Maryland Law Review

Volume 72 | Issue 2 Article 4

The Anonymous Internet

Bryan H. Choi

THE ANONYMOUS INTERNET

BRYAN H. CHOI*

ABSTRACT

This Article argues in favor of regulating online anonymity, not from the standpoint that doing so will prevent harmful abuses or improve security, but instead that refusing to do so will ultimately harm other liberty interests. One principle that has emerged from cyberlaw scholarship is that we should safeguard the Internet's "generativity"—a key attribute representing the latitude and plasticity with which a technology (like the Internet) can be adapted to perform new, unanticipated uses—because generativity is the root source of the Internet's unique vitality. Yet, if we want regulators to leave generativity alone, we must offer them another point of leverage with which to regulate abusive behavior. It is not enough to recommend simply that regulators should exercise restraint to minimize loss to generative potential.

The descriptive claim here is that the desire to regulate the Internet can manifest itself either as restrictions on anonymity or as restrictions on generativity, and that one can be traded for the other. The normative claim that follows is that we should favor the generative Internet over the anonymous Internet for at least two reasons. First, generativity is the engine that ignites the Internet's most essential and electrifying function, as a platform that perpetuates technological innovation and output. Second, restrictions on generativity impose restraints further upstream and are therefore more troubling than restrictions on anonymity. Third, anonymity is a value held

* Director of Law & Media, Information Society Project, Yale Law School. I thank Jack Balkin, Nicholas Bramble, Danielle Citron, Laura DeNardis, Victoria Ekstrand, Richard Fallon, Michael Froomkin, Heather Gerken, James Grimmelmann, Margot Kaminski, Brian Krebs, Daniel Kreiss, Lyrissa Lidsky, Christina Mulligan, John Palfrey, Seeta Peña Gangadharan, Andrew Selbst, Wendy Seltzer, Rebecca Wexler, and Jonathan Zittrain, as well as the participants in workshops at the Berkman Center, the Information Society Project, and the Kauffman Foundation, for extraordinarily helpful comments, suggestions, and guidance. I am also grateful to the Kauffman Foundation and Thomson Reuters for financial support. All opinions, errors, and omissions are my own.

in only modest esteem—the so-called constitutional "right to anonymity" is a narrow protection that does not contemplate the unbridled use of anonymizing technologies. Thus, where regulatory goals are being pursued, we should encourage Internet regulators to look to limitations on anonymity as a means of averting more onerous limitations on generativity.

TABLE OF CONTENTS

I. INTRODUCTION

The Internet has made anonymity seem like an entitlement. We have become accustomed to assuming that we are hidden in obscurity within the confines of our computer screen. The early days of "signing online"—literally, signing one's account number or screenname as authorization to access a networked line—have been succeeded by always-on broadband that never prompts for any personal login information.[1] We are not asked for identification when we browse most websites and, when we are, we select monikers that are fanciful and disposable.[2] If real identity is required, such as to check one's bank

1. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 32 (2008) (noting that CompuServe and AOL were "built to identify the people using [the network]," whereas today, "[u]ser identification is left to individual Internet users and servers to sort out if they wish to demand credentials of some kind from those with whom they communicate").

2. *See, e.g.*, Richard Siklos, *A Virtual World but Real Money*, N.Y. TIMES, Oct. 19, 2006, at C1 (reporting that on Second Life, "an online service . . . that allows computer users to create a new and improved digital version of themselves," most of the users "have chosen their names from a whimsical menu of supplied surnames, resulting in monikers like

account balance, it is always requested separately, further bolstering the illusion that authenticated realms are distinct islands that are visited only at the prerogative of the user.[3]

The activities of groups like Anonymous, LulzSec, and WikiLeaks, as well as the uses of Internet-based organizing during the recent Arab Spring revolutions, have enhanced the romanticism and notoriety of anonymity.[4] The idea that anonymity can provide a check on abusive power is deeply appealing. Yet, anonymity can be abused in turn;[5] those who criticize anonymity argue that it breeds its own form of unaccountability.[6] Asking whether anonymity is good or bad is the wrong question, because our instincts change depending on whose anonymity is at issue. We know that some anonymity must be preserved, yet we worry that the Internet currently offers too much anonymity. We also know that anonymity is a fragile construct, and so we fear that altering the balance might compromise too much. The resulting reluctance to confront anonymity on its face has led to seeming paralysis in the near term. In the longer term, that hesitation will squeeze out the real value of the Internet.

While anonymity has been a longstanding attribute of the Internet, this Article will argue that preserving it will increasingly come at the expense of another attribute that is arguably more essential to the Internet's exceptionalism. In a set of recent publications, Jonathan Zittrain has posited that the key to the Internet's success is "generativity," a quality he defines as *"a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences."*[7]

Snoopybrown Zamboni and Bitmason Pimpernel"). *But see* Catherine Greenman, *On the Net, Curiosity Has a Price: Registration*, N.Y. TIMES, Dec. 23, 1999, at G8 ("N[o] matter where you go on the Internet these days, it seems you won't get very far without first registering, signing in or becoming a 'member,' all of which require that you provide your name, your e-mail address and other personal information.").

3. *Cf.* ZITTRAIN, *supra* note 1, at 32–33 ("[A] particular Web site might demand that a user create an ID and password in order to gain access to its contents[, but b]ecause the user does not have to log in [to the Internet] the way he or she would to use a proprietary service, identity is obscured.").

4. *See, e.g.*, Quinn Norton, *2011: The Year Anonymous Took on Cops, Dictators and Existential Dread*, WIRED (Jan. 11, 2012, 6:00 AM), http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/all/.

5. *See infra* Parts II–III.A.

6. *See infra* Part III.A.

7. ZITTRAIN, *supra* note 1, at 70; *see id.* at 101 ("[T]he generative nature of the PC and Internet . . . is both the cause of their success and the instrument of their forthcoming

In other words, generativity is the essential ingredient of innovation, representing the freedom to tinker and to transform a technology far beyond its originally intended uses.[8]

Generative technologies do not know what they want to be when they grow up. As an analog, paper is highly generative because it can be adapted to accomplish any number of tasks, such as writing, wrapping fish, flying kites, storing gunpowder, and so on.[9] The set of possible uses for paper is diverse and expanding, not fixed upon fabrication. Not all technologies are endowed with equal generative potential.[10] For example, LEGO blocks are a more generative tool than jigsaw puzzle pieces, because LEGO blocks are more open-ended and allow for more variations and permutations. Smartphones are more generative than landline phones. The potency of the Internet, and of digital computing more generally, is that it has been one of the most generative technologies we have ever encountered.[11]

But by the same token, that versatility is a double-edged sword: generativity enables abuses that threaten, and occasionally effectuate, disastrous disruptions on personal, national, and global scales. Paper can be used to libel someone's good name, set a forest fire, or start a war. The more generative a technology is, the more dangerous it can be. By definition, the abuses of generativity cannot be separated from the benefits; the freedom to experiment required to produce good

---

failure."); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1980 (2006) ("Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences."); *see also* James Grimmelmann & Paul Ohm, *Dr. Generative or: How I Learned to Stop Worrying and Love the iPhone*, 69 MD. L. REV. 910, 924 (2010) (book review) ("[Zittrain's] work on generativity is a milestone in Internet law scholarship. It's the best descriptive and normative theory to date on what makes the Internet special."); David G. Post, *The Theory of Generativity*, 78 FORDHAM L. REV. 2755, 2756 (2010) [hereinafter Post, *The Theory of Generativity*].

8. *See* ZITTRAIN, *supra* note 1, at 71–73 (describing "five principal factors" that "make[] something generative," including leverage, adaptability, ease of mastery, accessibility, and transferability); Zittrain, *supra* note 7, at 1981–82 ("[G]enerativity increases with the ability of users to generate new, valuable uses that are easy to distribute and are in turn sources of further innovation.").

9. Zittrain, *The Generative Internet*, *supra* note 7, at 1981.

10. ZITTRAIN, *supra* note 1, at 75–76 (listing many examples of generative tools and their less generative counterparts).

11. *See* Zittrain, *The Generative Internet*, *supra* note 7, at 1982–94 ("It is difficult to identify . . . a technology bundle more generative than the PC and the Internet to which it attaches.").

outcomes necessarily allows bad ones too.[12] The unusually broad range of uses enabled by the Internet means that the Internet also poses an unusually broad range of potential abuses.[13]

Zittrain warns that generativity is not an immutable feature of the Internet, and that we could too easily surrender the best aspects of the Internet in response to our worst fears.[14] He acknowledges the need for compromise, but worries that the antidote will be too strong.[15] To avoid a future in which the Internet is locked down, Zittrain advances a "generativity principle," which asks that "any modifications to the Internet's design . . . be made where they will do the least harm to generative possibilities."[16]

Zittrain's conclusion is sound, but he glosses over a crucial step: how to determine least harm. After all, if generativity is the very engine that enables the abuses to be remedied, then leaving that generativity intact will continue to permit those same abuses. One response in the literature has been that we need some way to measure generativity, to distinguish between those incarnations that are more valuable and those that are expendable.[17] The point is valid, but measuring the erosion of generative potential will not prevent it. As long as generativity is our only bargaining chip, each new harm will call for a one-way ratcheting of incremental restrictions on generativity. What

12. *See* ZITTRAIN, *supra* note 1, at 96–97 ("[T]he Internet's very generativity . . . sows the seeds for a 'digital Pearl Harbor.'"); Grimmelmann & Ohm, *supra* note 7, at 917 ("The problem is that not all innovation is to the good; swamps are fecund places too."); *see also* ACLU v. Reno, 31 F. Supp. 2d 473, 476 (E.D. Pa. 1999) ("But with freedom come consequences. Many of the same characteristics which make cyberspace ideal for First Amendment expression . . . make it a potentially harmful media for children.").

13. *See infra* Part III.B.

14. *See generally* ZITTRAIN, *supra* note 1, at 149–99 ("[T]he Internet's generative characteristics primed it for extraordinary success—and now position it for failure. The response to the failure will most likely be sterile tethered appliances and Web services that are contingently generative, if generative at all.").

15. *See id.* at 150 ("We need a strategy that blunts the worst aspects of today's popular generative Internet and PC without killing these platforms' openness to innovation.").

16. *Id.* at 165.

17. *See* Grimmelmann & Ohm, *supra* note 7, at 932, 934 ("When we predict the likely consequences of a given intervention, we need to be able to say whether it will nourish generativity or suffocate it. We need, in other words, a good way to measure generativity. . . . Zittrain also isn't clear on when and how to sacrifice some generativity for the greater good.").

we need instead is another point of leverage that can relieve the regulatory pressure on generativity.[18]

This Article will argue that anonymity is that alternate lever. While generativity creates the capacity for abuse, anonymity allows it to be committed with impunity. A choice to allow both generativity and anonymity is an implicit decision not to regulate at all.[19] Yet, if we accept that some regulation is necessary, then preserving generativity requires a reduction in anonymity and, conversely, preserving anonymity requires a reduction in generativity. Thus, the fate of the generative Internet is inversely linked to how vigorously we choose to defend the anonymous Internet. Those who think generativity is the most important attribute of the Internet should be prepared to cede some anonymity. As long as anonymity remains inviolate, generativity will be the loser. That choice should be seen not as sacrificing liberty for security, but as prioritizing one liberty over another.

Part II of this Article will explore the relationship between anonymity and generativity by reframing a familiar set of cyberlaw problems and the regulatory approaches taken therein. Under that clarifying lens, it will become apparent that the regulatory responses have revolved around a central, implicit choice to restrict either anonymity or generativity. Exposing that dichotomy will be useful in formulating a more principled approach for modeling future Internet regulations.

Part III will step back to compare the theoretical underpinnings of anonymity and generativity, and to expand on the proposition that one might be exchanged for the other for purposes of regulation. It is easy to see the harmonies between anonymity and generativity. Both are liberty values that confer freedom of choice over when and how to use our identities or our technologies, thereby maximizing our capacity to produce change through decentralized action. Anonymity and generativity represent bottom-up mechanisms for disrupting the prevailing status quo by permitting new or alternative ideas to perco-

18. *Cf. id.* at 937–39 (pointing out that "[g]enerativity is an important value in Internet law, but only one of many").

