Arizona Legal Studies

Discussion Paper No. 12-28

Censorship V3.1

Derek E. Bambauer
The University of Arizona
James E. Rogers College of Law

September 2012

CENSORSHIP V3.1

Derek E. Bambauer[*]

Abstract

Internet censorship has evolved. In Version 1.0, censorship was impossible; in Version 2.0, it was a characteristic of repressive regimes; and in Version 3.0, it spread to democracies who desired to use technology to restrain unwanted information. Its latest iteration, Version 3.1, involves near-ubiquitous censorship by democratic and authoritarian countries alike. This Article argues that the new censorship model involves four changes: a shift in implementation to private parties; a hybrid approach mixing promotion of favored viewpoints with suppression of disfavored ones; a blend of formal mandates with informal pressures; and a framing of censorship using uncontroversial labels. It suggests a set of responses to censorship that cabin its abuses and push it towards more legitimate methods: focusing on governmental restrictions, insisting on labeling censorship as such, supporting distributed Internet governance, demanding a default right of access to information, and addressing corporate involvement.

Table of Contents

[*] Associate Professor of Law, University of Arizona James E. Rogers College of Law. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Robert Glennon, Dan Hunter, Thinh Nguyen, Hal Roberts, Chris Robertson, and several anonymous referees. The author welcomes comments at <derekbambauer@email.arizona.edu>.

And if all others accepted the lie which the Party imposed – if all records told the same tale – then the lie passed into history and became the truth.
- George Orwell, *1984*

I. INTRODUCTION

Like the Internet itself, censorship adapts. Its latest incarnation, Censorship v3.1, is particularly pernicious, for it is less visible, less transparent, and less vulnerable to challenge than previous iterations. This Article argues that on-line content control has passed through several distinct periods, with definitive characteristics. It then describes the contours of Censorship v3.1, and suggests an initial set of legal and technical responses that can cabin censorship, perhaps pushing it into more legitimate spaces and methods.[1]

A. A Brief History of Internet Censorship

There have been three epochs in Internet censorship. In the first, Censorship v1.0, preventing access to on-line material via technological constraint was considered impossible – a fool's errand. John Gilmore famously opined that the Internet treats censorship as damage, and routes around it.[2] The network, designed to adapt to major disruptions such as war and physical damage, would simply bypass informational barriers put in place by governments, those "weary giants of flesh and steel."[3] Technological optimism abounded.[4]

Censorship v1.0 passed even before the crash of the dotcom economy.[5] Version 2.0 conceded the feasibility of technological screening of information, but made instead a normative claim: only benighted governments would engage in such practices. Nation-states contemplating censorship would have to join a virtual rogue's gallery: China, Saudi

[1] *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. (forthcoming 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926415.
[2] Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62.
[3] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, http://homes.eff.org/~barlow/Declaration-Final.html. On the network design and disruption, *see* Cade Metz, *Paul Baran, the link between nuclear war and the Internet*, WIRED, Sept. 4, 2012, http://www.wired.co.uk/news/archive/2012-09/04/h-bomb-and-the-internet (noting surviving nuclear attack was but one goal of packet-switched routing).
[4] *See, e.g.*, ADAM WISHART & REGULA BOCHSLER, LEAVING REALITY BEHIND (2003); JAMES GLASSMAN & KEVIN HASSETT, DOW 36,000 (1999).
[5] Saudi Arabia demonstrated effective Internet filtering in 1999; China's Golden Shield project (the "Great Firewall of China") began in 1998. OPENNET INITIATIVE, INTERNET FILTERING IN SAUDI ARABIA IN 2004, http://opennet.net/studies/saudi; ETHAN GUTMANN, LOSING THE NEW CHINA 127-31 (2004). On the crash, see JOHN CASSIDY, DOT CON: THE GREATEST STORY EVER SOLD (2002).

Arabia, Iran, Burma, Vietnam, and others. This provided a norms-based check on governments. The label "censorship," and the set of fellow travelers who filtered the Internet, created some political disincentives for content control.

This easy formula – filtering equates with authoritarian government – no longer held true by 2006-2007, when an increasing number of democratic countries were engaging in censorship. The list grew rapidly. France blocked hate speech[6]; South Korea filtered North Korean sites[7]; Great Britain censored child pornography[8] and then copyright infringement[9]; India curtailed access to political and religious content[10]. Censorship v3.0, where filtering was increasingly ubiquitous regardless of political system, had definitively arrived when the United States began seizing domain names and blocking access to the content located at them, primarily due to allegations of intellectual property infringement. Countries such as the U.S. sought to retain the rhetorical and normative advantages of the prior period by describing their efforts as enforcing property rights, protecting children, or preventing dignitary harms. Such assertions became increasingly untenable. Censorship functions identically when America redirects access to domain names about Cuban culture or hip hop music and when Vietnam redirects ones about political minorities.[11] While one can distinguish between the legitimacy of the actions of these two states, both countries plainly censor the Internet.[12]

B. Legitimacy and Resistance

Widespread censorship on-line is not necessarily bad. Most countries find certain content – such as child pornography, or hate speech – sufficiently objectionable to want to prevent its distribution and consumption. Since even democratic countries are heterogeneous in their disapproval, we cannot reliably assess censorship's legitimacy by

---

[6] Sean Gallagher, *French president promises law to make viewing "hate sites" an offense*, ARS TECHNICA, Mar. 23, 2012, http://arstechnica.com/tech-policy/2012/03/thoughtcrime-french-president-promises-law-to-make-viewing-hate-sites-criminal/.

[7] OpenNet Initiative, *South Korea*, Aug. 6, 2012, http://opennet.net/research/profiles/south-korea.

