# THE MYTH OF PERFECTION

*Derek E. Bambauer**

Cyberlaw is plagued by the myth of perfection.

Consider three examples: censorship, privacy, and intellectual property. In each, the rhetoric and pursuit of perfection has proved harmful, in ways this Essay will explore. And yet the myth persists—not only because it serves as a potent metaphor, but because it disguises the policy preferences of the mythmaker. Scholars should cast out the myth of perfection, as Lucifer was cast out of heaven. In its place, we should adopt the more realistic, and helpful, conclusion that often good enough is . . . good enough.

Start with Internet censorship. Countries such as China, Iran, and Vietnam use information technology to block their citizens from accessing on-line material that each government dislikes. Democracies, too, filter content: Britain blocks child pornography using the Cleanfeed system,[1] and South Korea prevents users from reaching sites that support North Korea's government.[2] This filtering can be highly effective: China censors opposition political content pervasively,[3] and Iran blocks nearly all pornographic sites (along with political dissent).[4] However, even technologically sophisticated systems, like China's Golden Shield, are vulnerable to circumvention. Users can employ proxy servers or specialized software, such as Tor, to access proscribed sites.[5] This permeability has led many observers to conclude that effective censorship is impossible, because censorship is inevitably

* Associate Professor of Law, Brooklyn Law School (through spring 2012); Associate Professor of Law, University of Arizona James E. Rogers College of Law (beginning fall 2012). Thanks for helpful suggestions and discussion are owed to Jane Yakowitz Bambauer, Dan Hunter, Thinh Nguyen, Derek Slater, and Chris Soghoian. The author welcomes comments at derek.bambauer@brooklaw.edu.

1. Richard Clayton, *Failures in a Hybrid Content Blocking System*, *in* PRIVACY ENHANCING TECHNOLOGIES: 5TH INTERNATIONAL WORKSHOP PET 2005 78 (George Danezis & David Martin eds., 2006).

2. Eric S. Fish, *Is Internet Censorship Compatible With Democracy? Legal Restrictions of Online Speech in South Korea*, ASIA-PAC. J. HUM. RTS. & THE L. (forthcoming 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1489621.

3. *China*, OpenNet (June 15, 2009), http://opennet.net/research/profiles/china-including-hong-kong.

4. *Iran*, OpenNet (June 16, 2009), http://opennet.net/research/profiles/iran.

5. *See, e.g.*, James Fallows, *"The Connection Has Been Reset"*, THE ATLANTIC (March 2008), http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/.

imperfect.[6] Filtering is either trivially easy to bypass, or doomed to failure in the arms race between censors and readers. The only meaningful censorship is perfect blocking, which is unattainable.

And yet, leaky Internet censorship works. Even in authoritarian countries, few users employ circumvention tools.[7] Governments such as China's capably block access to most content about taboo subjects, such as the Falun Gong movement[8] or coverage of the Arab Spring uprisings.[9] Those who see imperfect censorship as useless make three errors. First, they ignore offline pressures that users face. Employing circumvention tools is like using a flashlight: it helps find what you seek, but it draws attention to you. China has become adept at detecting and interfering with Tor,[10] and Iran recently purchased a sophisticated surveillance system for monitoring Internet communications.[11] Bypassing censorship in cyberspace may have adverse consequences in realspace. Second, most Internet users are not technologically sophisticated. They use standard software, and the need to install and update specialized circumvention tools may be onerous.[12] Finally, governments do not need perfect censorship to attain their goals. They seek to prevent most people from obtaining prohibited content, not to banish it entirely. Censorship that constrains the average user's ordinary web browsing generally suffices.

Privacy discourse too is obsessed with perfection. The reidentification wars have pitted researchers who assert that anonymizing data is impossible[13] against those who argue the risk of

---

6. *See, e.g.*, Oliver August, *The Great Firewall: China's Misguided—and Futile—Attempt to Control What Happens Online*, WIRED (Oct. 23, 2007), http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all; Troy Hunt, *Browsing the broken Web: A Software Developer Behind the Great Firewall of China*, TROY HUNT'S BLOG (Mar. 16, 2012), http://www.troyhunt.com/2012/03/browsing-broken-web-software-developer.html; Weiliang Nie *Chinese Learn to Leap the "Great Firewall"*, BBC NEWS (Mar. 19, 2010), http://news.bbc.co.uk/2/hi/8575476.stm.

7. Erica Naone, *Censorship Circumvention Tools Aren't Widely Used*, TECH. REV. (Oct. 18, 2010), http://www.technologyreview.com/web/26574/.

8. *China*, *supra* note 3.

9. Richard Fontaine & Will Rogers,*China's Arab Spring Cyber Lessons*, THE DIPLOMAT (Oct. 3, 2011), http://the-diplomat.com/2011/10/03/china%E2%80%99s-arab-spring-cyber-lessons/.

