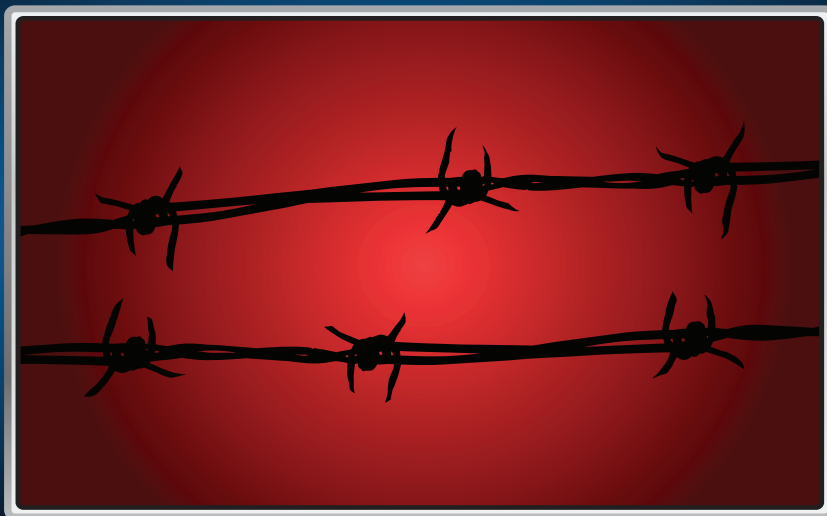


BY DEREK E. BAMBAUER



DEREK E. BAMBAUER

is an Associate Professor of Law at the University of Arizona James E. Rogers College of Law. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Robert Glennon, Dan Hunter and Thanh Nguyen. The author welcomes comments at derekbambauer@email.arizona.edu.

Saudi Arabia censors the Internet because it fears blasphemy. Britain censors it to interdict child pornography. America does so to block sales of fake NFL shirts and downloads of pop songs.

Americans—especially lawyers—are invariably surprised to learn that their government censors the Internet. And they should be surprised to learn why it does so. Such actions seem in tension with the country's robust protection for unfettered discourse, including hate speech, lies about one's military record, and video games featuring graphic disembowelment.¹ Those versed in the history of U.S. Internet regulation recall that a pair of seminal Supreme Court cases rejected congressional attempts to prevent minors from reaching sexually explicit material online.² Moreover, just last winter, an unprecedented wave of political advocacy by Silicon Valley, Netizens and civic groups beat back attempts to pass laws cutting off sites that allegedly infringed IP from funding and access by American users.³ The war against

Internet censorship seemed won. What happened?

In this article, I trace briefly the rise of the new American way of censorship. Next, I suggest a rationale grounded in public choice theory for why censorship of porn failed, but that of IP infringement succeeded. Put simply, porn has a posse, and peer-to-peer does not. Finally, I argue that while curtailing IP infringement is a worthwhile pursuit, the means currently employed pose significant risk to other key American values, such as due process, transparency and accountability.

Censorship Reborn

One of the Internet's founding myths is that censorship is made impossible by the network's adaptable, end-to-end architecture. Countries such as China and Saudi Arabia quickly proved that wrong, successfully designing their networks to block access to disfavored content. Because America's network architecture did not permit centralized technological restric-

tions, would-be censors turned to law. Driven by concerns over the ready access to pornography online, the federal government passed restrictive legislation shortly after the Net opened to commercial content. The first bill, hastily and inartfully drafted, contained two provisions. One banned knowing transmission of obscene or indecent communications to anyone known to be under age 18.⁴ The second prohibited displaying online, in a way accessible to minors, any patently offensive communication depicting or describing sexual or excretory activities or organs.⁵ Although the statute created a set of affirmative defenses, several—such as adult access codes or adult personal identification numbers—existed only in the congressional imagination, and others were wholly ineffective in preventing access by minors.⁶ The statute's vagueness in specifying prohibited content, and the effects upon speech lawful for adults, led the Supreme Court to strike down those provisions of the Communications Decency Act (CDA)

based on the First Amendment in *Reno v. ACLU*.⁷

Undaunted, Congress tried again. Looking to language in the prior case's dissenting opinion, the Child Online Protection Act (COPA) sought to mirror the Supreme Court's obscenity test.⁸ It restricted the law's ambit to commercial material harmful to minors that was designed to appeal to prurient interests, depicted sexual acts or organs, and lacked serious literary, artistic, political or scientific values for minors.⁹ The statute provided for affirmative defenses similar to the CDA, though no less ephemeral.¹⁰

The Supreme Court again invalidated Congress' censorship attempt in *Ashcroft v. ACLU*. Though the justices no longer viewed the statute as insolubly vague, they found there existed alternative means of protecting minors with fewer detrimental effects upon speech—in particular, end-user filtering software. (This broadening of the Court's scope of regulatory options is a fascinating instantiation of Larry Lessig's New Chicago School taxonomy of mechanisms for altering behavior.¹¹) The Court was careful not to foreclose regulation of online smut, but it clearly signaled the difficulty such statutes would have in surviving scrutiny.