[8] Frank Fisher, *Caught in the Web*, GUARDIAN, Jan. 17, 2008, http://www.guardian.co.uk/commentisfree/2008/jan/17/caughtintheweb.

[9] *Twentieth Century Fox Film Corp v British Telecommunications PLC*, [2011] EWHC 1981 (Ch) *3–4 at ¶¶1–4, *67 at ¶ 204.

[10] Jonah Force Hill, *India's Internet Freedom Nightmare*, THE DIPLOMAT, Aug. 25, 2012, http://thediplomat.com/2012/08/25/indias-internet-freedom-nightmare/?all=true.

[11] Adam Liptak, *A Wave of the Watch List, and Speech Disappears*, N.Y. TIMES, Mar. 4, 2008, at A16; OpenNet Initiative, *Vietnam*, Aug. 7, 2012, http://opennet.net/research/profiles/vietnam.

[12] Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377 (2009).

examining what is blocked.[13] Rather, as I argue elsewhere, we must look to the robustness of the processes by which citizens decide to make information unavailable. In particular, censorship is legitimate when a state performs it openly, describes transparently the content it blocks, narrowly targets only prohibited material, and provides accountability in its decisionmaking to the citizens it affects (including countermajoritarian protections).[14]

Recent controversies over Internet censorship in countries with democratic governments and long traditions of free speech reinforce this point. Formal censorship through law has increasingly been met with organized, politically effective opposition, which has succeeded at times. In Germany, the federal government passed a bill in 2009 that would have mandated filtering of child pornography.[15] However, widespread opposition to the bill forced the governing coalition to promise not to enforce the law, even though it had been signed by Germany's president.[16] Similarly, legislation implementing censorship of sites that allegedly infringe intellectual property rights was introduced in the last two Congressional sessions in the United States. While neither the Stop Online Piracy Act (SOPA) nor the PROTECT IP Act was even put to a vote, the PROTECT IP Act was passed by the Senate Judiciary Committee, and SOPA was in committee mark-up when protests forced its suspension.[17] SOPA in particular led to the rapid formation of an ad hoc coalition opposed to Internet censorship, comprised of technology companies such as Google, civil liberty groups, new media sites, and individual users.[18] The removal of PROTECT IP and SOPA from the Congressional agenda represented a surprising victory for this new coalition, whose most effective arguments were that the bills would align America with nations like China and Iran, and that the new regulation would "break the Internet."[19]

The SOPA and PROTECT IP battles demonstrate the virtues of democratic governance: both sides of the debate enjoyed access to legislators and media outlets; the bills morphed during consideration; and,

---

[13] *Id.* at 381-86.
[14] *Id.* at 390-409.
[15] *Germany's President Signs an Internet Bill Against His Own Party*, EDRI, Feb. 24, 2010, http://www.edri.org/edrigram/number8.4/german-president-adopts-internet-childporn-law.
[16] *Id.*
[17] Eric Goldman, *Celebrating (?) the Six-Month Anniversary of SOPA's Demise*, FORBES, July 18, 2012, http://www.forbes.com/sites/ericgoldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopas-demise/.
[18] Hayley Tsukuyama & Cecilia Kang, *SOPA opposition goes viral*, WASH. POST, Nov. 22, 2011, http://www.washingtonpost.com/business/economy/sopa-opposition-goes-viral/2011/11/22/gIQAZX7OmN_story.html.
[19] *Id.*; Goldman, *supra* note 17.

arguably, popular opposition stopped laws designed to benefit politically powerful industries at the expense of free speech. These lessons were not lost on SOPA proponents; Record Industry Association of America President Cary Sherman stated that, "it's very difficult to counter the misinformation when the disseminators also own the platform."[20] While both bills suffered flaws regarding transparency and narrowness[21], the openness of the proposals (though proponents refused to call them "censorship") and the accountability created by an elected legislature gave the bills greater legitimacy than, for example, President Barack Obama's policy of seizing domain names of sites alleged to violate intellectual property law[22]. Censorship emerging from such a process is more likely to be legitimate.

C. The Next Wave

Censorship v3.1 has particular salience in late 2012, given ongoing controversies about the nature and form of Internet governance that will be contested at the World Conference on Internet Telecommunications (WCIT-12).[23] The level and nature of state control over the Internet are one of the most contentious issues that WCIT-12 will debate. Put crudely, the fight pits the United States, with its emphasis on multi-stakeholder governance through the ICANN structure (albeit with the backdrop of passive U.S. government control), against much of the rest of the world, which seeks a greater voice for governments in how the Internet is run, likely through the International Telecommunication Union.[24] The U.S. position at WCIT-12 is weakened, though. Previously, America could plausibly claim to champion free, open Internet communication against the risk that, for example, Libya

---

[20] Jenna Wortham, *With Twitter, Blackouts and Demonstrations, Web Flexes Its Muscle*, N.Y. TIMES, Jan. 19, 2012, http://www.nytimes.com/2012/01/19/technology/protests-of-antipiracy-bills-unite-web.html.

[21] Mark Lemley, David S. Levine, & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (Dec. 19, 2011), http://www.stanfordlawreview.org/online/dont-break-internet.

[22] Margaret Grazzini, *Four Rounds of ICE Domain Name Seizures and Related Controversies and Opposition*, BERKELEY TECH. L.J. BOLT (Feb. 23, 2011), http://btlj.org/?p=917.

[23] Cale Guthrie Weissman, *Documents Leaked Detailing Proposals for UN Telecommunications Summit*, OPENNET INITIATIVE, June 21, 2012, http://opennet.net/blog/2012/06/documents-leaked-detailing-proposals-un-telecommunications-summit.