10. Tim Wilde, *Knock Knock Knockin' on Bridges' Doors*, TOR (Jan. 7, 2012), https://blog.torproject.org/blog/knock-knock-knockin-bridges-doors.

11. Phil Vinter, *Chinese Sell Iran £100m Surveillance System Capable of Spying on Dissidents' Phone Calls and Internet*, DAILY MAIL (Mar. 23, 2012), http://www.dailymail.co.uk/news/article-2119389/Chinese-sell-Iran-100m-surveillance-capable-spying-dissidents-phone-calls-internet.html.

12. *See generally* Nart Villeneuve, *Choosing Circumvention: Technical Ways to Get Round Censorship*, *in* REPORTERS WITHOUT BORDERS, HANDBOOK FOR BLOGGERS AND CYBERDISSIDENTS 63 (2005), *available at* http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf.

13. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1752 (2010); Latanya Sweeney, *Patient Identifiability in Pharmaceutical Marketing Data*,

breaching properly sanitized datasets is vanishingly small.[14] While the arguments are dauntingly technical (for those unfamiliar with advanced statistics), the empirical evidence points toward the less threatening conclusions. The only rigorous study demonstrating an attack on a properly de-identified dataset under realistic circumstances revealed but 2 out of 15,000 (.013%) participants' identities.[15] Moreover, critics of anonymized data overlook the effects of incorrect matches. Attackers will have to weed out false matches from true ones, complicating their task.

Opponents make three mistakes by focusing on the theoretical risk of re-identification attacks on properly sanitized data. First, the empirical evidence for their worries is slight, as the data above demonstrates. There are no reports of such attacks in practice, and the only robust test demonstrated minimal risk. Second, anonymized data is highly useful for socially beneficial purposes, such as predicting flu trends, spotting discrimination, and analyzing the effectiveness of medical and legal interventions.[16] Finally, the most significant privacy risk is from imperfectly sanitized data: organizations routinely release, deliberately or inadvertently, information that directly identifies people, or that enables an attacker to do so without advanced statistical knowledge. Examples are legion, from the California firm Biofilm releasing the names and addresses of 200,000 customers who asked for free Astroglide samples[17] to AOL's disclosure of user queries that allowed researchers to link people to their searches.[18] Concentrating on whether perfect anonymization is possible distracts from far more potent privacy threats emanating from data.

Intellectual property ("IP") in the digital age is similarly obsessed with perfection. IP owners argue that with the advent of perfect digital copies, high-speed networks, and distributed dissemination technologies, such as peer-to-peer file-sharing software, any infringing copy of a protected work will spread without limit, undermining incentives to create. This rhetoric of explosive peril has

---

(Data Privacy Lab, Working Paper No. 1015, 2011), *available at* http://dataprivacylab.org/projects/identifiability/pharma1.html.

14. *See, e.g.*, Jane Yakowitz, *The Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 52 (2011); Khaled El Emam et al., *A Systematic Review of Re-identification Attacks on Health Data*, PLOS ONE (Dec. 2011), http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.002807.

15. Deborah Lafky, Program Officer, Dep't Health and Human Servs., *The Safe Harbor Method of De-Identification: An Empirical Test, ONC Presentation* (October 9, 2009), *available at* http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf.

16. *See* Yakowitz, *supra* note 14.

17. Christopher Soghoian, *Astroglide Data Loss Could Result in $18 Million Fine*, DUBFIRE (July 9, 2007), http://paranoia.dubfire.net/2007/07/astroglide-data-loss-could-result-in-18.html.

18. Katie Hafner, *Leaked AOL Search Results Create Ethical Dilemma for Researchers*, N.Y. TIMES (Aug. 23, 2006), http://www.nytimes.com/2006/08/23/technology/23iht-search.2567825.html?pagewanted=all.

resulted in a perpetual increase in the protections for copyrighted works and in the penalties for violating them.[19]

The quest for perfect safeguards for IP predates the growth of the commercial Internet. In September 1995, President Clinton's administration released its White Paper, which argued that expanded copyright entitlements were necessary for content owners to feel secure in developing material for the nascent Information Superhighway.[20] Without greater protection, the Paper argued, the Superhighway would be empty of content, as copyright owners would simply refuse to make material available via the new medium.