19. There are, of course, those who would celebrate an unregulated Internet. *See, e.g.*, *LulzSec—100th Tweet, Statement* (June 17, 2011), http://pastebin.com/HZtH523f ("This is the lulz lizard era, where we do things just because we find it entertaining. . . . People who can make things work better within this rectangle have power over others . . . . This is the Internet, where we screw each other over for a jolt of satisfaction."); *see also* H. Brian Holland, *In Defense of Online Intermediary Liability: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 377–78 (2008) (summarizing the cyberlibertarianism movement).

late up from any arbitrary source, be received on a level plane, and win acceptance on their merits. Thus, the conventional wisdom is that anonymity and generativity go hand in hand, and that restricting one value also harms the other. What is often overlooked are the tensions between the two values and how we ought to prioritize if forced to pick.

One reason to favor generativity is that it carries a higher opportunity cost—at least when it comes to the Internet. The Internet offers an exceedingly rare breed of generativity, and we have not yet seen all that it can do. Even the ability to communicate anonymously online is an outgrowth of the Internet's vitality, not the primary source. Unless we were convinced that anonymous speech is the "killer app,"[20] locking ourselves into a static Internet would be the larger loss.

A second reason is that acting against generativity creates broader concerns of prior restraint. On one hand, restrictions on anonymity can impose a chilling effect, but each individual retains leeway to make that calculation of risk, even if it is an unpleasant one. Removing generative capacity, on the other hand, quashes the very ability to challenge a rule, often without any real opportunity to invoke the legal process.

A third argument, to be developed in future work, is that anonymity is a value traditionally held in weak esteem. Contrary to what many liberal scholars have suggested, the jurisprudence of offline anonymity points to a rejection of any fundamental "right" to anonymity, limited or otherwise. The relatively disfavored status of offline anonymity diminishes the view of online anonymity as sacrosanct, and lends further weight to the idea that the anonymous Internet should be reined in to safeguard the generative Internet.

Finally, Part IV will conclude by examining the channels and challenges of building attribution into the Internet. In the end, some generative compromise may be inevitable. But if we are committed to maximizing generativity, then we must at least re-examine our commitment to online anonymity. A certain degree of anonymity may be inviolate. Yet, if generativity represents the core value of the Internet, then sacrificing anonymity may be the lesser evil.

---

20 "The phrase 'killer app' is short for 'killer application' and refers to the form of content that makes a new technology desirable to a critical mass of consumers." Chad Woodford, Comment, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Manage*ment, 75 U. COLO. L. REV. 253, 271 (2004).

II. FREE AS IN GENERATIVITY, NOT AS IN ANONYMITY

Revisiting a few familiar cyberlaw problems will help set the stage and illustrate the basic tension between anonymity and generativity. The four examples selected here are copyright infringement, adult content, spam, and defamation, but others could easily be substituted. While each conflict has its own idiosyncrasies, the commonality is that every effort at resolution has turned on limiting either anonymity or generativity.

One noteworthy theme has been the consistent reluctance of courts to allow expansive encroachments on online anonymity.[21] Restrictions of online anonymity are characterized as a nuclear option with far-reaching repercussions, while restrictions of online generativity are often seen as a localized solution with contained impact. Perhaps the scales have been tipped by the fact that "anonymity" is a familiar concept that judges understand how to grapple with, whereas "generativity" has not yet achieved such salience and is still regarded as largely the province of technology rather than law. The threat to generativity can be difficult to apprehend if generativity is viewed as a diffuse, intangible quality that is accessible to all inventors and tinkerers at large, but unclaimable by any one in particular until after it has ripened into a concrete, derivative technology.[22]

Exposing on a systemic level the implicit choices being made between anonymity and generativity will sharpen the policy discussion going forward. As a general rule, we do not insist on perfect generativity, because it would take too much surveillance and police power to offset the potential destructiveness.[23] For the same reason, we should be wary of eroding too much generativity for the sake of perfect anonymity.

A. File Sharing and Copyright Infringement

The music industry's fight to enforce its copyrights against digital file sharing offers a useful starting point because the campaign featured a stark shift from efforts targeting generativity to efforts target-

21. *See, e.g.*, *infra* note 41 and accompanying text.

22. The difficulty in representing a claim of anti-generative harm might be comparable to the difficulty in representing a claim of anticommons harm. *Cf.* Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998).

23. *Cf.* Grimmelmann & Ohm, *supra* note 7, at 912 ("[G]enerativity is essential but can never be absolute. . . . Tradeoffs are inevitable.").

ing anonymity. Although the strategy was heavily criticized at the time, the intuition was sound: If generativity and anonymity are regulatory substitutes, then one can choose to assert control over the technologies that enable abuse or over the individuals who commit it. All else equal, if the goal of enforcing the music industry's copyrights is held constant, the question is whether to confront those who create illegitimate copies, or whether to remove the means by which such copies can be created.[24] A choice to do neither is a constructive forfeiture of the entitlement.[25]

Early regulatory efforts focused on quashing the generative flood of peer-to-peer platforms that were rushing to solve the technological challenges of digital file sharing.[26] Representatives of the music industry, including the now-notorious Recording Industry Association of America ("RIAA"), sought to suppress the technology by suing the developers and operators of all the major file-sharing networks. In a series of high-profile lawsuits, the music industry achieved favorable results against entities such as MP3.com, Napster, Aimster, AudioGalaxy, Kazaa, Morpheus, Grokster, iMesh, Limewire, and The Pirate Bay.[27] At the same time, the music industry also pursued technologi-

24. *See* Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1373–78 (2004) ("Copyright owners have understandably cast about for an alternative to suing end users. The strategy they have settled on is to sue facilitators. Suing facilitators is cost-effective for the content industries because a single lawsuit can eliminate the dissemination mechanism for a large number of end-user copies.").

25. Some have argued that there is a third way: reducing the incidence of abuse by cultivating better behavior, through devices such as default settings, community norms, or educational outreach. Voluntary compliance is wonderful when it works, but relying on it as the sole recourse turns a copyright holding into a donation request, not a legal entitlement. For a longer discussion, see *infra* notes 200–212.

26. *See* Lemley & Reese, *supra* note 24, at 1353–72 (describing expansions in application of secondary liability and vicarious infringement theories, as well as reductions in safe harbors, as a "seismic shift in copyright infringement in the digital environment, away from suing direct infringers and towards suing facilitators with less and less connection to the act of copyright infringement").

27. *See id.* at 1349 ("So far, the courts have been largely willing to go along, shutting down a number of innovative services in the digital music realm."); *see generally* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 919–21, 941 (2005); *In re* Aimster Copyright Litig., 334 F.3d 643, 645, 656 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1095 (9th Cir. 2002); Arista Records LLC v. Lime Group LLC, 715 F.

cal measures to cripple file sharing, such as flooding peer-to-peer networks with fake files[28] and creating digital rights management ("DRM") systems that used encryption to prevent unauthorized access.[29]

Those tactics enjoyed some success, but with diminishing returns.[30] The legal attacks strained the limits of copyright protection,[31] as well as those of international jurisdiction.[32] The technological at-

Supp. 2d 481 (S.D.N.Y. 2010); UMG Recordings, Inc. v. MP3.Com, Inc., 92 F. Supp. 2d 349, 353 (S.D.N.Y. 2000).

28. *See* RUBEN CUEVAS ET AL., IS CONTENT PUBLISHING IN BITTORRENT ALTRUISTIC OR PROFIT-DRIVEN 5 (ACM CoNEXT 2010), *available at* http://conferences.sigcomm.org/conext/2010/CoNEXT_papers/11-Cuevas.pdf ("Surprisingly, fake publishers are responsible for around . . . 30% of the published content and 25% of the downloads in [The Pirate Bay data set] . . . [which] suggests that major BitTorrent portals are suffering from a systematic poisoning index attack."); Doug Lichtman & David Jacobson, *Anonymity a Double-Edged Sword for Pirates Online*, CHI. TRIB., Apr. 13, 2000, at N25.

29. *See* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 50 (2006) ("Distributors of copyrighted digital works may deploy 'digital rights management' ('DRM') mechanisms that allow only certain types of access to, or uses of, the underlying copyrighted work and forbid all others."); Alfred C. Yen, *What Federal Gun Control Can Teach Us About the DMCA's Anti-Trafficking Provisions*, 2003 WIS. L. REV. 649, 677–79 (2003) (objecting that "DRM gives copyright holders an unprecedented degree of control over their works," which "could change copyright's balance" by allowing copyright holders to charge for non-infringing uses that should be free).

30. *See, e.g.*, Armstrong, *supra* note 29, at 50–51 ("[T]echnologically sophisticated users may be able to bypass a DRM mechanism and obtain greater access to the work than the DRM mechanism is intended to permit . . . ."); Nick Bilton, *Internet Pirates Will Always Win*, N.Y. TIMES, Aug. 5, 2012, at SR5.

31. *See* Bryan H. Choi, Note, *The* Grokster *Dead-End*, 19 HARV. J.L. & TECH. 393, 399 (2006) (arguing that the Supreme Court's decision in *Grokster* "suggests that we are reaching the limit as to how far secondary liability doctrine can be stretched to cover file-sharing technologies"); *see also* Lemley & Reese, *supra* note 24, at 1349–50, 1379–90 ("The key policy point is that going after makers of technology for the uses to which their technologies may be put threatens to stifle innovation. . . . The fundamental difficulty is that while courts can make decisions about direct infringement on a case-by-case basis, lawsuits based on indirect liability sweep together both socially beneficial and socially harmful uses of a program or service, either permitting both uses or condemning both.").

32. *See* John Tagliabue, *In Sweden, Taking File Sharing to Heart. And to Church.*, N.Y. TIMES, July 26, 2012, at A8 (describing the growth of Europe's Pirate Party, which has spread to "at least nine European countries" over the last decade); Ben Sisario, *An Apology for Kim Dotcom, and a New Royalties Deal for Clear Channel*, N.Y. TIMES MEDIA DECODER (Sept.

tacks were repeatedly thwarted, whether through superior countermeasures or through clever workarounds such as the so-called "analog hole."[33]

In frustration, the music industry switched gears to identifying and suing individual file-sharers—a tack that was widely condemned by the public.[34] Even before the advent of peer-to-peer file-sharing,

---

27, 2012, 2:11 PM), http://mediadecoder.blogs.nytimes.com/2012/09/27/digital-notes-an-apology-for-kim-dotcom-and-a-new-royalties-deal-for-clear-channel/ (observing that the Megaupload case "is being watched intently . . . as a test of whether the United States can pursue copyright infringement cases overseas"). The controversial (and ultimately unsuccessful) Stop Online Piracy Act ("SOPA") and PROTECT IP Act ("PIPA") legislative proposals were promoted and defended as a necessary response to the ineffectiveness of copyright enforcement efforts abroad. *See infra* note 54.

33. *See, e.g.*, Timothy L. O'Brien, *Technology; Norwegian Hacker, 19, Is Acquitted in DVD Piracy Case*, N.Y. TIMES, Jan. 8, 2003, at C4 (reporting on the acquittal of the Norwegian teenager who helped write DeCSS, the software program that disabled the original DRM system for DVDs); Liza Daly, *The Analog Hole: Another Argument Against DRM*, O'REILLY RADAR (Oct. 23, 2008), http://radar.oreilly.com/2008/10/the-analog-hole-in-digital-boo.html (explaining that the analog hole is "the one weakness found in all DRM'ed media," since it can be exploited just by playing the digital media and recording the analog output); Daniel Roth, *The Pirates Can't Be Stopped*, UPSTART BUS. J. (Jan. 14, 2008, 6:00 AM), http://upstart.bizjournals.com/news-markets/national-news/portfolio/2008/01/14/Media-Defenders-Profile.html?page=all (describing the exploits of a high school hacker who broke into the servers of MediaDefender, an antipiracy company employed by the entertainment industry, and exposed and discredited its methods). Those failures eventually led the music industry to abandon DRM schemes. *See* Brad Stone, *Copy an iTunes Song? Go Ahead, Apple Says*, N.Y. TIMES, Jan. 6, 2009, at B1 (reporting on the decision by all four major music labels to begin selling digital music without DRM); Brad Stone & Jeff Leeds, *Amazon to Sell Music Without Copy Protection*, N.Y. TIMES, May 17, 2007, at C1 (reporting on the much earlier decision to shed DRM by EMI, the only major music label to do so at the time).