For nearly a decade after COPA's passage, Internet censorship in the United States was mostly dead. A number of states re-fought *Ashcroft* by passing COPA-like statutes, with predictable results, but Congress moved on to less direct tactics, such as conditioning funding for public libraries on the installation of filtering soft-

Censorship is resurgent. Yet its focus has shifted from pornography in the 1990s and early 2000s to intellectual property infringement today.

ware, or establishing second-level domains (.kids.us) within which material harmful to minors was contractually prohibited.¹² Most observers saw America's free speech protections as exemplary, if not outright exceptional, in an international environment of increasingly pervasive censorship.

Yet there has been a recent sharp increase in America's Internet censorship. While there were sporadic efforts under President George W. Bush, such as seizure of domain names owned by travel agencies enabling Cuban tourism, the real resurgence took place under President Barack Obama.¹³ (One notes the irony, given the Obama administration's advocacy for Internet freedom in the Middle East, and for network neutrality domestically.) The administration has employed a number of indirect mechanisms—"soft censorship"—to surprisingly potent effect.

For example, the Departments of Homeland Security and Justice have seized more than 1,600 domain names for Web sites offering counterfeit National Football League jerseys, streaming Premier League soccer matches, and storing putatively unauthorized copies of hip-hop music.¹⁴

These seizures have, at times, resulted in exactly the overbreadth problems that troubled the Supreme Court in *Ashcroft* and *Reno*. When the government seized the mooo.com domain name, it knocked over 80,000 websites offline to capture 10 allegedly involved in child pornography. The mooo.com action itself is unusual—only a handful of seizures have involved traditional censorship concerns, such as child pornography, or cybercrime issues, such as botnets.¹⁵

The federal government has employed other censorship means. Congress included provisions in the Higher Education Opportunity Act (HEOA) of 2008 that require institutions of higher education to undertake technology-based deterrence measures against copyright infringement via peer-to-peer networks.¹⁶ Governments at all levels employ filtering software to prevent employees and ordinary citizens who use their wireless networks from reaching disfavored material. The Obama administration's IP Enforcement Coordinator pressed ISPs to take proactive measures against alleged file-sharers on their networks, even though service providers were already legally immune from suit under the Digital Millennium Copyright Act.¹⁷ Senators and State Department officials pressured Amazon, Domain Name Service registrars, and payment processors to stop providing services to WikiLeaks after the site released sensitive U.S. military and diplomatic materials.

Censorship, in short, is resurgent. Yet its focus has shifted significantly: from pornography in the 1990s and early 2000s to intellectual property infringement today. The next section explains this shift, and analyzes why the new American Way of Censorship has been more successful than initial efforts.

INTERNET Timeline 1996

- U.S. Communications Decency Act (CDA) becomes law to prohibit distribution of indecent materials over the Net. A few months later a three-judge panel imposes an injunction against its enforcement. Supreme Court unanimously rules most of it unconstitutional in 1997.
- ISPs such as Sprint and MCI begin appearing.

INTERNET Timeline 1997

- The American Registry for Internet Numbers (ARIN) is established to handle administration and registration of IP numbers to the geographical areas currently handled by Network Solutions (InterNIC).
- The domain google.com was registered on Sept. 15, 1997. Google Inc. was formally incorporated on Sept. 4, 1998, and operated out of a garage in Menlo Park, Calif.
- *Reno v. ACLU*, 521 U.S. 844 (1997). The CDA's "indecent transmission" and "patently offensive display" provisions abridge "the freedom of speech" protected by the First Amendment. *The Court said the Internet was so expansive and so much of a "marketplace of ideas" that it deserved the highest level of First Amendment protection. The Court ruled that any restriction on content would require a compelling reason and would have to be narrowly tailored, and that the Act at issue did not pass that test.*

Porn, P2P and Public Choice

The new wave of censorship has succeeded where the initial one failed for two principal reasons. First, it satisfies the political demands of powerful interest groups, without facing countervailing pressures. Second, it operates more indirectly than the straightforward legislative

mandates challenged in *Ashcroft* and *Reno*. These mechanisms are less amenable to challenge than statutes. This last point, I argue, constitutes the most troubling aspect of the new censorship regime.