This prediction proved unfounded, but still persuasive. In the last fifteen years, Congress has reinforced technological protection measures such as Digital Rights Management with stringent legal sanctions;[21] has augmented penalties for copyright infringement, including criminal punishments;[22] has pressed intermediaries, such as search engines, to take down allegedly infringing works upon notification by the copyright owner;[23] and has dedicated executive branch resources to fighting infringement.[24] And yet, pressures from content owners for ever-greater protections continue unrelentingly. In the current Congress, legislation introduced in both the House of Representatives and the Senate would, for the first time in American history, have authorized filtering of sites with a primary purpose of aiding infringement[25] and would have enabled rightsowners to terminate payment processing and Internet advertising services for such sites.[26] These proposals advanced against a backdrop of relatively robust financial health for the American movie and music industries.[27]

---

19. *See generally* ROBERT LEVINE, FREE RIDE: HOW DIGITAL PARASITES ARE DESTROYING THE CULTURE BUSINESS, AND HOW THE CULTURE BUSINESS CAN FIGHT BACK (2011); JESSICA LITMAN, DIGITAL COPYRIGHT (2001); Mike Masnick, *Why Is The MPAA's Top Priority "Fighting Piracy" Rather Than Helping the Film Industry Thrive?*, TECHDIRT (Feb. 22, 2011), http://www.techdirt.com/articles/20110221/15024713194/why-is-mpaas-top-priority-fighting-piracy-rather-than-helping-film-industry-thrive.shtml.

20. Pamela Samuelson, *The Copyright Grab*, WIRED (Jan. 1996), http://www.wired.com/wired/archive/4.01/white.paper.html.

21. 17 U.S.C. § 1201 (2006).

22. 17 U.S.C. § 1204 (2006); No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997).

23. 17 U.S.C. § 512(c) (2006).

24. Prioritizing Resources and Organization for Intellectual Property (PRO IP) Act, Pub. L. No. 110-403, 122 Stat. 4256 (2008).

25. PROTECT IP Act of 2011, S.968, 112th Cong. (2012).

26. Stop Online Piracy Act of 2011, H.R. 3261, 112th Cong. (2012).

27. Robert Andrews, *Music Industry Can See The Light After "Least Negative" Sales Since 2004*, TIME (Mar. 26, 2012), http://business.time.com/2012/03/26/music-industry-can-see-the-light-after-least-negative-sales-since-2004/; Brooks Barnes, *A Sliver of a Silver Lining for the Movie Industry*, N.Y. TIMES (Mar. 22, 2012), http://mediadecoder.blogs.nytimes.com/2012/03/22/a-sliver-of-a-silver-lining-for-the-movie-industry/#; Bob Lefsetz, *Movie Industry Is Making Money from*

Thus, the pursuit of perfection in IP also contradicts empirical evidence. Content industries have sought to prohibit, or at least hobble, new technologies that reduce the cost of reproduction and dissemination of works for over a century—from the player piano[28] to the VCR[29] to the MP3 player[30] to peer-to-peer file-sharing software.[31] And yet each of these advances has opened new revenue horizons for copyright owners. The growth in digital music sales is buoying the record industry,[32] and the VCR proved to be a critical profit source for movies.[33] New copying and consumption technologies destabilize prevailing business models, but not the production of content itself.[34]

Moreover, perfect control over IP-protected works would threaten both innovation and important normative commitments. The music industry crippled Digital Audio Tapes[35] and failed to provide a viable Internet-based distribution mechanism until Apple introduced the iTunes Music Store.[36] The movie industry has sought to cut off supply of films to firms such as Redbox that undercut its rental revenue

---

*Technologies It Claimed Would KILL Profits*, THE BIG PICTURE (Jan. 30, 2012, 4:30 PM), http://www.ritholtz.com/blog/2012/01/movie-industry-is-making-money-from-technologies-it-claimed-would-kill-profits/.

28. *See* White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1, 13–14 (1908) (holding that a piano roll does not infringe composer's copyright because the perforated sheets are not copies of the sheet music).

29. *See* Sony v. Universal Studios, 464 U.S. 417, 442 (1984) (holding that the manufacture of a VCR does not constitute contributory copyright infringement because it "is widely used for legitimate, unobjectionable purposes").

30. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., 180 F.3d 1072, 1081 (9th Cir. 1999) (upholding a district court denial of preliminary injunction against the manufacture of the Rio MP3 player because the Rio is not subject to the Audio Home Recording Act of 1992).

31. *See* Metro-Goldwyn-Mayer Studios v. Grokster, 545 U.S. 913, 918 (2005) (holding that distributor of peer-to-peer file sharing network is liable for contributory copyright infringement when "the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement").

32. Andrews, *supra* note 27.

33. Michelle Schusterman, *Infographic: Why the Movie Industry is So Wrong About SOPA*, MATADOR (Jan. 17, 2012), http://matadornetwork.com/change/infographic-why-the-movie-industry-is-so-wrong-about-sopa/.

34. *See generally* Mark A. Lemley, *Is the Sky Falling on the Content Industries?*, 9 J. TELECOMM. & HIGH TECH. L. 125 (2011) (explaining that while the introduction of new technologies in the past may have disrupted certain industries, the new technology did not stop the creation of new content).