34. *See* David W. Opderbeck, *Peer-to-Peer Networks, Technological Evolution, and Intellectual Property Reverse Private Attorney General Litigation*, 20 BERKELEY TECH. L.J. 1685, 1701–02 (2005) ("Because the RIAA was unable to control the technology [of peer-to-peer file-sharing], it instead focused on influencing end-user behavior. To this end, in September 2003 the RIAA began suing individual end users . . . ."); Amy Harmon, *The Price of Music: The Overview; 261 Lawsuits Filed on Music Sharing*, N.Y. TIMES, Sept. 9, 2003, at A1 (relaying numerous concerns and criticisms expressed in reaction to the first set of lawsuits); John Schwartz, *More Lawsuits Filed in Effort to Thwart File Sharing*, N.Y. TIMES, Mar. 24, 2004, at C4 (reporting on more lawsuits filed in the RIAA's "crusade against file sharing," which con-

the content industries had persuaded Congress to include in the Digital Millennium Copyright Act ("DMCA")[35] a provision to expedite the identification of suspected copyright infringers. Just by filing a subpoena request with the clerk of any federal district court, copyright holders could easily compel an Internet service provider to furnish the identity of any alleged infringer.[36] After successfully persuading a few district courts to accept the use of the DMCA procedural shortcut,[37] the RIAA issued more than 1,500 subpoenas, filed lawsuits against several hundred individuals, and reached settlements with many others.[38]

---

tinued to receive censure as a strategy that was "wreak[ing] havoc on ordinary people" and that would "really backfire").

35. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C. §§ 512, 1201-05, 1301-32, 28 U.S.C. § 4001 (2006)).

36. 17 U.S.C. § 512(h)(1)–(4) (2006); Kristina Groennings, Note, *Costs and Benefits of the Recording Industry's Litigation Against Individuals*, 20 BERKELEY TECH. L.J. 571, 574 (2005) ("[Section] 512(h) provided a fast, cheap mechanism for discovering suspected file-sharers' identities. The RIAA needed only to supply $35, a copy of notification, the proposed subpoena, and a sworn declaration that the information sought was for the sole purpose of protecting copyright.").

37. *See, e.g.*, RIAA v. Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 246–47 (D.D.C. 2003) (denying Verizon's motion to quash the RIAA's DMCA subpoena), *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003); RIAA v. Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 26 (D.D.C. 2003) (granting the RIAA's motion to enforce its DMCA subpoena), *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003); *see also* RIAA v. Charter Commc'ns, Inc., 393 F.3d 771, 772–74 (8th Cir. 2005) (vacating the lower court's issuance of DMCA subpoenas to the RIAA); Pac. Bell Internet Servs. v. RIAA, No. C03-3560, 2003 WL 22862662, at *1 (N.D. Cal. Nov. 26, 2003) (dismissing an Internet service provider's request for declaratory judgment to invalidate the DMCA subpoena provision).

38. *See* ELEC. FRONTIER FOUND., RIAA V. THE PEOPLE: FIVE YEARS LATER 3 (2008), *available at* https://www.eff.org/files/eff-riaa-whitepaper.pdf ("Verizon and the privacy advocates lost the first rounds in court. That gave the RIAA the green light to start delivering thousands of subpoenas . . . . Between August and September 2003, the RIAA issued more than 1,500 subpoenas to ISPs around the country. On September 8, 2003, the RIAA announced the first 261 lawsuits against individuals that it had identified using the DMCA subpoenas."). The RIAA changed its strategy in response to criticism and "began sending threat letters [before suing an individual directly], giving the accused an opportunity to settle the matter before a lawsuit was filed." *Id.*; *see also* Opderbeck, *supra* note 34, at 1705–07 (stating that most defendants choose to settle rather than incur the costs of litigation and that "many trial courts endorse [that] strategy by issuing broad discovery orders and approving form settlements").

The music industry's aggressive use of DMCA subpoenas was overturned on appeal in *RIAA v. Verizon Internet Services, Inc.*[39] Based on a technical reading of the statute, the appellate court exempted all ordinary Internet service providers ("ISPs") from the subpoena provision, ruling that only certain providers (those that actively stored infringing materials on their servers) could be served proper notice within the meaning of the statute.[40] While the *Verizon* decision did not preclude the possibility of acquiring user identities through other means,[41] it was emblematic of a general reluctance among the courts to commit drastic changes to the established contours of online anonymity.

Undeterred, the RIAA pursued other ways to identify infringing users. One route involved petitioning the courts by filing "John Doe" lawsuits. Unlike the DMCA subpoenas, which could be obtained without formal proceedings, the "John Doe" subpoenas required a pending cause of action.[42] To save on legal fees, however, the RIAA filed the claims en masse.[43] Coming on the heels of the furor over the DMCA subpoenas, the strategy smelled like a bad-faith workaround, and so the courts again balked at giving away identities so freely.[44]

---

39. 351 F.3d 1229, 1231 (D.C. Cir. 2003); *see also supra* note 37.

40. *Verizon*, 351 F.3d at 1231, 1233; *accord Charter Commc'ns*, 393 F.3d at 771, 776–77.

41. *Cf. Verizon*, 351 F.3d at 1231 (declining to rule on Verizon's claim that the DMCA subpoena provision "violates the First Amendment because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously").

42. The "John Doe" lawsuits proceeded in the following manner:

> [T]he record label lawyers sued unidentified "John Doe" uploaders that their investigators had traced to an IP address. After filing the lawsuit, the record labels would ask the court to authorize subpoenas against the ISPs. After delivering these subpoenas and obtaining the real name of the subscriber behind the IP address, the record label lawyers would then either deliver a letter demanding a settlement or amend their lawsuit to name the identified individual.

ELEC. FRONTIER FOUND., *supra* note 38, at 4.

43. *See* Opderbeck, *supra* note 34, at 1703–04 (comparing the RIAA end-user litigation to mass tort litigation in three respects: "Groups of ostensibly related cases are centralized in one court; the suits are not filed as discrete actions relating to each set of transactions; and discovery is managed, at least initially, on a collective basis").

44. *See id.* at 1707–08 (stating that "not all trial courts have been so sanguine about the RIAA's tactics" and describing how some courts have raised administrative concerns over "the RIAA plaintiffs [attempting to] avoid paying individual filing fees by aggregating claims against Doe defendants").

Some courts refused to allow the mass joinders on the basis of unfairness to individual defendants.[45] Other courts focused on the unfairness to ISPs, and offered protective measures such as limiting the number of identification requests and requiring full reimbursement for any costs incurred in fulfilling the requests.[46] Those rulings contributed to making the mass litigation strategy prohibitively expensive,[47] and the RIAA subsequently announced that it was suspending its campaign.[48]

45. *See, e.g.*, BMG Music v. Does 1-203, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004) (ruling that joinder was improper because "[p]laintiffs are attempting to bring over [200] factually distinct actions in one lawsuit[, but e]ach claim involves different property, facts, and defenses"); *see also* Opderbeck, *supra* note 34, at 1708 & n.104 (noting decisions in Florida, Georgia, and Pennsylvania rejecting joinder of claims against hundreds of individual defendants because there was no joint action or connective nexus among the defendants). *But see* Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332, 344 (D.D.C. 2011) (holding that unnamed parties cannot demonstrate any harm because they "are not required to respond to the plaintiffs' allegations or assert a defense," and adding that "joinder in a single case of the putative defendants who allegedly infringed the same copyrighted material . . . is beneficial to the putative defendants").

46. DigiProtect USA Corp. v. Does 1-240, No. 10 Civ. 8760(PAC), 2011 WL 4444666, at *4 (S.D.N.Y. Sept. 26, 2011) (noting that "[DigiProtect] should recognize that its approach imposes a substantial burden on parties [like the ISPs] with no formal interest in the outcome of the litigation" and "requir[ing] DigiProtect to reimburse the ISPs for the cots [sic] incurred in each IP address look-up, including notifying the relevant subscribers"). *But see Call of the Wild Movie*, 770 F. Supp. 2d at 355–59 (denying motions by ISP Time Warner to quash mass subpoenas, because its claims of undue burden were contradicted by the evidence, and all costs would be covered by the plaintiffs).

47. *See* Lemley & Reese, *supra* note 24, at 1376–77 (calculating the costs of end-user litigation, and observing that "suing even a fraction of the end users could bankrupt the content industries"); Mike Masnick, *RIAA Spent $17.6 Million in Lawsuits . . . to Get $391,000 in Settlements?*, TECHDIRT (July 14, 2010, 9:44 AM), http://www.techdirt.com/articles/20100713/17400810200.shtml (characterizing the RIAA lawsuits as "an economic disaster" and noting that the record industry "admitted [they] were 'a money pit'").

48. Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1. Reports indicate that more than 30,000 suits were filed, including both named and John Doe suits, and over 18,000 people were contacted—of whom 11,000 settled immediately or were not prosecuted, and 7,000 were sued in federal court. Nate Anderson, *Has the RIAA Sued 18,000 People . . . or 35,000?*, ARSTECHNICA (July 8, 2009, 2:50 PM), http://arstechnica.com/tech-policy/2009/07/has-the-riaa-sued-18000-people-or-35000/.

Instead, the music industry has now turned to the option of partnering directly with ISPs and other third parties to access user information, which avoids the friction, expense, and uncertainty of litigation. In the United States, the major ISPs have agreed to participate in a "six-strikes" plan, which would allow the RIAA to send copyright infringers several warnings before initiating an escalating series of punitive measures.[49] In Great Britain, a similar arrangement was announced in 2009—though it was later abandoned—in which an ISP had offered to assist with policing copyright infringement on its network in exchange for access to unrestricted music downloads for its customers.[50] Other developments, such as the rising popularity of subscription-based streaming services,[51] may create additional opportunities to forge private partnerships that give content owners direct control over subscriber identities.

Of course, it should be noted that the pursuit of identity-based solutions does not mean that the content industries have abandoned other efforts. Generativity is still at stake in ongoing lawsuits against intermediaries such as YouTube and MegaUpload,[52] the ongoing development of new DRM systems,[53] and efforts to alter the Internet's

49. *See* Ross Drath, *Hotfile, Megaupload, and the Future of Copyright on the Internet: What Can Cyberlockers Tell Us About DMCA Reform?*, 12 J. MARSHALL REV. INTELL. PROP. L. 204, 233–34 & n.215 (2012) (describing the terms of the arrangement); David Kravets, *Copyright Scofflaws Beware: ISPs to Begin Monitoring Illicit File Sharing*, WIRED (Oct. 8, 2012, 4:10 PM), http://www.wired.com/threatlevel/2012/10/isp-file-sharing-monitoring/ (reporting the additional measures as including "temporary reductions of internet speeds, redirection to a[n educational] landing page . . . , or other measures (as specified in published policies) that the ISP may deem necessary to help resolve the matter").

50. Eric Pfanner, *Universal Music and Virgin Reach a Download Deal*, N.Y. TIMES, June 16, 2009, at B2. That deal was eclipsed by a subsequent agreement between Virgin Media and Spotify, a Swedish music-streaming service. David Meyer, *Virgin Media: Spotify Deal Will Bring Down Piracy*, ZDNET (July 6, 2011, 2:57 PM), http://www.zdnet.com/virgin-media-spotify-deal-will-bring-down-piracy-3040093328/.

51. Brad Stone, *The Music Streams That Soothe an Industry*, N.Y. TIMES, July 26, 2009, at BU3.

52. *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (reversing dismissal of copyright claims against YouTube for hosting infringing videos); Ben Sisario, *U.S. Charges Popular Site with Piracy*, N.Y. TIMES, Jan. 20, 2012, at B1 (reporting the case against MegaUpload, which operated a network of "cyberlocker" services).