[24] Eric Pfanner, *Debunking Rumors of an Internet Takeover*, N.Y. TIMES, June 11, 2012, http://www.nytimes.com/2012/06/11/technology/debunking-rumors-of-an-internet-takeover.html?pagewanted=all; *U.S. Contributions to the World Conference on International Telecommunications (WCIT-12)*, Aug. 3, 2012, http://www.state.gov/e/eb/rls/othr/telecom/196031.htm.

could head a U.N. committee on human rights and the Internet.[25] However, the era of American benign neglect regarding content control online is over: America has begun censoring the Net.[26] Here too one sees the evolution of censorship: the contest is no longer about whether censorship is legitimate, but under what conditions.

The debate is also tilted towards issues, and solutions, that could empower censors. Many of the most urgent issues at WCIT-12 contemplate greater on-line attribution as solutions: cybercrime, IP enforcement, privacy protection, and cybersecurity all suffer from a lack of robust authentication. In combination with the capabilities of IPv6, where every connected device can have a unique, permanent network address, these policy demands may lead to decisions that enhance censorship capabilities as a byproduct. Embedding attribution in Internet protocols and devices offers states greater control over who can speak, and to whom.[27] Moreover, these concerns re-align the traditional coalitions in Internet governance. The United States in particular seeks to enhance cybersecurity, which has been a policy priority of administrations of both major political parties since 1997.[28] The need for better security could lead to measures that can be adapted to censorship. Indeed, countries such as Russia explicitly define information security in terms of controlling political dissent.[29]

Thus, censorship remains on the policy agenda at both a national and international level, even as its methods evolve.

II. EVOLUTION

Both in democratic and non-democratic states, on-line censorship is beginning to morph. It is characterized by four trends. First, states increasingly seek to offload the technical burdens and the political accountability for censorship onto private actors, including Internet Service Providers (ISPs), application providers, and users. Second, governments mix positive information strategies that paint their efforts in a beneficent light with suppression of dissent or disfavored information. Third, censorship in this new era blends formal mandates with informal pressures on key actors. Finally, governments seek to frame censorship as something else entirely – as necessary efforts directed to other, less contentious ends.

---

[25] *Cf. Libya takes human rights role*, BBC NEWS, Jan. 20, 2003, http://news.bbc.co.uk/2/hi/africa/2672029.stm.

[26] Bambauer, *supra* note 1.

[27] Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 601-02 (2011).

[28] THE PRESIDENT'S COMM. ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 3 (Oct. 1997), http://www.fas.org/sgp/library/pccip.pdf.

[29] Tom Gjelten, *Seeing the Internet As An Information Weapon*, NPR, Sept. 23, 2010, http://www.npr.org/templates/story/story.php?storyId=130052701.

A. Outsourcing

States are outsourcing content control. Initial models of Internet censorship employed state-controlled choke points in the physical or logical network. Saudi Arabia, which routes all Internet communications through a set of proxy servers under the control of the Communications and Information Technology Commission[30], and China, which performs most Web filtering at the network backbone via its Golden Shield project[31], are the paradigmatic cases. These efforts, while initially effective, created resource constraints that led to decreased speeds and underblocking.[32] Subsequent efforts sought to deputize intermediaries via legal mandates. Examples include French restrictions on hate speech such as Holocaust denial[33]; British pressure on ISPs to adopt BT's Cleanfeed system for blocking child pornography and copyright infringement[34]; and Singapore's strict licensing requirements that ISPs and content providers follow a code of practice mandating censorship[35]. This transfer of implementation from the state to private actors privatizes the burden of censorship. In effect, censorship becomes a tax upon users of ISPs who must engage in filtering and blocking.

The shift also diffuses responsibility for decisions about content restrictions. Formally, decisions about blocking material are made by private entities, such as ISPs or trade organizations. This can enable governments to bypass both political opposition and judicial scrutiny of state actions. Australia provides an excellent example. The Labour government of Kevin Rudd came to power in late 2007 with, as part of its electoral platform, a plan to require national Internet filtering.[36] The program immediately encountered political opposition in Australia's

---

[30] ACCESS CONTROLLED 562-63 (Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., 2010).

[31] OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004-2005: INTERNET INFRASTRUCTURE AND ACCESS, http://opennet.net/studies/china#toc2b.

[32] James Fallows, *"The Connection Has Been Reset,"* THE ATLANTIC, March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-the-connection-has-been-reset/306650/.

[33] OpenNet Initiative, *Europe*, http://opennet.net/research/regions/Europe (2007); Tribunal de Grande Instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, Ordonnance de référé (Order for Summary Judgment), No. RG 00/05308, at 3, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf.

[34] *Twentieth Century Fox Film Corp.* EWHC 1981.

[35] OpenNet Initiative, *Singapore*, May 10, 2007, http://opennet.net/research/profiles/singapore.

[36] Derek E. Bambauer, *Filtering in Oz: Australia's Foray Into Internet Censorship*, 31 U. PA. J. INT'L L. 493, 497-77 (2009).

Senate, forcing the government to place it on hold.[37] The Senate stalemate and leadership changes pressed the government to seek an alternative path: it pushed the trade organization for Australian ISPs, the Internet Industry Association, to engage in co-regulation.[38] In practice, this involved ISPs agreeing to a code of practice – enforceable by the Australian Media and Communications Authority (ACMA)[39] – mandating that they filter domains designated by Interpol as hosting child pornography.[40] Even formally, the system is a hybrid: adoption is voluntary, but results from an ACMA request for assistance under Australia's Telecommunications Act.[41] So, too, the purposes of the scheme are twofold. The ISPs are provided immunity from civil liability for acting in response to a request under the Telecommunications Act.[42] And, the government can avoid accountability for the decision to block (taken by the ISP) or the materials selected for blocking (compiled by Interpol).[43] In turn, ISPs can forestall legislative mandates that might be more onerous than the putatively voluntary arrangement; can present themselves as protecting children; and can also place the onus for content decisions on Interpol.