35. *See generally* Tia Hall, *Music Piracy and the Audio Home Recording Act*, 2002 DUKE L. & TECH. REV. 0023 (2002).

36. Derek Slater et al., *Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries*, (Berkman Center for Internet & Society at Harvard Law School, Research Publication No. 2005-10, 2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=654602.

model,[37] and Apple itself has successfully used copyright law to freeze out companies that sold generic PCs running MacOS.[38] And, the breathing room afforded by the fair use and de minimis doctrines, along with exceptions to copyright entitlements, such as cover licenses, enables a thriving participatory culture of remixes, fan fiction, parody, criticism, and mash-ups. Under a system of perfect control, copyright owners could withhold consent to derivative creators who produced works of which they disapproved, such as critical retellings of beloved classics, for example *Gone With The Wind*,[39] or could price licenses to use materials beyond the reach of amateur artists.[40] Perfection in control over intellectual property is unattainable, and undesirable.

The myth of perfection persists because it is potent. It advances policy goals for important groups—even, perhaps, groups on both sides of a debate. For censorship, the specter of perfect filtering bolsters the perceived power of China's security services. It makes evasion appear futile. For those who seek to hack the Great Firewall, claiming to offer the technological equivalent of David's slingshot is an effective way to attract funding from Goliath's opponents. Technological optimism is a resilient, seductive philosophical belief among hackers and other elites[41] (though one that is increasingly questioned).[42]

Similarly, privacy scholars and advocates fear the advent of Big Data: the aggregation, analysis, and use of disparate strands of information to make decisions—whether by government or by private firms—with profound impacts on individuals' lives.[43] Their

---

37. Paul Bond, *Warner Bros., Redbox Divided on DVD Terms*, THE HOLLYWOOD REPORTER (Feb. 29, 2012), http://www.hollywoodreporter.com/news/warner-bros-redbox-dvd-ultraviolet-flixster-kevin-tsujihara-296071.

38. *See* Apple Inc. v. Psystar Corp., 658 F.3d 1150, 1162 (9th Cir. 2011).

39. *See* SunTrust Bank v. Houghton Mifflin Co., 268 F.3d 1257, 1275 (11th Cir. 2001) (denying a preliminary injunction because a fair use defense would prevent the plaintiff, owner of the copyright of *Gone With the Wind*, from preventing the defendant from publishing a novel that critiques *Gone With the Wind*).

40. *See generally* Derek E. Bambauer, *Faulty Math: The Economics of Legalizing* The Grey Album, 59 ALA. L. REV. 345 (2007) (contending the economics of the derivative works right prevents the creation of new works and stifles the re-mix culture).

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

42. *See generally* EVGENY MOROZOV, THE NET DELUSION (2011) (arguing that the Internet makes it easier for dictators to prevent democratic uprisings).

43. *See generally* JULIE COHEN, CONFIGURING THE NETWORKED SELF (2011) (making the case that flows of private information are not restricted and proposing legal reforms to address the problem); Jessica Litman, *Information Privacy / Information Property*, 52 STAN. L. REV. 1283 (2000) (contending that industry's self-regulation of information privacy has failed and proposing that torts may be the best available avenue to improve privacy rights); danah boyd & Kate Crawford, *Six Provocations for Big Data*, Symposium, *A Decade in Internet Time: Symposium on the Dynamics of Internet and Society*, OXFORD INTERNET

objections to disclosure of anonymized data are one component of a broader campaign of resistance to changes they see as threatening to obviate personal privacy. If even perfectly anonymized data poses risks, then restrictions on data collection and concomitant use gain greater salience and appeal.

Finally, concentrating on the constant threat to incentives for cultural production in the digital ecosystem helps content owners, who seek desperately to adapt business models before they are displaced by newer, more nimble competitors. They argue that greatly strengthened protections are necessary before they can innovate. Evidence suggests, though, that enhanced entitlements enable content owners to resist innovation, rather than embracing it. The pursuit of perfection turns IP law into a one-way ratchet: protections perpetually increase, and are forever insufficient.

We should abandon the ideal of the sublime in cyberlaw. Good enough is, generally, good enough. Patchy censorship bolsters authoritarian governments. Imperfectly anonymized data generates socially valuable research at little risk. And a leaky IP system still supports a thriving, diverse artistic scene. Pursuing perfection distracts us from the tradeoffs inherent in information control, by reifying a perspective that downplays countervailing considerations. Perfection is not an end, it is a means—a political tactic that advances one particular agenda. This Essay argues that the imperfect—the flawed—is often both effective and even desirable as an outcome of legal regulation.

---

INST. (Sept. 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431 (proposing six questions about the potential negative effects of Big Data).