53. *See* Michelle Kung, *Movies in the Clouds*, WALL ST. J., Oct. 11, 2011 (describing the movie industry's UltraViolet initiative); Brad Stone, *Amazon Faces a Fight Over Its E-Books*, N.Y. TIMES, July 27, 2009, at B3 (discussing Amazon's use of DRM for the Kindle).

domain name system to enable the unilateral takedown of any offending website.[54]

As a policy matter, the question of whether the copyright system needs substantive reform has become highly contentious in recent years,[55] but this Article is not an attempt to revisit that debate. Rather, the point here is simply that, if we assume the copyright system *will* be enforced, then the path of regulation will travel through either anonymity or generativity. Protecting both is a two-front war that cannot be won.

B. Adult Content and the Child Online Protection Act

The fight to make the Internet safer for children has also centered on the choice between anonymity and generativity, and again shows how excluding one regulatory lever implicitly forces regulators to lean more heavily on the other one. From the outset, Congress was focused on restricting anonymity. Both the Communications Decency Act ("CDA")[56] and the Child Online Protection Act ("COPA")[57] were attempts to require distributors of online pornography to identify users by age. The United States Supreme Court, on the other hand, was skeptical of applying an identity-based approach to the Internet, and rebuffed those efforts in favor of alternative solutions such as content filters.

The CDA, enacted in 1996, sought to reinstate the offline norm of requiring proof of proper age in order to obtain sexually explicit

---

54. *See* Stop Online Piracy Act ("SOPA"), H.R. 3261, 112th Cong. (2011); PROTECT IP Act ("PIPA"), S. 968, 112th Cong. (2011); *see also* Mark Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011); Jenna Wortham, *Protest on Web Takes on 2 Bills Aimed at Piracy*, N.Y. TIMES, Jan. 18, 2012, at A1; Rebecca MacKinnon, Op-Ed, *Stop the Great Firewall of America*, N.Y. TIMES, Nov. 16, 2011, *available at* http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html (arguing that SOPA and PIPA "would empower the attorney general to create a blacklist of sites to be blocked by Internet service providers, search engines, payment providers and advertising networks, all without a court hearing or a trial"); *see also supra* note 32.

55. *See, e.g.*, LAWRENCE LESSIG, FREE CULTURE: THE NATURE AND FUTURE OF CREATIVITY (2004).

56. Pub. L. No. 104-104, tit. V, 110 Stat. 133–43 (1996), *invalidated by* Reno v. ACLU, 521 U.S. 844 (1997).

57. Pub. L. No. 105-277, tit. XIV, 112 Stat. 2681-736 to 2681-741 (1998), *invalidated by* ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008).

materials. To be sure, the statute imposed criminal penalties on anyone who used an interactive computer service to transmit "obscene," "indecent," or "patently offensive" materials to persons under eighteen years of age.[58] But the true thrust of the CDA lay in its affirmative defenses, which provided immunity to those who validated age "by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number," or by taking other "good faith, reasonable, effective, and appropriate actions" to restrict access by minors.[59] In effect, Congress's intention was to compel the use of identification measures, not to prohibit the transmission of adult content over the Internet.

In *Reno v. ACLU*,[60] the Supreme Court invalidated the CDA for two reasons. First, the statute was poorly drafted—the terms "indecent" and "patently offensive" had been left undefined, and potentially swept in "large amounts of nonpornographic material with serious educational or other value."[61] Because the coverage was overbroad, and the sanctions so severe, the Court feared that the statute would unintentionally silence constitutionally protected speech.[62]

---

58. *See Reno*, 521 U.S. at 858–60 (describing the "indecent transmission" provision and the "patently offensive display" provision of the statute).

59. *Id.* at 860–61 & n.26. *But see* Ashcroft v. ACLU (*COPA II*), 542 U.S. 656, 674 (2004) (Stevens, J., concurring) (expressing concern that affirmative defenses "cannot guarantee freedom from prosecution," and that "[s]peakers who dutifully place their content behind age screens may nevertheless find themselves in court, forced to prove the lawfulness of their speech on pain of criminal conviction"). COPA took the same approach as the CDA, using similar language to provide an affirmative defense for

> the defendant [who], in good faith, has restricted access by minors to material that is harmful to minors—(A) by requiring the use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology.

47 U.S.C. § 231(c)(1). *But see* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 418 (1999) (describing the ways in which the affirmative defenses in COPA were broader than those contained in the CDA).

60. 521 U.S. 844 (1997).

61. *Id.* at 871 & n.35, 877.

62. *Id.* at 871–72, 874 ("The vagueness of the CDA is a matter of special concern . . . because of its obvious chilling effect on free speech" and because "[t]he severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. . . . Given the vague contours of the coverage of

More importantly, though, the Court concluded that there was no good way to authenticate the ages of Internet users.[63] Had such an option been technologically and economically feasible at the time, perhaps the affirmative defenses would have negated the risk of criminal sanction and saved the CDA. Instead, the Court found the affirmative defenses to be illusory because age verification methods were still "unproven future technology."[64]

In response, Congress immediately redrafted the legislation to address the Court's concerns, and enacted it as COPA.[65] In *Ashcroft v. ACLU*,[66] the Court acknowledged that, as a result of those efforts, COPA successfully fixed the problems of statutory scope that had plagued the CDA.[67] But by that time the culture of anonymity had

---

the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection.").

63. *Id.* at 855–57, 876–77 ("The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. . . . As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial—as well as some commercial—speakers who have Web sites to verify that their users are adults.").

64. *Id.* at 881–82; *see also* Lessig & Resnick, *supra* note 59, at 418 (commenting that the Supreme Court read the affirmative defenses in the CDA "not as an ordinary tort standard [of reasonableness], but as an absolute effectiveness requirement").

65. Ashcroft v. ACLU (*COPA II*), 542 U.S. 656, 661 (2004) ("COPA is the second attempt by Congress to make the Internet safe for minors by criminalizing certain Internet speech. The first attempt was the [CDA]."); *see also supra* note 59.

66. Ashcroft v. ACLU (*COPA I*), 535 U.S. 564 (2002).

67. *See id.* at 578–79 ("COPA . . . does not appear to suffer from the same flaw [of overbreadth and vagueness] because it applies to significantly less material than did the CDA and defines the harmful-to-minors material restricted by the statute in a manner parallel to the *Miller* definition of obscenity."); *see also COPA II*, 542 U.S. at 660, 665 (noting that "[i]n enacting COPA, Congress gave consideration to our earlier decisions on this subject, in particular the decision in *Reno*," and declining to review the lower court's finding of unconstitutionality based on statutory construction); *id.* at 690 (Breyer, J., dissenting) (observing that "Congress . . . dedicated itself to the task of drafting a statute that would meet each and every criticism of the predecessor statute that this Court set forth in *Reno*"). Specifically, Congress imported language directly from the obscenity standard articulated in *Miller v. California*, 413 U.S. 15 (1973); narrowed COPA to cover only commercial material; relaxed the criminal sanctions by reducing the maximum term of imprisonment from two years to six months; and lowered the age threshold to seventeen years. *See COPA I*, 535 U.S. at 569–71; S. REP. NO. 105-225 (1998).

become so embedded in the Internet that the Court was loath to uproot it. The Court invalidated COPA on the grounds that there were other alternatives, such as filtering software, that were less restrictive than COPA's age verification scheme.[68]

To the Court, filtering software was preferable precisely because it did not require adults to reveal identifying information in order to gain access to explicit materials.[69] The Court claimed that filtering software was less restrictive because it was a "selective" restriction, visited only upon those children whose parents opted in and chose to install the software.[70] Anyone not using the filtering software would remain unaffected.[71] By contrast, COPA was a "universal" restriction applied at the source; all adults would be burdened by having to disclose identifying information that otherwise could remain secret.[72]

The Court's decision invalidating COPA embodies the generative tradeoff: By rejecting approaches that rely on identification, the Court forced regulators to turn to approaches that lock down functionality. An age-check mechanism minimizes the need for technological intervention because it enlists the cooperation of the appropriate parties on both sides, that is, adult viewers and content providers. By contrast, a filtering wall places its reliance solely on technological controls, not just to block inappropriate content but—more troublingly—to block users from circumventing the controls (and the controls on those controls).

The selective/universal distinction emphasized by the Court was the wrong dichotomy. The affirmative defenses in COPA did not specify that age verification needed to be performed locally or re-

68. *COPA II*, 542 U.S. at 666–70 (majority opinion).

69. *Id.* at 667 (finding filters to be less restrictive than COPA in part because, "[u]nder a filtering regime, adults without children may gain access to speech they have a right to see without having to identify themselves or provide their credit card information").

70. *Id.* ("Filters . . . impose selective restrictions on speech at the receiving end, not universal restrictions at the source.").

71. *Id.* ("Under a filtering regime, . . . [e]ven adults with children may obtain access to the same speech on the same terms simply by turning off the filter on their home computers.").

72. *See supra* note 70. As an aside, the Court's statement assumed that the adults' identifying information *should* remain secret. *But see COPA II*, 542 U.S. at 683 (Breyer J., dissenting) (acknowledging that identification requirements may lead users to fear embarrassment, but noting that the Constitution does not protect against such embarrassment in other contexts such as libraries and nightclubs).

motely.[73] In other words, age-validating software can be installed on home computers in the same "selective" manner as content-filtering software.[74] Conversely, content filters can be installed remotely to have a "universal" effect on all Internet users.[75]

More importantly, the Court's discussion obscured the fact that if we are genuinely committed to the goal of restricting "children" from accessing "inappropriate materials," then age verification and content filtering are equally unavoidable components, respectively.[76] The real issues at stake are: (1) who should be required to disclose their identities—adults or children; and (2) who should be responsible for labeling and restricting access to adult materials—content providers or third-party screeners. In effect, COPA chose "adults" and "content providers," while the Court favored "children" and "third-party screeners." The Court's judgment was sensible when considering anonymity interests alone, but it was not duly mindful of the generative trade-off.

A child-ID scheme—i.e., any setup that affects only a child's Internet usage—avoids disturbing the anonymity interest of adults, because it allows adults to continue to view adult content without having to reveal their age or any other identifying information.[77] Likewise, a third-party filtering scheme protects the "anonymity" of adult-content

73. *See* Lessig & Resnick, *supra* note 59, at 419 ("If . . . asking whether COPA mandated the least burdensome adult-ID regime possible, then we believe this statute does impose the smallest adult-ID regime burden possible . . . [because] COPA includes a catchall provision that permits 'any other reasonable measures that are feasible under available technology.'").

74. For example, a "kids-mode browser" could identify its user as a minor and request websites to block harmful content accordingly, without affecting the browsing activities of adults. *See id.* at 416–22 (describing a hypothetical kids-mode browsers as an alternative to the CDA and COPA); *see also* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 516–19 (1999) (same).

75. *See* Robert A. Gomez, *Protecting Minors from Online Pornography Without Violating the First Amendment*, 11 SMU SCI. & TECH. L. REV. 1, 17 (2007) (describing the available filter options as including not only client-side filtering software, but also filters installed by intermediaries such as ISPs, search engines, and local server operators).

76. *But see COPA II*, 542 U.S. at 690 (Breyer, J., dissenting) ("I recognize that some Members of the Court, now or in the past, have taken the view that the First Amendment simply does not permit Congress to legislate in this area.").

77. *Id.* at 667 (majority opinion).

providers in the sense that they are not obligated to label themselves as being harmful to children.[78]

The generative difference lies in how that system fails. First, independent entities that process and screen large quantities of content can be expected to make more classification errors than content providers that are individually responsible for selecting and serving the content themselves.[79] In part, those classification errors are caused by mistake and uncertainty; yet there is also a natural incentive to err on the side of overblocking rather than underblocking, since content filters are created and marketed to block content rather than to allow content. That danger is compounded when features that should be available, and content that should be viewable, are seamlessly concealed, making it difficult to even recognize when a mistake has occurred.