Co-opting intermediaries – especially those with dominant market positions – both greatly raises the cost of information access, and also reduces the efficacy of circumvention. For example, Google will remove certain results from its listings (such as those for which it received a formal notification of claimed infringement under the Digital Millennium

---

[37] *Id.* at 501.

[38] *See* Senator Stephen Conroy, *Outcome of consultations on Transparency and Accountability for ISP Filtering of RC content*, July 9, 2010, http://www.minister.dbcde.gov.au/media/media_releases/2010/068.

[39] Australia Media & Communications Auth., *What if an ISP does not comply with an industry code of practice or an ACMA direction or notice?*, Aug. 20, 2012, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90157#comply.

[40] Filtering at the domain level – such as telstra.com – risks massive overblocking. *See Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 633-34, 650-52, 655 (E.D. Pa. 2004) (documenting overblocking of 1.1 million unrelated sites via filtering of 400 domain names). For Australia, though, this is not a bug, it is a feature: "There is a big incentive to big hosting providers to keep them honest and to get that stuff off their hosting site." Natalie Apostolou, *First Australian ISPs launch Interpol internet filter*, THE REGISTER, July 3, 2011, http://www.theregister.co.uk/2011/07/03/interpol_fiter_hits_aus/ (quoting CEO of ContentKeeper Technologies, a firm assisting Interpol with implementation).

[41] § 313(4), Telecommunications Act of 1997, *available at* http://www.comlaw.gov.au/Details/C2012C00584/Html/Text#_Toc332105895; *see Renai LeMay, Most ISPs will filter Interpol list this year: IIA*, ZDNET, June 27, 2011, http://www.zdnet.com/most-isps-will-filter-interpol-list-this-year-iia-1339317482/.

[42] § 313(5), Telecommunications Act of 1997.

[43] Renai LeMay, *More ISPs sign up to AFP's Interpol filter*, DELIMITER, Dec. 4, 2011, http://delimiter.com.au/2011/12/04/more-isps-sign-up-to-afps-interpol-filter/.

Copyright Act[44], or that list sensitive personal information such as a Social Security Number or credit card data[45]), and will de-prioritize other results based on their content[46]. It may still be possible to reach these sites, but discovering them becomes much more difficult or expensive. And if a hosting company can be persuaded to remove content, as when Amazon was convinced by Senator Joseph Lieberman's staff to drop WikiLeaks from its cloud computing platform, that material must be moved elsewhere, and users must be informed of the change.[47] These measures are not perfect, but they reduce availability, and may shift users onto methods that are one-to-one communication (such as instant messaging, or e-mail) rather than one-to-many (such as the Web or BitTorrent). Circumvention techniques such as proxy servers or virtual private networks are designed to bypass interference with a user's attempt to reach information at a known location.[48] When that location is no longer known, and no longer easily discovered, circumvention becomes less effective.

B. Positive and Negative Approaches

Second, censorship's sophistication is increasing, as states provide information favoring their positions along with repressing dissenting views. Iran, for example, blocks Web sites and some blogs that take views at odds with the government's political and religious positions, but the state also promotes blogging by users who have more favorable stances.[49] China employs volunteers, some of whom are paid by the state, to create comments and posts that praise the government's positions, and to designate

---

[44] *Removing Content from Google*, http://support.google.com/bin/static.py?hl=en&ts=1114905&page=ts.cs.

[45] *Keeping personal information out of Google*, http://support.google.com/webmasters/bin/answer.py?hl=en&answer=164133&rd=1.

[46] Danny Sullivan, *The Emanuel Update: Google Will Penalize Sites Repeatedly Accused Of Copyright Infringement*, SEARCH ENGINE LAND, Aug. 10, 2012, http://searchengineland.com/dmca-requests-now-used-in-googles-ranking-algorithm-130118.

[47] Lance Whitney, *Amazon Cuts Off WikiLeaks*, CNET NEWS, Dec. 2, 2010, http://news.cnet.com/8301-13578_3-20024376-38.html (discussing Amazon.com's removal of WikiLeaks from its cloud computing service one day after Senator Lieberman criticized the company for hosting the site).

[48] Nart Villeneuve, *Technical Ways to Get Round Censorship*, in REPORTERS WITHOUT BORDERS, HANDBOOK FOR BLOGGERS AND CYBER-DISSIDENTS (2005), *available at* http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf.

[49] 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; Neil MacFarquhar, *Iranian Blogosphere Tests Government's Limits*, N.Y. TIMES, Apr. 6, 2008, http://www.nytimes.com/2008/04/06/world/middleeast/06iranblog.html?pagewanted=all.

for takedown those that oppose it.[50] The "Fifty-Cent Army," named for the fee purportedly paid for each post, seeks to shift the on-line information environment by altering not only people's views on issues, but their perception of how widely shared those views are. For example, China appears to have encouraged its new Army to attack calls for the country to launch a "jasmine revolution" and follow in the footsteps of the democratic shifts in the Middle East.[51] And South Korea has mixed a surge in blocking of Web sites and legal pressures on government critics with pressures on traditional media to support the state's policies.[52] Censoring states are thus adopting hybrid tactics, combining repression with strategies to generate and disseminate supportive views. This approach threatens transparency: it disguises government propaganda as the product of private voices, and it invisibly skews the balance and content of on-line discourse.