Censorship has strong support from politically and economically powerful actors. Opposition to pornography online came from all parts of the political spectrum—conservative evangelical groups and liberal feminist ones both favored restrictions. For the latest wave, the Recording Industry Association of America and the Motion Picture Association of America, two Hollywood giants, have both taken firm stands in favor of greater IP enforcement, including censorship legislation such as the Stop Online Piracy Act (SOPA) and the PROTECT IP Act. Similarly, the fashion industry and professional sports leagues have supported domain name seizures. These groups have a concentrated pecuniary interest in enforcing IP laws via Internet censorship, and they lobby accordingly.

With censorship of porn, there was an opposition with a direct financial interest in the outcome: the porn industry itself. While outgunned, groups such as the Free Speech Coalition could organize chal-

lenges and lobby for the industry's interests (often disguised as free speech concerns). By contrast, opposition to IP-related censorship is dispersed, relatively impetuous, and politically weak. There is no lobbying group for P2P users or streaming sites. Indeed, some targets of the new wave are foreign, further reducing their political clout. This public choice story explains, ironically, why formal attempts to codify censorship—SOPA and PROTECT IP—failed. The bills moved through Congress with lightning speed until segments of the IT community, such as ISPs and Google, recognized the potential economic impact for their businesses. They swiftly mounted an expensive and effective campaign that combined lobbying with media pressure. And they succeeded.

The popular image of the defeat of SOPA/PROTECT IP is of the Internet going dark—of blackouts of sites such as Reddit and Wikipedia in protest, and of petitions by outraged Internet users. This is a lovely story, but it is a story: The real work of opposition was performed by newly energized corporate actors with financial interests on the line. Soft censorship does not threaten these entities' businesses, and that is why it thrives while leg-

islative initiatives failed.

The indirect nature of the new wave of censorship—which relies on pretext-based use of general-purpose statutes, informal pressures, and funding-based incentives—makes it more difficult to challenge. First, the federal government faces few constitutional constraints on its spending power. Indeed, Congress can even engage in viewpoint-based discrimination in funding, if it frames such restrictions elliptically.¹⁸ Thus, the government can condition its largesse upon agreement by institutions such as libraries and universities to censor their networks.¹⁹ Second, courts rarely second-guess how the executive implements laws of general application, so long as there is no overt invidious intent. The civil forfeiture provisions of the PRO IP Act of 2008, while opaque, manifest no such discriminatory purpose. The decision to employ them to pursue, principally, pirates rather than pornographers is one conferred upon executive agencies. Finally, informal pressures—such as the Obama administration's role in the negotiations between ISPs and content producers over the new Copyright Alert System (CAS)—evade judicial review because they do not involve sufficient state action.²⁰ Jawboning is not unconstitutional.

This pattern presents an irony: The government may do indirectly what it may not do directly, even when such actions are less accountable, less trans-

INTERNET Timeline 1998

- Electronic postal stamps become a reality, with the U.S. Postal Service allowing stamps to be purchased and downloaded for printing from the Web.
- U.S. enters into an agreement with the Internet Corporation for Assigned Numbers (ICANN) to establish a process for transitioning DNS from U.S. Government management to industry.
- Digital Millennium Copyright Act of 1998 passed.

endnotes

1. *Nat'l Socialist Party v. Village of Skokie*, 432 U.S. 43 (1977); *U.S. v. Alvarez*, 567 U.S. ___ (2012); *Brown v. Ent'mt Merchants Ass'n*, 564 U.S. ___ (2011).
2. *Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997); *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656 (2004).
3. Eric Goldman, *Celebrating (?) the Six-Month Anniversary of SOPA's Demise*, FORBES, July 18, 2012, www.forbes.com/sites/eric-goldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopas-demise/.

4. *Reno*, 521 U.S. at 859 (describing then-47 U.S.C. § 223(a)).
5. *Id.* at 860 (describing then-47 U.S.C. § 223(d)).
6. *Id.* at 860 n.26, 876-77.
7. *Id.* at 876-886.
8. *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. at 656 (striking down 47 U.S.C. § 231); see *Reno*, 521 U.S. at 895-96 (O'Connor, J., dissenting). The obscenity test is set out in *Miller v. California*, 413 U.S. 15 (1973).
9. *Ashcroft*, 542 U.S. at 661-662 (describing then-U.S.C. 47 § 231(e)(6)).