Second, it is far more likely that a child-ID scheme would fail to flag a child than that an adult-ID scheme would allow a child to masquerade as an adult using false credentials.[80] Blocking a child's access

78. *Id.* ("[P]romoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished."); *cf.* Robert D. Richards & Clay Calvert, *Adult Websites and the Top-Level Domain Debate: ICANN's Adoption of .XXX Draws Adult-Industry Ire*, 29 CARDOZO ARTS & ENT. L.J. 527, 529 (2011) (describing objections from the adult entertainment industry against the creation of a new .XXX domain name label, including that it would "provide a very convenient tool for those who have the power to either censor or prevent lawful speech to be disseminated"). *But see* Robert D. Richards & Clay Calvert, *Untangling Child Pornography from the Adult Entertainment Industry: An Inside Look at the Industry's Efforts to Protect Minors*, 44 CAL. W. L. REV. 511, 520, 536–40 (2008) (describing a self-regulatory initiative by the adult entertainment industry to create a "Restricted to Adults" ("RTA") website label, and noting further that adult sites are already labeled "Sexually Explicit" or "Adult" because they want to be found").

79. *See COPA II*, 542 U.S. at 685–86 (Breyer, J., dissenting) (observing that filtering software suffers from serious problems of underblocking and overblocking); *cf. id.* at 671 (majority opinion) ("[T]here is a serious gap in the evidence as to the effectiveness of filtering software."); United States v. Am. Library Ass'n, Inc., 539 U.S. 194, 221–22 (2003) (Stevens, J., dissenting) (describing "fundamental defects in the filtering software that is now available or that will be available in the foreseeable future").

80. In *COPA II*, the Court noted that age verification systems could be "subject to evasion and circumvention, for example, by minors who have their own credit cards." *Id.* at 668 (majority opinion). Of course, if that were the Court's real concern, then the Court should have been even more critical of opt-in filtering schemes, which allow children to pass as adults by default. *Cf.* Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 128–31

across all Internet devices is a Herculean task compared with blocking a child's access to adult credentials. Thus, although the Court praised the "selective" nature of end-user filtering software—that is, voluntary identification of children by their parents—the dissent's rejoinder was that many parents had neither the money nor the attention to impose that limitation on their children.[81] If a substantial amount of that "selective" inaction is in fact involuntary, the collective backlash will push filtering systems to be embedded at more "universal" locations such as ISPs, search engines, and public computers.[82] In other words, the Court's rejection of adult identification, combined with the general ineffectiveness of child identification, will lead not to an abandonment of purpose, but rather to a redoubling of efforts against the tools of enablement.

When we abandon identification as a regulatory tool, we encourage regulators to encroach on generative qualities. Since the demise of COPA, advocates have made progress in promoting proposals such as the mandatory zoning of explicit content, which would divide the Internet at an architectural layer into a "green" zone and a "red" zone.[83] Such a proposal could successfully screen content for minors

(1989) (discussing the likelihood that "enterprising youngsters could and would evade the rules and gain access to communications from which they should be shielded"); Janine Hiller et al., *POCKET Protection*, 45 AM. BUS. L.J. 417, 441–44 (2008) (describing the ineffectiveness of the parental consent model in the Children's Online Privacy Protection Act, which also constitutes a child-ID scheme).

81. *See COPA II*, 542 U.S. at 685 (Breyer, J., dissenting) (asserting that many parents do not have the money or the attention to impose filtering software on their children). *But see id.* at 669–70 (majority opinion) ("COPA presumes that parents lack the ability, not the will, to monitor what their children see."); United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 824 (2000) ("[A] court should not presume parents, given full information, will fail to act.").

82. *See, e.g.*, United States v. Am. Library Ass'n, Inc., 539 U.S. 194 (2003) (upholding the Children's Internet Protection Act, which requires federally funded libraries to install filtering software on all publicly accessible computers).

83. *See* COMM'N ON CHILD ONLINE PROTECTION, REPORT TO CONGRESS 31 (2000), *available at* http://www.copacommission.org/report/COPAreport.pdf (discussing a proposal for the "[e]stablishment of a 'green zone' or 'red light zone' by means of allocation of a new set of IP numbers" and concluding that "[t]echnical difficulties involved in implementing this technology make effectiveness uncertain"). The first step to pushing such content into a separate top-level domain was passed in early 2011. *See* Jacqui Cheng, *ICANN Approves .XXX Red-Light District for the Internet*, WIRED.COM (Mar. 19, 2011, 2:06 PM), http://www.wired.com/epicenter/2011/03/icann-approves-xxx. Other methods of seg-

without forcing adults to reveal any identifying information, but the cost to generativity would be high.[84] Requiring adult content to remain technologically segregated at all times would make it difficult to create or do anything online that might blur or cross the boundary lines.[85] Services that host user-generated content would become infeasible; search engines and data storage services would be hobbled; advertisements and other embedded content would have to be reworked; commenting systems would have to be curtailed. All that extra cost might permit adults to consume pornography anonymously—but then again it might be simpler just to show ID.

C. Spam and the CAN-SPAM Act

The example of unsolicited "spam" emails bears close resemblance to the example of adult content—and not just because spam was once a heavy carrier of pornography. In both contexts, the wholly subjective nature of the problem and the wide disparities in recipient preferences make it difficult to draw clear boundaries around objectionable content. Additionally, a substantial proportion of the abuse

---

regating content have been proposed as well. *See, e.g.*, Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BYU L. REV. 1417, 1431–32 (2007) (discussing the use of separate Internet ports as a means of regulating online content).

84. *See* COMM'N ON CHILD ONLINE PROTECTION, *supra* note 83, at 31 (evaluating the red zone/green zone proposal and noting that "[t]his approach could potentially reduce flexibility and impede optimal network performance"); ZITTRAIN, *supra* note 1, at 154–57 (describing the generative cost of dividing a PC into two virtual machines, a Green PC and a Red PC, which would segregate "reliable software and important data" from "everything else").

85. *See* ZITTRAIN, *supra* note 1, at 156–57 ("[M]any of the benefits of generativity come precisely thanks to an absence of walls. . . . [W]e may be hesitant to adopt complex access control and privilege lists to designate what software can and cannot do."). That disadvantage would explain why the dot-kids domain has failed so spectacularly. Maintaining a sterile, rigid sandbox makes it unappealing to populate with either content or usertime. *See* Press Release, NeuStar, Inc., NeuStar Announces Significant Wholesale Price Reductions for KIDS.US Registrars (June 20, 2007), http://www.prnewswire.com/news-releases/neustar-announces-significant-wholesale-price-reductions-for-kidsus-registrars-58226767.html (describing significant reductions in price for domain name registrations at KIDS.US, as well as other efforts to "raise awareness among both potential content providers and the ultimate users of the space," reflecting the dismal unpopularity of kids-only zones).

is conducted by bad actors (many foreign) who are financially motivated to evade regulatory efforts.[86]

An important difference, however, is that the identity-centric approach has been embraced in the spam context. In 2003, Congress passed the CAN-SPAM Act,[87] which neatly divides the problem into two spheres: civil guidelines for mainstream marketers willing to conform their behavior to regulation, and criminal provisions for rogue entities tempted to avoid compliance by remaining anonymous.[88] In the civil section, Congress mandated an opt-out mechanism that allows recipients to refuse future messages, and requires senders to identify themselves accurately and conspicuously so that recipients are not misled when choosing to opt out.[89] The criminal section, then, is directed at the remaining parties who would ignore the civil regulations by hiding behind false mail headers, open relays, zombie computers, and other anonymizing means.[90] Framed in that manner, it is not surprising that the identification requirements have gone unchallenged—the affected parties are either legitimate companies unwilling to be associated with fraudulent spam or illegitimate groups with little interest in coming forward to petition the courts of law.[91]

86. *See COPA II*, 542 U.S. at 667 (noting that a substantial amount of pornography comes from overseas, and that "COPA does not prevent minors from having access to those foreign harmful materials"); *cf. id.* at 663 (describing other efforts by Congress "to prevent Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them").

87. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), Pub. L. No. 108–187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701-13, 18 U.S.C. § 1037 (2006)).

88. *See* Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. ¶ 1, ¶¶ 66–72 (2005) (detailing criminal provisions and civil prohibitions); John Soma, Patrick Singer & Jeffrey Hurd, *Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions*, 45 HARV. J. LEGIS. 165, 178 (2008) ("The CAN-SPAM Act of 2003 does not outlaw spam per se, but instead divides the universe of spam into lawful and unlawful categories.").

89. 15 U.S.C. § 7704(a)(4)–(5).

90. 18 U.S.C. § 1037(a)–(b); *see also* FED. TRADE COMM'N, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT: A REPORT TO CONGRESS A-2 to A-3 (2005), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf (explaining that 18 U.S.C. §§ 1037(a)(1)–(3) criminalize the use of "zombie drones," "open relays with intent to deceive," and "materially false header information," respectively).

91. *Compare* FED. TRADE COMM'N, *supra* note 90, at 8 ("CAN-SPAM has established a framework for lawful commercial email, and legitimate marketers are largely complying

The main criticism of CAN-SPAM has been that it is anemic and ineffective.[92] Much of that discussion has focused on the civil provisions, lambasting the opt-out framework for being too lenient[93] and, by extension, the federal pre-emption provision for prohibiting individual states from experimenting with stricter opt-in schemes.[94] Such debates miss the boat, however, since the overwhelming majority of spam comes from sources that would refuse to comply regardless of what those alternative schemes might be.[95] The merits of a civil regu-

with it, as evidenced by a July 2005 FTC staff study of CAN-SPAM compliance by 100 top online marketers or 'etailers' with the opt-out provisions of the Act."), *with* Bambauer, *supra* note 88, at ¶ 85 (citing a report that "95% of spammers were 'ignoring the law completely'" and noting that spammers have "also reacted to CAN SPAM by shifting activities to foreign jurisdictions such as China that do not criminalize their activities"); *see also* Adam Hamel, Note, *Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-Mail?*, 39 NEW ENG. L. REV. 961, 994–95 (2004–2005) (noting that one surprising effect of CAN-SPAM was "the temporary reduction in commercial e-mail from 'legitimate' on-line marketers immediately after the Act went into effect" in order to "digest the law," while "disreputable spammers . . . reacted to CAN-SPAM by ignoring it, or by trying to find ways around it").

92. *See, e.g.*, Bambauer, *supra* note 88, at 83–85 ("CAN SPAM has been widely derided as ineffective. . . . [S]pam's share of e-mail traffic has increased since CAN SPAM passed."); Soma, Singer & Hurd, *supra* note 88, at 178–79 ("[CAN-SPAM] has been ineffective. Confirming the predictions of some experts, the volume of spam has actually increased since the passage of the Act."); Jeffrey D. Sullivan & Michael B. de Leeuw, *SPAM After CAN-SPAM: How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial E-Mail Policy*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 887, 895–96 (2004) ("Critics also point out that the Act pointedly refrains from providing any private right of action to individual victims of spam. Instead, it vests all enforcement authority in the hands of federal and state agencies and, to some extent, ISPs.").

93. *See* Soma, Singer & Hurd, *supra* note 88, at 178–79 (criticizing the opt-out provision as having "proven to be like trusting the fox with watching over the hen house," and noting that "spam experts discourage the use of opt-out features found in e-mails"); Sullivan & de Leeuw, *supra* note 92, at 895 (explaining anti-spam activists' complaint that the opt-out provision shifts the burden of avoiding spam from the sender to the receiver).

94. *See, e.g.*, Sullivan & de Leeuw, *supra* note 92, at 898–90 (explaining anti-spam activists' complaint that CAN-SPAM is inferior to anti-spam regulations from other jurisdictions); Katherine Wong, Recent Development, *The Future of Spam Litigation After* Omega World Travel v. Mummagraphics, 20 HARV. J.L. & TECH. 459, 469, 473 (2007) (arguing that parallel state enforcement measures would be more effective at reducing spam than a national, uniform liability standard).