C. Hybrids

Third, as part of the shift of censorship's burden to private actors, governments are turning increasingly to informal pressures as well as formal ones. The Australian example above demonstrates how a government blocked from filtering may be able to transmogrify its plan through pressure on private stakeholders. So, too, the administration of U.S. President Barack Obama has employed leverage over major ISPs to push them to agree to a new program, the Copyright Alert System, that seeks first to educate and then to penalize Internet users who allegedly engage in copyright infringement.[53] First, the administration sought to include a graduated response system (popularly described as the "three strikes" scheme) in the Anti-Counterfeiting Trade Agreement, an international instrument that would have required signatories to transpose its provisions

---

[50] Selina Wang, *China's Fifty Cent Party*, HARVARD POLITICAL REV., Feb. 7, 2012, http://hpronline.org/world/chinas-fifty-cent-party/.

[51] Joshua Keating, *China's "50-cent party" takes on the jasmine revolutions*, FOREIGN POLICY, Mar. 1, 2011, http://blog.foreignpolicy.com/posts/2011/03/01/chinas_50_cents_party_take_on_the_jasmine_revolutions.

[52] Chico Harlan, *In S. Korea, a shrinking space for speech*, WASH. POST, Dec. 21, 2011, http://www.washingtonpost.com/world/asia_pacific/in-s-korea-a-shrinking-space-for-speech/2011/12/21/gIQAmAHgBP_story.html; Choe Sang-Hun, *Korea Policing Internet. Twist? It's South Korea*, N.Y. TIMES, Aug. 13, 2012, at A1.

[53] Center for Copyright Information, *Copyright Alert System (CAS)*, http://www.copyrightinformation.org/alerts; Greg Sandoval, *Exclusive: Top ISPs poised to adopt graduated response to piracy*, CNET NEWS, June 22, 2011. Disclosure: the author represents computer security researcher Christopher Soghoian in a Freedom of Information Act suit against the Office of Management and Budget that seeks to compel release of documents related to the copyright alert system. *Soghoian v. Office of Management and Budget*, No. 1:11-cv-02203-ABJ (D.D.C. 2012).

into national law.[54] These American efforts were thwarted first by disclosure of the proposed text, and then by political opposition in the European Union.[55]

Stymied, and with no assurance that the Congress would pass similar legislation[56], the administration turned to private ordering. ISPs and content providers, such as recorded music labels and motion picture studios, had been negotiating over voluntary steps ISPs might take to reduce infringement by their users.[57] The administration pushed ISPs to agree to take such measures, and to do so aggressively.[58] Indeed, it did so via threat: if ISPs did not cooperate voluntarily, the administration would press for legislation that they would find even less amenable.[59] (The Obama administration followed a similar course on data retention: when voluntary negotiations with ISPs over a proposed 18-month retention program for user data broke down, it supported a bill in Congress that would make such efforts mandatory.[60]) The effort was successful. ISPs agreed to take remedial measures for recalcitrant infringers on their networks, despite having no legal obligation to do so. While the Obama administration has repeatedly characterized the bargain as a private arrangement, its influence over the deal is manifest, from the one-sided sharing of information between content companies and the administration[61], to an NBC Universal

[54] David Kravets, *ACTA Backs Away from Three Strikes*, WIRED, Apr. 21, 2010, http://www.wired.com/threatlevel/2010/04/acta-treaty/.

[55] *Id.*

[56] The most directly relevant, and likely viable, legislation at the time was the Combating Online Infringement and Counterfeits Act, S.3804 (111th Cong., 2010). The measure passed the Senate Judiciary Committee unanimously, but was blocked through parliamentary procedure by one senator.

[57] ISPs were clearly immunized from liability for copyright infringement under the relevant provisions of the Digital Millennium Copyright Act. 17 U.S.C. §§ 512(a), (c); *see generally Viacom Int'l v. YouTube*, No. 10-3270 (2d Cir. 2012); *UMG Recordings v. Shelter Capital Partners*, 667 F.3d 1022 (9th Cir. 2011).

[58] Sandoval, *supra* note 53.

[59] Jason Mick, *Obama Conscripts ISPs as "Copyright Cops," Unveils "Six Strikes" Plan*, DAILYTECH, July 8, 2011, http://www.dailytech.com/Obama+Conscripts+ISPs+as+Copyright+Cops+Unveils+Six+Strikes+Plan/article22107.htm.

[60] Declan McCullagh, *Justice Department seeks mandatory data retention*, CNET NEWS, Jan. 24, 2011, http://news.cnet.com/8301-31921_3-20029423-281.html?part=rss&subj=news&tag=2547-1_3-0-20.

[61] *See, e.g.*, e-mail from Matthew Gerson, Universal Music, to Intellectual Property Enforcement Coordinator Victoria Espinel, Nov. 12, 2010 (sharing ISP proposal regarding alert system with Espinel). *Available at* http://blogs.law.harvard.edu/infolaw/files/2012/07/Soghoian_Redacted_Docs.pdf (p.2).

executive's request to the White House's IP Enforcement Coordinator for help with the "cajole issues" in the deal.[62]

The hybrid approach – where censorship is a government goal, but one carried out informally by willing or reluctant private entities – impedes scrutiny of a state's efforts to limit access to content. Legal checks, such as constitutional constraints on prior restraint[63], and transparency measures that limit state action[64] may apply less, or not at all, to private firms. Indeed, such content filtering decisions may be protected by statute[65], or as speech by firms or individuals[66]. Private action may thus be less vulnerable to legal challenge, particularly if there is covert acquiescence by government regulators. Decisionmaking can be performed behind closed boardroom doors, rather than in open democratic processes. And while market competition may be presented as a checking force – intermediaries do not wish to annoy their customers – this constraint declines in efficacy when there are fewer competitors (such as with broadband access providers in the U.S.), or when those competitors also censor.[67]

