users a bowdlerized version of Anonymizer that blocked access to sites with the words "gay" or "teen" in their addresses, but failed to encrypt the service's communications, potentially exposing users to state surveillance of their on-line activity.<sup>426</sup>)

This suggests that, like corporations offering technology to filter Internet content, individuals and organizations who distribute circumvention tools should evaluate a state's censorship regime before enabling its citizens to bypass it. If a country's decision to block access to certain material qualifies as legitimate, then helping that nation's users to evade restrictions should be criticized, not celebrated. For example, if the United States passes legislation to block children's access to sites selling controlled substances without a prescription, helping children to bypass that filtering would likely be illegitimate.<sup>427</sup> Thus, this Article's framework can serve another purpose: to guide circumvention designers and anti-censorship activists as well as their ideological opponents.

The second challenge is that framework's four prongs are interdependent to a degree. Accountability, for example, requires a level of free information exchange that filtering impedes. It is difficult to assess a state's censorship – or to criticize it – if dissenting views are blocked. For example, in Russia, allies of the current government have moved to purchase existing media outlets and to create new ones<sup>428</sup>, enhancing pro-government viewpoints, while prosecutors have begun to apply existing

---

<sup>425</sup> See Robert Lemos, *Tor hack proposed to catch criminals*, SECURITYFOCUS, Mar. 8, 2007, at <http://www.securityfocus.com/news/11447>.

<sup>426</sup> Declan McCullagh, *U.S. blunders with keyword blacklist*, CNET NEWS.COM, May 3, 2004, at [http://news.cnet.com/2010-1028\\_3-5204405.html](http://news.cnet.com/2010-1028_3-5204405.html) (describing International Broadcasting Bureau's program).

<sup>427</sup> See, e.g., "Keep Internet Neighborhoods Safe", Testimony of Professor Philip Heymann before the U.S. Senate Committee on the Judiciary, May 16, 2007, at [http://judiciary.senate.gov/testimony.cfm?id=2755&wit\\_id=6468](http://judiciary.senate.gov/testimony.cfm?id=2755&wit_id=6468); *Teens Tapping Into Illegal Online Drugs Sales*, CBS NEWS, May 16, 2007, at <http://wbztv.com/national/teens.prescription.drugs.2.283851.html>. The author 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, at <http://www.drugstrategies.org/internetdrugs/iep.html#1>.

<sup>428</sup> Troianovski & Finn, *supra* note 131.

laws more stringently and frequently to bloggers and on-line critics<sup>429</sup>. An effective filtering system – even an imperfect one – can alter sufficiently the information environment such that, while censorship appears popular, accountability is significantly diminished. Narrowness also affects the other factors. Overbroad filtering could indicate incompetence, but probably means a state is less than forthright about what material it targets, reducing transparency and openness. Thus, the four factors are not always separable; shifts in one can (and perhaps should) alter the others.

Finally, the critical test case for evaluating Internet filtering's legitimacy is almost certainly China. China poses considerable difficulties. First, Chinese citizens themselves are divided over government's proper role in shaping on-line content, and over the actions of American technology companies.<sup>430</sup> Anecdotal evidence suggests that many users hate Yahoo! and (perhaps grudgingly) like Microsoft<sup>431</sup>; empirical evidence from market share suggests that both play a far smaller role in China's on-line environment than domestic entities such as Baidu<sup>432</sup>. Any conclusion about how technology firms should behave in China will be a contested one.

Second, companies – and perhaps even governments – have economic motivation to resolve doubts in favor of participating in the burgeoning Chinese market. While statistics are not entirely clear, China appears to have the greatest number of Internet users and bloggers<sup>433</sup> of any country – an attractive target for technology providers. Companies such as IBM have rushed to set up research arms in the state to tap its technological talent and to build relationships that can lead to future sales.<sup>434</sup> Moreover, China's apparatus of on-line control is itself a sales opportunity, as companies such as Cisco and Nortel Networks have realized.<sup>435</sup> Technology companies may be willing to forgo sales in states such as Burma or Sudan for ethical reasons, but China may be too lucrative an opportunity to pass up. It is likely that applying the framework to China's Internet censorship

---

<sup>429</sup> See, e.g., Alex Rodriguez, *Trial in Russia sends message to bloggers*, CHICAGO TRIBUNE, Mar. 31, 2008, at [http://www.chicagotribune.com/news/nationworld/chi-russia-blogs\\_rodriguezmar31,1,3321029.story](http://www.chicagotribune.com/news/nationworld/chi-russia-blogs_rodriguezmar31,1,3321029.story).

<sup>430</sup> Fallows, *supra* note 200.