95. *See supra* note 91.

lation cannot be evaluated based on harms that are being committed by anonymous actors.

Instead, it is CAN-SPAM's criminal provisions that are key because they establish a norm of identifiability. Presently, spam activities are conducted almost entirely through a small number of "botnets"—vast networks of computers that are owned and operated by legitimate users but covertly controlled by spammers.[96] Botnets allow spammers to steal bandwidth and computational resources, while also obscuring the spammer's trail and helping the spammer evade detection.[97] One recent study found that, in the first half of 2011, just eight botnets were responsible for more than ninety percent of detected spam.[98]

Because complex computer systems invariably contain errors and vulnerabilities, the likelihood that technological responses will eradicate infiltrations is diminishingly small—especially as botnets have become more sophisticated and capable of self-adapting to survive.[99] In recent years, takedowns of major botnets such as Rustock,[100] Mega-

96. *See* M86 SEC. LABS, SECURITY LABS REPORT: JANUARY–JUNE 2011 RECAP 6 (2011), *available at* http://www.sysec.co.uk/media/3357/m86_security_labs_report_1h2011.pdf ("The bulk of spam is emitted from botnets, which are networks of computers compromised by malware."); *see also* Wong, *supra* note 94, at 173 n.52 ("'[B]otnets,' are created by infecting unwitting users' computers with malicious software designed specifically for the purpose of spamming."); Nicholas Ianelli & Aaron Hackworth, *Botnets as a Vehicle for Online Crime* 15 (Proceedings of the International Conference of Forensic Computer Science, 2006), http://www.icofcs.org/2006/ICoFCS2006-pp03.pdf (describing how legitimately owned and operated computers are taken over and controlled by botnets).

97. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415, 428–30 (2012) ("Botnets offer attackers many advantages, such as helping them to evade detection and enabling them to do more harm by controlling a large number of computers.").

98. M86 SEC. LABS, *supra* note 96, at 6–7.

99. *See, e.g.*, Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011 (describing how the Stuxnet virus was able to evolve to avoid detection); John Markoff, *Computer Experts Unite to Hunt Worm*, N.Y. TIMES, Mar. 18, 2009, at A17 (discussing how the Conficker virus has been able to update itself in order to elude detection by computer security firms).

100. *Id.* at 21; Nick Wingfield, *Spam Network Shut Down*, WALL ST. J., Mar. 18, 2011, at B1 ("The Rustock botnet [was] the largest source of spam in the world at the end of [2010].").

D,[101] and McColo,[102] have led to meaningful dips in spam activity.[103] But those reprieves have been temporary, as spam operators remaining at large have been able to resurrect and regrow their networks, or take over territory left behind by others.[104]

More lasting success will depend on tracking down and prosecuting the botnet operators. CAN-SPAM's criminal penalties are crucial in that regard because they validate efforts to root out identities, not just the latest malware.[105] To be sure, legal remedies are not self-executing, so identifiability remains an essential precondition to enforcement.[106] One promising option is to enlist payment intermediaries such as banks and credit cards, on the presumption that spam is fundamentally a for-profit business, and that money is harder to disguise than bits.[107] Whether identity is embedded in the network or

101. Joe Barrett, *Accused Spam King to Be Arraigned*, WALL ST. J., Dec. 3, 2010, at A4 (discussing the takedown of Mega-D); Jeremy Kirk, *FireEye Moves Quickly to Quash Mega-D Botnet*, REUTERS, Nov. 10, 2009, *available at* http://www.reuters.com/article/2009/11/10/urnidgns852573c4006938800025766a-idUS343920408120091110.

102. Brian Krebs, *Major Source of Online Scams and Spams Knocked Offline*, WASH. POST (Nov. 11, 2008, 7:06 PM), http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html (discussing the takedown of McColo Corp.); MARSHAL8E6 TRACELABS, MARSHAL8E6 SECURITY THREATS: EMAIL AND WEB THREATS 3 (2009), *available at* http://www.marshal.com/newsimages/trace/marshal8e6_trace_report_jan2009.pdf (discussing the aftermath and implications of the McColo takedown).

103. *See e.g.*, M86 SEC. LABS, *supra* note 96, at 6 ("The Mega-D botnet slowly ground to a halt as law enforcement authorities identified and pursued the operator in late 2010."); MARSHAL8E6 TRACELABS, *supra* note 102, at 3 (noting that spam dropped fifty percent overnight after the McColo botnet was disabled).

104. *See, e.g.*, MARSHAL8E6 TRACELABS, *supra* note 102, at 3 ("[M]ajor botnets with control servers hosted at McColo (Mega-D and Rustock) eventually recovered and continue to spam strongly.").

105. *But see* Kesan & Hayes, *supra* note 97, at 453–55 (detailing the many shortcomings of a cybercrime approach, including jurisdictional limitations, unwillingness to prosecute, difficulty of attribution, and other evidentiary problems).

106. *See infra* notes 257–275 and accompanying text; *cf.* Hamel, *supra* note 91, at 1001 (noting that computer scientists need to "develop a means of reliably identifying spammers [so that] law enforcement officials can locate spammers and prosecute them under the law").

107. *See* Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037 (2010) (arguing that payment intermediaries offer a way for governments to control illegal activities on the Internet); John Markoff, *Study Sees Way to Win Spam Fight*, N.Y. TIMES, May 20, 2011, at B1 (reporting on a study find-

elsewhere, however, the larger point is that the survival of CAN-SPAM represents a reversal from the invalidations of COPA and the CDA—and a step toward normalizing the use of anonymity-restrictive measures to regulate Internet conduct.

In the meantime, we should be highly skeptical of proposals that seek to modify email technology to fit the problem. Economics-minded commentators have pointed out that the profitability of spam depends on the zero marginal cost of email, and therefore have proposed a range of solutions that would inject artificial cost into the equation.[108] Such proposals include levying a tax on emails, requiring digital postage, compensating recipients for reading spam, adding temporal or computational penalties, and capping the total daily email traffic allowed per sender.[109]

Making people pay for email is problematic in an immediate sense because the additional cost will likely be absorbed by botnet vic-

---

ing that "95 percent of the credit card transactions for the spam-advertised [products purchased in the study] were handled by just three financial companies"); *see also* BEN HAYES, TRANSNAT'L INST. STATEWATCH, COUNTER-TERRORISM, 'POLICY LAUNDERING' AND THE FATF: LEGALISING SURVEILLANCE, REGULATING CIVIL SOCIETY 21 (2012) (describing the global enforcement regime that has been established by the Financial Action Task Force ("FATF"), and the "overall effect" it has had on "revers[ing] the long-established principle of secrecy in financial transactions and introduc[ing] a much broader framework for the surveillance of financial systems").

108. *See* Soma, Singer & Hurd, *supra* note 88, at 169 ("The economic efficiency of spam as an advertising tool contributes to the problem. . . . The marginal cost of adding additional e-mail addresses to a recipient list is minimal, meaning that there is only a negligible cost difference between sending, for example, 1,000 and 10,000 spam e-mails."); Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319, 346 (2005) ("The ease of sending e-mail stems from the open philosophy designed into e-mail technologies. This has led some commentators to propose modifications to the underlying structure for transmitted e-mail messages."); David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. ¶ 1, ¶¶ 18–19 (2004) ("Spam presents a classic tragedy of the commons, arising because individual actors lack an adequate incentive to avoid overusing and abusing valuable resources . . . .").

109. *See* Bambauer, *supra* note 88, ¶¶ 101-08, 164–69 (describing various proposals to impose artificial cost on the spammer such as a "spam tax," e-mail postage, "hash cash," bandwidth limits, reward-based postage, "attention bonds," and more); Soma, Singer & Hurd, *supra* note 88, at 171–74 (describing email postage, computational charges, and email bonds); Hamel, *supra* note 91, at 1002–03 (describing the use of fees, CPU cycles, and "challenge-response" software).

tims (whose computers have been commandeered to send spam) rather than by the spammers themselves.[110] But even if one takes the ruthless attitude that botnet victims should be given an incentive to clean up their computer systems, there is still a larger problem. Making email difficult to use makes email difficult to use. Symbolically, it would represent a giant step back from the advances that we have achieved in global communications, and it would hobble the further development of innovative technologies and business methods that could otherwise be built on top of an unfettered email system. Instead of fixing our sights directly on the real culprits, we would be taxing ourselves twice: financially and innovationally.

D. Defamation and the Communications Decency Act

Of all the online abuses mentioned thus far, the most distressing may be the casual perpetration of "trolling"[111] and cyberbullying.[112] Malicious barbs aired on discussion forums and social networking sites have devastated individuals and outraged communities.[113] Those

110. *See supra* notes 96–98 and accompanying text.

111. *See* Daniel H. Kahn, *Social Intermediaries: Creating a More Responsible Web Through Portable Identity, Cross-Web Reputation, and Code-Backed Norms*, 11 COLUM. SCI. & TECH. L. REV. 176, 187 (2010) ("[A] 'troll' refers to someone who intentionally engages in disruptive behavior characterized by abusiveness to other Web users."); Julie Zhuo, *Where Anonymity Breeds Contempt*, N.Y. TIMES, Nov. 30, 2010, at A31 ("Trolling [is] defined as the act of posting inflammatory, derogatory or provocative messages in public forums.").

112. *See generally* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 377 (2009) (exploring the "gendered nature of online harassment" and "the expressive role that law can play in detrivializing cyber harassment"). *But see* Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 147–51 (1996) ("[M]ore defamation does not necessarily mean more harm; 'anonymous remarks will be greatly devalued precisely because they are anonymous and easy to make.' . . . The effects of speech are difficult to predict because listeners are different; one man's vulgarity may be another's lyric.").

113. *See, e.g.*, Tamara Jones, *A Deadly Web of Deceit A Teen's Online 'Friend' Proved False, and Cyber-Vigilantes are Avenging Her*, WASH. POST, Jan. 10, 2008, at C1 (writing about Megan Meier, a teenager who committed suicide after being bullied through a fake MySpace account by a classmate's mother); Tamar Lewin, *Teenage Insults, Scrawled on Web, Not On Walls*, N.Y. TIMES, May 6, 2010, at A1 (discussing the community outrage in response to Formspring, a social networking site that "has become a magnet for comments, many of them nasty and sexual, among the Facebook generation"); Choe Sang-Hun, *Korean Star's Suicide Reignites Debate on Web Regulation*, N.Y. TIMES, Oct. 13, 2008, at B7 (describing the

who have sought to fight back have encountered two hurdles. First, the Internet's architectural protocols do not provide an easy way for one user to identify other users.[114] Second, Internet intermediaries facilitating the misconduct have little incentive to assist victims by removing or blocking such content, because section 230 of the Communications Decency Act ("CDA") immunizes any "interactive computer service" from civil liability for third-party content.[115]

The original motivation behind section 230 was to propel the generative potential of the Internet. At the time, Congress was concerned about sustaining the nascent growth of the Internet.[116] Online providers were trapped between wanting to supervise and maintain

national reaction to cyberbullying after the suicide of Choi Jin-sil, a famous South Korean actress who committed suicide because of malicious rumors written about her on the Internet); A.G. Sulzberger, *In Small Towns, Gossip Moves to the Web, and Turns Vicious*, N.Y. TIMES, Sept. 19, 2011, at A1 (describing how unsubstantiated gossip on small towns' websites has caused "widespread resentment in communities"); Heather Timmons, *'Any Normal Human Being Would Be Offended'*, N.Y. TIMES INDIA INK (Dec. 6, 2011, 7:35 AM), http://india.blogs.nytimes.com/2011/12/06/any-normal-human-being-would-be-offended/ (reporting that the Indian government has asked social media companies to create a mechanism for screening out offensive content from the Internet).

114. *See* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397–400 (2011) (explaining how the Internet's architecture "provide[s] attackers numerous opportunities to hide their identities or assume another").