D. A Rose By Any Other Name

Lastly, censorship is never portrayed as censorship. Governments always frame their efforts to control content online under another rubric. This Orwellian re-shaping both acknowledges the power of the moniker "censorship" and seeks to make the tactic seem not only desirable, but inevitable, given the underlying issue. Thus, the U.S. describes its ex parte seizure of domain names where material that infringes IP rights is allegedly located as "robust intellectual property enforcement."[68] South Korea claims to combat "character assassinations and suicides caused by excessive

---

[62] E-mail from Alec French, NBC Universal, to Intellectual Property Enforcement Coordinator Victoria Espinel, Jan. 6, 2010. *Available at* http://blogs.law.harvard.edu/infolaw/files/2012/07/Soghoian_Redacted_Docs.pdf (p.60).

[63] *Freedman v. Maryland*, 380 U.S. 51, 59–60 (1965).

[64] 5 U.S.C. § 552.

[65] 47 U.S.C. § 230(c)(2)(A).

[66] Eugene Volokh & Donald M. Falk, *First Amendment Protection for Search Engine Search Results*, Apr. 20, 2012, http://www.scribd.com/doc/93009737/Volokh-First-Amendment-Paper-Copy. Note that this research was funded by Google.

[67] Industry Analysis and Technology Division, Wireline Competition Bureau, *Internet Access Services: Status as of June 30, 2010* 7 (Mar. 2011), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-305296A1.pdf (showing limited competition for broadband Internet access in U.S.).

[68] U.S. Immigration and Customs Enforcement, *Operation In Our Sites protects American online shoppers, cracks down on counterfeiters ICE-led IPR Center seizes 150 website domains selling counterfeit and pirated merchandise*, Nov. 28, 2011, http://www.ice.gov/news/releases/1111/111128washingtondc.htm (quoting Attorney General Eric Holder).

insults, the spreading of false rumors and defamation."[69] Russian Prime Minister Dmitri Medvedev described the country's new Internet censorship legislation as safeguarding people's "right to be protected against harmful content."[70] The legislation itself is titled as the "Provoking children to act in ways which are harmful to themselves and their health and development" bill.[71] While censorship as a practice is spreading, censorship as a description is not. This lack of candor by governments seeks to divert attention from the proposed solution – filtering access through technological or legal means – to the underlying problem. Rebranding efforts attempt to portray censorship as directed to less contentious ends, and as driven by popular demand. Such efforts risk burning the house to roast the pig.[72]

In short, the evolution of censorship to Version 3.1 is worrisome, for this new iteration is less apparent, less amenable to challenge, and less transparent than prior versions. This Article next turns to a potential set of responses to mitigate these problems.

III. RESPONSES

Censorship v3.1 is worrisome. It operates in democracies and dictatorships alike, and in both, bowdlerizing governments seek to avoid accountability by pressing intermediaries to act indirectly on their behalf. The hybrid form of on-line filtering impedes transparency, and reduces the efficacy of tested circumvention techniques. Even if this new era of censorship does not prevent access to information, it makes it considerably more costly and more difficult to achieve. And, Censorship v3.1 is less legitimate from a process-based perspective.

I suggest a set of five responses intended to rebalance the debate. This menu is necessarily general: statutory reform proposals for the U.S. are of little relevance to Iranian dissidents, or Indian activists. However, they form the core of a free speech immune system for the Net. The goal is not to eliminate censorship, but to cabin it to legitimate purposes and methods, and to drag it into the open.[73] To check Censorship v3.1, citizens should first concentrate on their government's role in information control. Second, they should insist that restrictions on information, no matter how popular, constitute censorship that must be defended. Third, they should advocate for continued decentralized governance and control of key Internet

[69] Sang-Hun, *supra* note 52.
[70] *Russia's parliament votes for Internet censorship law*, BBC NEWS, July 11, 2012, http://www.bbc.co.uk/news/technology-18805039.
[71] Zack Whittaker and Violet Blue, *Russia's Internet blacklist looms in freedom crackdown*, CNET NEWS, July 6, 2012, http://news.cnet.com/8301-13578_3-57466592-38/russias-internet-blacklist-looms-in-freedom-crackdown/.
[72] *Butler v. Michigan*, 352 U.S. 380, 383 (1957).
[73] For a discussion of what makes censorship legitimate, *see* Bambauer, *supra* note 12.

infrastructure. Fourth, they should press for a norm of access: users have a default right to access information from willing speakers, and overriding that default requires heightened justification. Finally, citizens and investors should push for measures that address corporate involvement in government censorship.

A. Governments With Guns

First, I contend that citizens should worry principally about governments restricting information, either directly or via collusion with the private sector. If private entities block information, users may be able to bypass restrictions by turning to competitors, or sharing information via a different means. If Facebook restricts information unilaterally, citizens can turn to Twitter, or Google+.[74] But if the government backs such bans with the force of law, risk-averse people will hesitate to use alternative channels. Unlike private firms, governments command a monopoly on the use of deadly force.[75] Or, if the government pressures companies to follow the same set of rules, competition becomes irrelevant. This is not to suggest ignoring corporate restrictions on speech. Rather, government-backed censorship is of a different and greater order, and warrants greater attention.