10. *Id.* at 674 (Stevens, J., concurring).
11. Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662-66 (1998).
12. 20 U.S.C. §§ 6801, 6777, 9134 and 47 U.S.C. § 254; 47 U.S.C. § 941. For state laws, see, e.g., *Am. Booksellers Found. for Free Expression v Sullivan*, 799 F. Supp. 2d 1078, 1080-81 (D. Alaska 2011).
13. See Adam Liptak, *A Wave of the Watch List, and Speech Disappears*, N.Y. TIMES, Mar. 4, 2008, at A16.
14. See U.S. INTELLECTUAL PROPERTY ENFORCEMENT

COORDINATOR, 2011 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR JOINT STRATEGIC PLAN: ONE YEAR ANNIVERSARY 5 (June 2011), online at www.whitehouse.gov/sites/default/files/ipcec_anniversary_report.pdf; Jennifer Martinez, *US government dismisses piracy case against Rojadirecta site*, THE HILL, Aug. 29, 2012, <http://thehill.com/blogs/hillconvalley/technology/246529-us-government-dismisses-case-against-rojadirecta>; David Kravets, *Feds Seized Hip-Hop Site for a Year, Waiting for Proof of Infringement*, WIRED, May 3,

parent, and less open to judicial review. This article closes by arguing that this state of affairs threatens core, shared American constitutional values.

Bowdlerizing Badly

The new American way of censorship is hardy: It is designed to resist challenge. With domain name seizures, for example, the federal government acts first and justifies later. When it makes a mistake—as it did in seizing the music blog Dajaz1, a conduit for covertly leaked yet legitimate music—the Obama administration has stalled, obfuscated and then dropped its efforts rather than face judicial scrutiny. (So, too, with the Rojadirecta streaming site.) Civil forfeiture provisions enable the government to censor first, employing *ex parte* procedures, and place the burden on the domain name owner to recover the site later. Funding pressures upon libraries and schools press them not only to filter, but to outsource content categorization to private software companies. And participation in closed-door negotiations (such as those over CAS) lets the government cloak its agenda as part of putatively private bargains.

These characteristics are troubling. Reducing intellectual property infringement is indubitably a worthwhile goal. IP production is a significant component of the U.S. economy. Yet the new model of censorship threatens core constitutional values. We generally insist that the government operate openly, transparently and

accountably. We demand that it admit to its actions; identify how it is pursuing avowed goals; and submit not only to political processes, but to the checks and counter-majoritarian constraints of judicial review. We demand due process.

Our new censorship regime falls short on each count. The government does not admit its role in pressuring private parties to adopt its agenda, and it frames its censorship as protecting property rights, or other euphemisms, rather than admitting and defending its content restraints. Similarly, the Obama administration has continually stalled, hidden information, and stonewalled in the few instances where censorship has been challenged. This poses a key question: If the government is engaging in salutary measures, why will it not defend them openly and transparently? Lastly, the government has stacked the

The federal government acts first and justifies later. It has stalled, obfuscated and then dropped its efforts rather than face judicial scrutiny.

censorship deck: Some of its methods are designed to evade judicial review, and when the administration has been hauled into court, it has sought to delay the inevitable, and then dropped its cases without explanation.

America has a profound commitment to free speech and free expression. Perhaps threats to intellectual property merit compromises of those commitments. But if they do, then our government should be willing to acknowledge that it is censoring the Internet, to explain why it does so, and to defend it openly. The new, American way of censorship poses a little-noticed threat to important shared values. ¹⁵

- 2012, www.wired.com/threatlevel/2012/05/weak-evidence-seizure/.
15. See, e.g., U.S. Dep't of Justice, *Federal Courts Order Seizure of Website Domains Involved in Advertising and Distributing Child Pornography*, Feb. 15, 2011, www.justice.gov/opa/pr/2011/February/11-crm-189.html; Public Interest Registry, *2011 Takedown Notices*, Apr. 12, 2011, <http://pir.org/why/takedowns2011>.
 16. 34 C.F.R. § 668.14(b)(30).
 17. 17 U.S.C. § 512.
 18. *Rust v. Sullivan*, 500 U.S. 173 (1991).
 19. *U.S. v. Am. Library Ass'n*, 539 U.S. 194 (2003); 34 C.F.R. § 668.14(b)(30).
 20. *Copyright Alert System (CAS)*, Center for Copyright Information, www.copyrightinformation.org/alerts.