115. *See* 47 U.S.C. § 230(c)(1) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); *see also* Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir. 2003) (stating in dicta that, "[a]s precautions are costly, . . . ISPs may be expected to take the do-nothing option and enjoy immunity under § 230(c)(1)"); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 159 (2007) ("Unfortunately, courts are interpreting Section 230 so broadly as to provide too much immunity, eliminating the incentive to foster a balance between speech and privacy."); Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 412–22, 429 (2009) (noting that the unavailability of easy remedies against malicious online speech has created a market for reputation defense services, which have "unsavory incentives . . . to stir up trouble, or at least to perpetuate the conditions that create it").

116. *See* 47 U.S.C. § 230(b)(1)–(2) (stating among its policy goals: "to promote the continued development of the Internet," and "to preserve the vibrant and competitive free market that presently exists for the Internet"); *cf.* S. CONF. REP. NO. 104-230, at 190 (1996) (expressing, with regard to a separate provision, the intent "to avoid impairing the growth of online communications").

attractive forums for users, and being exposed to crippling liability if that oversight were construed as accepting editorial responsibility for user content.[117] Congress therefore made a deliberate choice to prioritize the development of Internet services over the enforcement of tort liability. The gambit has paid off handsomely: countless innovative offerings have thrived on the Internet in large part because of section 230 immunity.[118]

Now that the Internet has matured, many scholars have pointed the finger at section 230, characterizing it as a well-meaning but mistaken relic of a bygone era.[119] In particular, the discrepancy that section 230 sets up between offline liability and online liability has been well tread in the literature: Ordinarily, publishers and distributors of printed materials are subject to certain duties of care regarding defamatory content, but on the Internet none of those duties apply.[120] As a result of that immunity, it has become exceedingly easy to pub-

117. *See* Holland, *supra* note 19, at 370–72 (recounting the historical context leading to the passage of the CDA, in which online service providers complained that they faced a "Hobson's choice" preventing them from creating "child safe" areas); Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 258–63 (2006) [hereinafter Zittrain, *Online Gatekeeping*] (same).

118. *See* Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 433–36 (2009) [hereinafter Balkin, *Free Expression*] ("Because online service providers are insulated from liability, they have built a wide range of different applications and services that allow people to speak to each other and make things together."); Nicholas W. Bramble, *Safe Harbors and the National Information Infrastructure*, 64 HASTINGS L.J. 101, 133–34 (2013) ("Together, section 512 of the DMCA and section 230(c) of the CDA risk a good deal of unregulated creativity and communication on the boundaries of copyright law and defamation law, on the theory that the rewards of such creativity . . . outweigh the risks of inefficient policing of violations of copyright, defamation, and obscenity law.").

119. *See* Kahn, *supra* note 111, at 189–93 & n.86 (2010) (describing the general discontent with section 230, and collecting academic articles calling for reform); Holland, *supra* note 19, at 392–93 ("Early critics of § 230 tended to focus on the issues of congressional intent and broad interpretation by the courts. More recent commentators have moved beyond these issues to engage the larger implications of providing such sweeping immunity to online intermediaries, suggesting amendments to § 230 intended to effectuate policies of efficiency and cost allocation.").

120. *See, e.g.*, Holland, *supra* note 19, at 374–75; Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 197–98 (2006); Paul Ehrlich, Note, *Communications Decency Act § 230*, 17 BERKELEY TECH. L.J. 401, 404–05 & n.29 (2002); Jae Hong Lee, Note, Batzel v. Smith & Barrett v. Rosenthal*: Defamation Liability for Third-Party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 492–93 (2004).

lish offensive statements online, and exceedingly difficult to expunge them from the record once they are posted—a problem that is further compounded by the Internet's broad reach.[121] Nevertheless, courts have consistently upheld that interpretation of section 230 immunity as a faithful reflection of congressional intent.[122]

Despite the rising calls for reform, it is not clear that section 230 has outlived its usefulness. The Internet has matured, but it is not dead. Narrowing the scope of section 230 would certainly aid in deterring defamation and sanitizing the Internet, but it would do so by forcing intermediaries to become more circumspect about tolerating experimental uses.[123] Few entities, if any, would be able to absorb the cost of indemnifying user-generated content, and those that could would likely demur.[124] Typically, that problem is presented in terms of harm to speech interests, i.e., that intermediaries will engage in "collateral censorship" by erring on the side of caution and suppress-

121. *See* Bartow, *supra* note 115, at 418 ("By writing § 230 into law, Congress left . . . Internet harassment victims vulnerable and helpless, especially if they are not able independently to identify the sources of the abuse, or to acquire forcibly identifying information from an ISP, assuming it had been logged, via the subpoena power of the courts."). *But see* Holland, *supra* note 19, at 393 (arguing that "it is not clear that a significant number of bad actors are beyond the reach of the law").

122. The judicial consensus runs so deep that two state appellate court decisions in California created a stir when daring to challenge it; both decisions were reversed on appeal. *See* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 153–54 (Cal. Ct. App. 2004) (acknowledging that "no court has subjected a provider or user of an interactive computer service to notice liability for disseminating third-party defamatory statements over the Internet," but that "most scholars" view that analysis as "flawed"), *rev'd*, 146 P.3d 510, 518–19 (Cal. 2006) (noting that the Court of Appeal was "[s]wimming aginst the jurisprudential tide"); Grace v. eBay Inc., 16 Cal. Rptr. 3d 192, 198–99 (Cal. Ct. App. 2004), *dismissed by* 101 P.3d 509 (Cal. 2004); *see also* David A. Myers, *Defamation and the Quiescent Anarchy of the Internet: A Case Study of Cyber Targeting*, 110 PENN. ST. L. REV. 667, 679–85 (2006) ("Two . . . important decisions providing some hope for the victims of cyber targeting are now before the California Supreme Court.").

123. *See* Holland, *supra* note 19, at 391, 395 (arguing that "narrow[ing] the grant of immunity [under section 230] would significantly damage the online environment," and that the extension of traditional liability rules to online intermediaries may "result[] in overly broad restrictions on expression and behavior").

124. *See* Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Liability*, 87 NOTRE DAME L. REV. 293, 300–04 (2011) (stating that most intermediaries would block or limit content rather than develop a system to police content).

ing protected speech that is controversial or borderline.[125] But the more pervasive problem is the upstream harm to generativity and innovation.[126] If section 230 were repealed, in part or in whole, then we would need to reevaluate major components of the Internet, especially those surrounding user-generated content. We could expect to lose much of the serendipity that makes the Internet special.

If we do not like that prognosis, the alternative is to turn to identification measures to reinstate offline laws and norms. The courts have been amenable to that approach on a case-by-case basis, issuing orders to assist individual victims in identifying their antagonizers as long as good cause is shown and due process is satisfied.[127] While those judicial measures are helpful, they depend on the victim being able and willing to sue. Even then, the measures are only partially effective, as they can be foiled by simple evasions such as the use of public computers, shared network connections, and proxy servers.[128]

---

125. *See* Balkin, *supra* note 118, at 435 ("[I]ntermediary liability produces a phenomenon called *collateral censorship:* Threats of liability against party *A* (the conduit or online service provider) give them reasons to try to control or block the speech of party *B* (the online speaker)."); *see also* Wu, *supra* note 124, at 296–97, 304–09 ("The unique harm of collateral censorship, as opposed to self-censorship, lies in the incentives that intermediaries have to suppress more speech than would be withheld by original speakers. This additional suppression occurs . . . both because original speakers obtain benefits from the speech not realized by intermediaries and because intermediaries face liability risks not borne by original speakers.").

126. *See, e.g.*, Balkin, *supra* note 118, at 435–36 ("The problem with the strategy of collateral censorship in the Internet context is that it leads to . . . too little innovation.").

127. *See* Clay Calvert et al., David Doe v. Goliath, Inc.: *Judicial Ferment in 2009 for Business Plaintiffs Seeking the Identities of Anonymous Online Speakers*, 43 J. MARSHALL L. REV. 1, 40–46 (2009) (comparing the legal standards for unmasking an online user across four recent cases); Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM. L. & POL'Y 405, 421 (2003) (same with six cases); *see also* Cohen v. Google, 887 N.Y.S.2d 424, 429 (N.Y. Sup. Ct. Aug. 17, 2009) ("Those who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights." (citation and quotation marks omitted)); Amir Efrati, *Subpoenas Allowed in AutoAdmit Suit*, WALL ST. J. LAW BLOG (Jan. 30, 2008, 9:08 AM), http://blogs.wsj.com/law/2008/01/30/subpoena-allowed-in-autoadmit-suit/ (reporting that subpoenas were issued in the AutoAdmit case for the identities of users who had posted allegedly defamatory remarks online).

128. *See* COLE STRYKER, HACKING THE FUTURE: PRIVACY, IDENTITY, AND ANONYMITY ON THE WEB 174–84 (2012) (describing a variety of obfuscation tactics, including web-based

Some regulators have begun to take more proactive steps such as imposing "real name" requirements. Among nations, the most visible efforts have come from China and South Korea,[129] and in the private sector, from operators of social networks such as Facebook and Google.[130] Thus far, those policies have been poorly implemented and inconsistently applied.[131] They have also drawn heavy criticism,

redirectors, encryption tools, proxy servers, VPN tunneling, and further measures such as buying a separate computer using a prepaid credit card, using prepaid phones, and using someone else's Internet connection); David Margolick, *Slimed Online*, UPSTART BUS. J. (Feb. 11, 2009, 8:00 AM), http://upstart.bizjournals.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying.html (noting that subpoenas in the AutoAdmit case "failed to yield much, in part because many posters had taken care to send their messages from internet cafés and other public computers").

129. *See* Eric S. Fish, *Is Internet Censorship Compatible with Democracy?: Legal Restrictions of Online Speech in South Korea*, 10 ASIA-PACIFIC J. ON HUM. RTS & L., No. 2, 2009, at 43, 85 (stating that the South Korean National Assembly passed "an amendment to the *Law on Internet Address Management* requiring Korean websites with over 100,000 daily visitors to have their users register with their real names and social security numbers"); John M. Leitner, *To Post Or Not to Post: Korean Criminal Sanctions for Online Expression*, 25 TEMP. INT'L & COMP. L.J. 43, 61–64 (2011) (describing the first two years of Korea's experience with the Real Name Verification System); Jonathan Ansfield, *China Adds Layer of Web Surveillance With a Rule Seeking Users' Names*, N.Y. TIMES, Sept. 6, 2009, at A4 ("News Web sites in China, complying with secret government orders, are requiring that new users log on under their true identities to post comments."); Chris Buckley, *Analysis: China Seeks to Tether the Microblog Tiger*, REUTERS, Sept. 16, 2011, *available at* http://www.reuters.com/article/2011/09/16/us-china-internet-idUSTRE78F04D20110916 (writing that one of the ways of regulating microblogs being considered by the Chinese government was "demanding that users who forward messages use their real names"). *But see* ACLU of Georgia v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (invalidating a state statute that criminalized any internet transmission that falsely identified or misrepresented the sender).

130. *See* danah boyd, *The Politics of 'Real Names': Power, Context, and Control in Networked Publics*, 55 COMM. ACM 29, 29–31 (2012) (contrasting the norm among many Facebook users to follow the terms of service requiring "real names and information," with Google's failure to impose a similar policy).

131. *See, e.g.*, Eric Pfanner, *Naming Names on the Internet*, N.Y. TIMES, Sept. 5, 2011, *available at* http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html (discussing the failure of South Korea's experiment with the real-name requirement after hackers stole 35 million national identification numbers that were being used for validation); Tini Tran, *Activist Michael Anti Furious He Lost Facebook Account—While Zuckerberg's Dog Has Own Page*, HUFFINGTON POST (Mar. 8, 2011, 7:35 PM), http://www.huffingtonpost.com/2011/03/08/michael-anti-facebook_n_832771.html (discussing how Facebook

for reasons ranging from wrongful enforcement and loss of privacy, to physical endangerment of activists and dissidents.[132] As a result, several entities have subsequently rescinded their policies while the remaining ones have not yet been very vigilant in their enforcement.[133]

Yet, in the long run, defeating policies like real name requirements may be a pyrrhic victory. The more ground we give to anonymity, the more we paint ourselves into a corner where the only way to regulate offensive speech is to pre-emptively block the tools and platforms used to produce it. As an example, website operators have found that they have two main options to deal with abusive comments. One option is to impose a registration requirement that creates some degree of accountability.[134] Email addresses have long been the dominant identifier on the Internet—a legacy of early UNIX computers and online service providers, which assigned only one account per user and made new accounts difficult to obtain. But free webmail services spoiled that assumption years ago, reducing registration requirements into little more than a formality.[135] The failure of

canceled the account of a Chinese activist because of a "strict" policy against pseudonyms, yet allows Mark Zuckerberg's dog to have its own account).