This focus may have important legal and technical ramifications. It could argue for reduced state involvement in the provision of Internet access services, for example, to mitigate the opportunity for state filtering on such networks.[76] Paradoxically, this could suggest that projects such as municipal wi-fi should be curtailed: in the U.S., many such networks are filtered, with the First Amendment imposing only minimal constraints on blocking.[77] And, it could suggest that American jurisprudence should adopt a more expansive version of the state action doctrine, to promote judicial scrutiny of censorship where the government is involved, but is not formally responsible for blocking decisions. This would, for example, require the government to meet a heightened standard when conditioning subsidies for higher education on universities taking steps to prevent infringing content from crossing their networks[78], or it could enable constitutional challenges to the Obama administration's involvement in private filtering decisions by ISPs[79]. Legislative constraints are also

---

[74] *See, e.g.*, Abigail R. Esman, *Facebook's Censors Strike Again – Is America To Blame?*, FORBES, Aug. 6, 2012, http://www.forbes.com/sites/abigailesman/2012/08/06/facebooks-censors-strike-again-is-america-to-blame/.
[75] Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601, 1613 (1986).
[76] Bambauer, *supra* note 1.
[77] *Id.*
[78] Higher Education Opportunity Act § 493, 122 STAT. 3078, 3309; 34 C.F.R. § 668.14(b)(30).
[79] Mick, *supra* note 59.

possible. However, every society has categories of content for which censorship is the obvious solution; legislation that proposes to set such content free is unlikely to be adopted.

B. Don't Think of an Elephant

Second, language matters: citizens should insist that restrictions on information, such as blocking of Web sites or de-listing of search results, be described as "censorship." It is possible for censorship to be legitimate. Title II of the Digital Millennium Copyright Act, which establishes a notice-and-takedown scheme for material that allegedly violates copyright law, is (I argue) just such a regime.[80] This semantic shift is difficult but necessary. For Americans, provisions that mandate removal or blocking of child pornography images seem not only intuitively obvious, but vital. Yet, if these measures are indeed of paramount importance, they should readily withstand the heightened scrutiny that "censorship" draws.[81] Classifying these measures as censorship forces us to confront the tradeoffs among competing values that we face. It makes the weighing of free speech against child welfare explicit rather than assumed.[82] Calling content restrictions "censorship" also ensures parity of treatment. It is hypocritical for America to chastise China when it censors political dissidents, and to criticize it when it fails to censor IP infringers.[83] It is difficult to take seriously American efforts to promote open communication abroad when our government seizes domain names without notice and then denies their owners due process of law.[84] When citizens admit that even seemingly obvious, vital restrictions on Internet information constitute censorship, they commit to justifying such actions openly and carefully, and to weighing other states' actions with equal care.

---

[80] Bambauer, *supra* note 12 at 401.

[81] *See, e.g.*, *Osborne v. Ohio*, 495 U.S. 103 (1990) (upholding ban on child pornography).

[82] For Americans who think this tradeoff obvious, recall that the Supreme Court has recently prioritized free speech over the emotional interests of bereaved families of deceased American soldiers, *Snyder v. Phelps*, 562 U.S. __ (2011); over the health risks to children from violent video games, *Brown v. Ent'mt Merchants Ass'n*, 564 U.S. __ (2011); over privacy interests in prescriptions, *Sorrell v. IMS Health*, 564 U.S. __ (2011): over citizens' ability to punish candidates who lie about winning military decorations, *U.S. v. Alvarez*, 567 U.S. __ (2012); and over equal funding for political campaigns, *Am. Tradition Partnership v. Bullock*, 567 U.S. __ (2012).

[83] Bambauer, *supra* note 12 at 385-86.

[84] Grant Gross, *DOJ drops charges against websites seized for 17 months*, COMPUTERWORLD, Aug. 29, 2012, http://www.computerworld.com.au/article/435018/doj_drops_charges_against_websites_seized_17_months/; Ben Sisario, *Hip-Hop Copyright Case Had Little Explanation*, N.Y. TIMES, May 6, 2012, http://www.nytimes.com/2012/05/07/business/media/hip-hop-site-dajaz1s-copyright-case-ends-in-confusion.html?_r=1.

C. Disorder's Delights

Third, the current state of Internet governance is a cacophony: it involves a confusing panoply of governments, private companies, public benefit corporations, non-profit organizations, international organizations, and ad hoc agglomerations of private citizens.[85] Efforts to describe the state of play of governance are book-length and always out of date. And yet, this chaos – while eluding description via organization chart – has a virtue for proponents of free speech. The core Internet protocols prioritize robust, open communication over countervailing values such as guaranteed reliability or authentication.[86] (They likely embed the normative perspective of their largely American, and at least North American, developers.) And, the combination of network effects and distributed governance has effectively prevented alteration to these initial value choices. Spam is the best example: despite widespread consensus on what constitutes junk e-mail, the Internet community has been utterly unable to reform core protocols such as TCP/IP or SMTP to mitigate spam's harms.[87] The mishmash of network address registries, DNS registrars, protocol developers, ICANN, governments, and engineers dissipates control, and helps to preserve the Internet's default settings of open, unintermediated communication.

Thus, perpetuating some level of bureaucratic competition – and gridlock – is a viable strategy for opponents of censorship. Providing any one entity, from the U.S. government to the ITU, with significant control over core Internet infrastructure risks allowing that entity to impose its view of permissible content on the Net as a whole. Such a risk might have seemed worth the gamble when the United States robustly defended unfettered communication. But that time is no more. Oddly enough, this suggests that the best path to resisting censorship is to support the U.S. position at WCIT-12. In effect, America seeks to defend the status quo, where broad multi-stakeholder involvement through ICANN is reified as the ideal, and where terrestrial governments are but one set of interested stakeholders.[88] The alternative, seemingly more multilateral approach envisions a much greater role for governments as decisionmakers for

---

[85] *See* MILTON MUELLER, RULING THE ROOT (2004 ed.).