<sup>431</sup> Thompson, *supra* note 114.

<sup>432</sup> *Baidu leads China Web search market in Q4*, REUTERS, Jan. 25, 2008, at <http://www.reuters.com/article/internetNews/idUSSHA11273420080125> (listing Baidu at 60.1% market share, Google at 25.9%, and Yahoo! China at 9.6%).

<sup>433</sup> China Internet Network Information Center, *CNNIC Releases 2007 Survey Report on China Weblog Market*, at <http://www.cnnic.cn/html/Dir/2007/12/27/4954.htm> (Dec. 27, 2007) (claiming nearly 73 million blogs and 47 million bloggers).

<sup>434</sup> IBM, *China Research Laboratory*, at <http://www.research.ibm.com/beijing/> (last visited Aug. 14, 2008).

<sup>435</sup> See GREG WALTON, CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA, at <http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html>.

will produce a range of outcomes (though probably not wholehearted approval). Firms will undoubtedly 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 indigenous censorship technology for media from blogs to text messaging to cybercafé computers.<sup>436</sup> Its citizens already seem to prefer Chinese technology providers.<sup>437</sup> Western firms will use this possibility to bolster their case for remaining engaged in China, even if the state's filtering regime is found to be 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 concerns.<sup>438</sup>

China thus poses difficult questions, for this Article's framework and for technology companies alike. How the country's censorship system will fare under the framework should wait for that work to be done, though most commentators have been critical of China's filtering.<sup>439</sup> (Tellingly, companies such as Google and Microsoft do not defend China's actions; instead, they claim their presence will mitigate filtering's ill effects.) Even if firms decide to support the state's practices in the face of negative assessments, that does not destroy the methodology's value. Indeed, the contrast between corporate choices and an objective, process-based evaluation would likely provide critics with powerful ammunition. Finally, it may be true that refusing to sell Western hardware, software, and services to China would diminish only slightly the country's censorship prowess, but inevitability does not erase agency. The question is whether it is appropriate for these firms to assist China's filtering, not whether they can prevent it. Substitution is not an argument acceptable in other contexts: North Korea will torture political dissidents with or without Western assistance, but few firms would consider it legitimate to sell thumbscrews to the state.<sup>440</sup>

Circumvention, interdependence, and China complicate application of the proposed framework, but do not diminish its utility as an analytical

---

<sup>436</sup> See Villeneuve, *supra* note 259; OPENNET INITIATIVE, *supra* note 83.

<sup>437</sup> See, e.g., *supra* note 432 and accompanying text.

<sup>438</sup> Cf. VILLENEUVE, *supra* note 104.

<sup>439</sup> See, e.g., Deibert, *supra* note 82; Viktor Mayer-Schonberger & Malte Ziewetz, *Jefferson Rebuffed: the United States and the Future of Internet Governance*, 8 COLUM. SCI. & TECH. L. REV. 188 (2007); Palfrey & Rogoyski, *supra* note 3.

<sup>440</sup> See generally U.S. DEPARTMENT OF COMMERCE, *Ch. 2: Crime Control / Human Rights*, in FOREIGN POLICY REPORT – YEAR 2004, at [http://www.bis.doc.gov/policiesandregulations/04forpolcontrols/chap2\\_crimehumanrights.htm](http://www.bis.doc.gov/policiesandregulations/04forpolcontrols/chap2_crimehumanrights.htm) (noting the U.S. has a “policy of denial for any license application to export specially designed implements of torture and thumbscrews”).

tool. The framework operates as a window onto a complex problem; even if its benefits are limited, it can helpfully clarify censorship's challenges.

## VI. CONCLUSION

If Internet filtering were a stock, one would be well-advised to buy it: on-line censorship is on the march, in democratic states as well as authoritarian ones. Ten years ago, a handful of countries used technology to censor the Internet; by 2006-2007, over three dozen tested by the OpenNet Initiative did so.<sup>441</sup> 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, in short, is not limited to bad actors – to repressive regimes such as North Korea and Iran.

This Article offers a new approach to evaluating the legitimacy of Internet filtering by focusing on the process by which censorship decisions are made. It proposes to rate states 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 regimes through quantitative metrics based on its four principles, and then to utilize these measurements in both public and private decisionmaking. Consistent, rigorous analysis that is applied to all censoring states, and that illuminates comparisons among them, will improve the quality of such decisions, and the perception of them. While filtering is increasingly normal, it should not be seen as natural – instead, citizens and their representatives should examine carefully, skeptically, and thoughtfully calls to restrict access to information on-line.

\* \* \*

---

<sup>441</sup> Zittrain & Palfrey, *supra* note 7, at 2.