[86] Bambauer, *supra* note 27 at 596; Chris Chambers et al., *TCP/IP Security*, LINUXSECURITY.COM, § 3.2, http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html.

[87] Bambauer, *supra* note 27 at 600-601.

[88] *See* Rebecca MacKinnon, *The United Nations and the Internet: It's Complicated*, FOREIGN POLICY, Aug. 8, 2012, http://www.foreignpolicy.com/articles/2012/08/08/the_united_nations_and_the_internet_it_s_complicated?page=0,0.

Internet governance.[89] This consolidation would provide greater voice to states with less robust views of free speech, in a venue (the ITU) where those voices are far louder. In short, those concerned about censorship should push for gridlock, and for dissipated control.

D. A Right to Read

Fourth, citizens must assert a default right of access to information. While this right cannot be absolute, it must be the baseline. Governments must be expected to justify restrictions on communication by reference to countervailing values, and to clear and present threats to those values. This position also helpfully frames expectations: citizens should expect that they can receive information from a willing speaker. Deviations from that norm are anomalous. A right of access is enshrined in the Universal Declaration of Human Rights.[90] However, it exists only in inchoate form in American constitutional jurisprudence – most free speech cases emphasize the rights of speakers, not listeners / viewers / readers.[91] Emphasizing the rights of receivers would provide greater opportunity to challenge restrictions to which both government and intermediaries (who may qualify as speakers) agree. Admittedly, this position takes a different perspective on free speech values – it prioritizes effects on listeners. However, this approach is consonant with speakers' rights, since it does not force anyone to convey information, and is also aligned with the First Amendment interests in self-governance and autonomy.[92]

E. The Censor's Handmaidens

Finally, citizens need to experiment with methods that address corporate involvement in censorship.[93] The U.S. has seen an array of such measures, from pressure on corporations through socially responsible investment funds[94] to tort lawsuits against firms involved in censorship[95]. In

---

[89] *Id.*
[90] Art. 19, Univ. Decl. of Human Rts.
[91] Bambauer, *supra* note 1 at 156-58.
[92] ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1948); *Whitney v. California*, 274 U.S. 357, 372-80 (1927) (Brandeis, J., concurring); Brian C. Murchison, *Speech and the Self-Governance Value*, 14 WM. & MARY BILL OF RTS. J. 1251 (2006).
[93] *See* Derek E. Bambauer, *Cool Tools for Tyrants*, LEGAL AFFAIRS, Jan./Feb. 2006, http://legalaffairs.org/issues/January-February-2006/feature_bambauer_janfeb06.msp.
[94] *See, e.g.*, Boston Common Asset Management, *Investors Representing Over $580 million in Cisco Shares Are Urging Cisco to Respond to Human Rights Risk in its Global Operations*, Nov. 10, 2009, http://www.bostoncommonasset.com/news/cisco111009.html.

particular, efforts should concentrate in three areas: firms' willingness to restrict access to material based on governmental requests (rather than lawfully generated orders)[96]; sales to states that censor their citizens' access to information[97]; and companies' willingness to disclose their content policies, along with their care in following them[98]. There are a variety of possible methods to effectuate these goals. Legislation could restrict corporate actions, or at least require reporting of them.[99] Civic organizations and journalists can document firms' activities, leading to market-based pressures from reputational sanctions.[100] From protests to purchasing decisions, citizens have considerable power to hold companies accountable. No single method is likely to check the profit motive that pushes corporations to assist in censorship. But, a combination of tactics can provide a counterbalancing force that helps protect open communication.

These five proposals are a partial response. The goal is to create a checking function for censorship – to put in place breakwaters that protect open Internet communication as a default, and as a core human value. They do not seek to prevent all censorship. Rather, these methods attempt to force careful weighing of free speech against countervailing concerns, and to ensure that censorship is as open, transparent, narrow, and accountable as possible.

IV. CONCLUSION

Censorship has evolved into a more sinister model, where state restrictions on information are less transparent, less accountable, and less vulnerable to challenge. Yet, the battles in the United States over censorship legislation, and internationally over the Anti-Counterfeiting Trade Agreement, lend hope for citizen-led resistance. Not all censorship is evil. But if states are to block access to information, they must operate openly, and must substantiate their actions with careful, grounded justification. As

---

[95] *See, e.g., Daobin v. Cisco Sys.*, No. 8:11-01538-PJM (D. Md. 2011) (suit filed by Falun Gong practitioners against Cisco based on Cisco's involvement in creating China's Golden Shield censorship system).

[96] Yahoo!, for example, has been particularly assiduous in voluntarily assisting China in censorship. Eli Milchman, *Yahoo "Strictest Censor" in China*, WIRED, June 15, 2006, http://www.wired.com/politics/onlinerights/news/2006/06/71166.

[97] *See, e.g., Canadian software used to censor Web abroad, help repressive regimes filter online content*, VANCOUVER OBSERVER, Aug. 1, 2011, http://www.vancouverobserver.com/world/canada/2011/08/01/canadian-software-used-censor-web-abroad-help-repressive-regimes-filter.

[98] *See, e.g., Google Transparency Report*, http://www.google.com/transparencyreport/.

[99] *See* H.R. 3605, Global Online Freedom Act of 2011 (112th Cong., 2011), http://www.govtrack.us/congress/bills/112/hr3605.

[100] Rebecca MacKinnon, *Shi Tao, Yahoo!, and the lessons for corporate social responsibility*, Dec. 30, 2007, http://rconversation.blogs.com/YahooShiTaoLessons.pdf.

censors evolve, so too users and authors must adapt, maintaining a balance between information and control.

* * *