132. *See* Alexis Madrigal, *Why Facebook and Google's Concept of 'Real Names' is Revolutionary*, ATLANTIC, Aug. 5, 2011 (arguing that "[o]n the boulevards and town squares of Facebook, you can't just say, 'Down with the government,'" because "if a government or human resources researcher or plain old enemy wants to get a hold of it, it is possible"); Pfanner, *supra* note 131 (citing privacy and political dissent); Tran, *supra* note 131 ("Dissidents in a variety of countries have argued that Facebook's policy can endanger human rights activists.").

133. *See, e.g.*, Loretta Chao, *Microblogs Survive Real-Name Rules–So Far*, WALL ST. J. BLOGS (Apr. 30, 2012, 5:24 PM), http://blogs.wsj.com/chinarealtime/2012/04/30/microblogs-survive-real-name-rules-so-far/ (observing that Chinese web users could still post messages on microblogs without verifying their identities despite a government-imposed deadline for real-name registration).

134. *See, e.g.*, Richard Pérez-Peña, *News Sites Rethink Anonymous Online Comments*, N.Y. TIMES, Apr. 11, 2012, at B1 ("The New York Times, The Post and many other papers have moved in stages toward requiring that people register before posting comments, providing some information about themselves that is not shown onscreen.")

135. Interestingly, a hierarchy developed among free webmail services in which some were deemed more reputable than others. Gmail quickly became the gold standard upon its launch in 2004, in part because the addresses were highly desirable and difficult to replace, and because they were initially doled out via social connections. *See* Juliet Chung, *For Some Beta Testers, It's About Buzz, Not Bugs*, N.Y. TIMES, July 22, 2004 (reporting that invitations to use Gmail were being auctioned for prices as high as $200). Yahoo and Hotmail

email-based registration forced many websites to move grudgingly in the other direction and restrict the commenting function itself—whether by adding a screening process, hiding all comments by default, or disabling the function entirely.[136] Only with the emergence of social networking sites, which have created better identifiers to replace the email address, has that trend reversed; a sea change is now under way to integrate validation through entities such as Facebook.[137]

Regulating defamation involves the same tradeoff. Reforming section 230 to restore intermediary liability for user-generated defamation would pressure websites to adopt corresponding restrictions that limit their exposure to risky user behavior.[138] Even confining liability to "cyber-cesspools"[139]—the worst of the worst—would invite def-

addresses—hardly trustworthy but too widely used to ignore—were a cut below and only sometimes refused as credentials, while addresses at webmail services that explicitly advertised anonymizing features (such as Hushmail or Mailinator) were almost always rejected by community forums.

136. *See, e.g.*, Pérez-Peña, *supra* note 134 ("Some sites and prominent bloggers, like Andrew Sullivan, simply do not allow comments.").

137. *See, e.g.*, Kahn, *supra* note 111, at 217–19 (explaining how social intermediaries enable individuals to project a consistent identity across the Internet); James Rainey, *On the Media: Your Words, Your Real Name*, L.A. TIMES, Feb. 26, 2011, *available at* http://articles.latimes.com/2011/feb/26/entertainment/la-et-onthemedia-20110226 (reporting that the Bay Area News Group is requiring commenters to use their Facebook identities); *Facebook Commenting FAQ*, USA TODAY, http://usatoday30.usatoday.com/news/story/2011-11-28/Facebook-comments-FAQ/51451552/1 (last visited Jan. 10, 2012) (explaining new policy requiring a Facebook account with a profile photo and at least four friends in order to comment on stories).

138. *See* Balkin, *Free Expression*, *supra* note 118, at 436 ("If I were liable for comments posted in response to my blog posts, I simply would not allow any comments. The same is true for online versions of newspapers and magazines which now allow readers to respond by posting comments. Without section 230, many website operators would simply disable these features."); David V. Richards, Note, *Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act*, 85 TEX. L. REV. 1321, 1350 (2007) (proposing a "notice-based liability" system in which Internet providers "would only be liable for defamatory or privacy-invading content of which they were actually aware or notified," but noting that under such a system, providers "would likely not monitor users and simply remove posts called to their attention").

139. *See* Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH AND REPUTATION 155 (Saul Levmore & Martha C. Nussbaum eds., 2010); Danielle Citron, *Revenge Porn and the Uphill Battle to Pierce Section 230 Immunity (Part II)*, CONCURRING OPINIONS (Jan. 25, 2013, 3:30 PM), http://www.concurring

initional uncertainty as to where the line should be drawn, as well as malicious attacks of planned vitriol at otherwise innocuous websites to cause mayhem.

Or we could push regulation down the other path by adopting a vicarious liability regime for anonymous content. Websites could allow anonymous content as long as they were willing to assume the risk. Conversely, websites that adopted identity-validating measures could continue to support user-generated content without having to make difficult judgment calls about whether doing so might confer liability—the key benefit of section 230. Defamation would be curtailed, or at least redressable, without adverse effects on generativity.

Another possible response is that we should simply accept the existence of defamatory speech, develop thicker skins, and forego all speech regulation.[140] That is not the approach we have chosen for offline speech, and it seems unlikely that it will be the choice we ultimately make for online speech. But, again, the purpose here is not to address whether or when defamation ought to be proscribed. Rather, it is to offer a lens for viewing the available options once the decision to regulate has been made.

Choosing to restrict anonymity does not mean we need to go as far as mandatory real-name policies. "Real enough" may be good enough.[141] Some proposals, for instance, have suggested promising

---

opinions.com/archives/2013/01/revenge-porn-and-the-uphill-battle-to-pierce-section-230-immunity-part-ii.html (advocating a narrower amendment to section 230 that would revoke immunity only against "websites designed to facilitate illegal conduct or [that] are principally used to that end").

140. *See* Rosenblatt v. Baer, 383 U.S. 75, 95 (1966) (Black, J., concurring in part and dissenting in part) ("The only sure way to protect speech and press against these threats is to recognize that libel laws are abridgments of speech and press and therefore are barred in both federal and state courts by the First and Fourteenth Amendments."); Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 160–61 (2008) (arguing that "such speech, even if uncivil, unrefined, or even frequently wrong, is an essential component of the marketplace of ideas").

141. *See, e.g.*, JOHN HENRY CLIPPINGER, A CROWD OF ONE 118–19 (2007) (noting that, in the late 1990s, eBay held fraud to less than 0.01% by creating a feedback system, and providing other community-building devices such as "neighborhood watch" groups and the Giving Board); Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problem of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991 (2004) (arguing that traceable pseudonymity offers the best compromise).

alternatives to the top-down model of assigning one unitary identity.[142] A federated model could offer more flexibility to create different, parallel identification models that fill different contextual needs. At the very least, we should consider the likelihood that the creation of some system of compulsory identifiability is (perhaps counterintuitively) the necessary first step toward preserving the "future of the Internet" that Zittrain and others seek.

III. THE GENERATIVE COST OF ANONYMITY

There is good reason why anonymity and generativity are key pressure points. Both are tools that empower individuals to resist rules that ordinarily constrain behavior. Anonymizing technologies allow dissenting voices to challenge existing norms and hierarchies.[143]

142. *See, e.g.*, KIM CAMERON, THE LAWS OF IDENTITY (2005), http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (describing a unifying identity metasystem that would allow diverse implementations and approaches to digital identity as long as they follow seven essential laws); Johnson, Crawford & Palfrey, *supra* note 108, at 15 (2004) (recommending a decentralized "peer production" model for the Internet that would allow individuals to develop a trust-based system for the flow of information).

143. *See, e.g.*, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 1003–07 (1996) (arguing that "[t]houghts and opinions, which are the predicates to speech, cannot arise in a vacuum," and that a right to read anonymously is necessary for the "iterative process of 'speech-formation'—which determines, ultimately, both the content of one's speech and the particular viewpoint one espouses"); Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1586–89 (2007) (arguing that "First Amendment jurisprudence . . . clearly prefers anonymous speech to no speech at all," because "governmental attempts to 'prescribe what shall be orthodox' have resulted frequently in suppression of truth and enshrinement of error"); Gayle Horn, Note, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 764–67 (2005) ("[A]nonymity not only mitigates the potential for individuals to be deterred from exercising their speech or associational rights, it also is crucial for identity formation and social interaction."); Alexander T. Nguyen, Note, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2 ¶ 52 (2002) (collecting cases that have protected anonymity in a variety of different contexts); Jennifer B. Wieland, Note, *Death of Publius: Toward a World Without Anonymous Speech*, 17 J.L. & POL. 589, 590 (2001) ("As the Supreme Court has observed, anonymous expression has played an important role in the progress of mankind."); A. Michael Froomkin, Lessons Learned Too Well 31–33 (Sept. 22, 2011) [hereinafter Froomkin, *Lessons Learned*] (unpublished manuscript), *available at* http://ssrn.com/abstract=1930017

Likewise, generative technologies allow new innovations to break settled patterns of behavior.[144] The freedom to transcend such constraints can foment positive change and progress. But it can also lead to harmful disruption and disorder. When anonymity allows perpetrators to escape detection, harms go unredressed[145] and the aggregate incidence of harmful behavior increases.[146] Generativity poses a similar threat—a lurking fear that at any moment irreparable damage could be committed in scary, unanticipated ways.[147] By their very nature, both anonymity and generativity are messy, and they cannot be channeled to show only their Sunday best.

(stating the importance of anonymity to prevent sinister profiling by corporate and public hands, which can constrict the economic and political freedoms of the persons profiled).

144. *See* ZITTRAIN, *supra* note 1, at 79–94 (describing the benefits of generativity as "at least two distinct goods, one deriving from unanticipated change, and the other from inclusion of large and varied audiences").

145. *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 404–05 (1996) [hereinafter Froomkin, *Flood Control*] ("Sissela Bok has argued that a society in which 'everyone can keep secrets impenetrable at will' . . . would be undesirable because 'it would force us to disregard the legitimate claims of those persons who might be injured, betrayed, or ignored as the result of secrets inappropriately kept.' . . . This damage to society's ability to redress legitimate claims is, I believe, the strongest moral objection to the increase in anonymous interaction."); Lidsky & Cotter, *supra* note 143, at 1559 ("Speakers may use the shield of anonymity for a variety of purposes, only some of which may be consistent with the public good."); Sharon K. Sandeen, *In for a Calf Is Not Always in for a Cow: An Analysis of the Constitutional Right of Anonymity as Applied to Anonymous E-Commerce*, 29 HASTINGS CONST. L.Q. 527, 543–44 (2002) (discussing "[t]he concern[s] that anonymity enables fraud" and makes it difficult to obtain information about an individual's actions, thus avoiding detection).

146. *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 142 [hereinafter Post, *Pooling Intellectual Capital*] (describing "the attendant moral-hazard problem: to the extent individuals can avoid internalizing the costs that their behavior imposes on others, widespread anonymity may increase the aggregate amount of harmful behavior itself"). Interestingly, although some studies have suggested that anonymity leads to an increase in anti-social behavior, others claim that the results are inconclusive. *See* Diane Rowland, *Griping, Bitching and Speaking Your Mind: Defamation and Free Expression on the Internet*, 110 PENN ST. L. REV. 519, 531–35 (2006).

147. *See* ZITTRAIN, *supra* note 1, at 96 ("Generative technologies . . . invite disruption—along with all the good things and bad things that can come with such disruption.").

The Internet amplifies those effects both in magnitude and in speed.[148] Any new technology can be expected to spawn a period of increased generativity, but the Internet is unique in that it has taxed the limits of society's tolerance along both axes at the same time. As we intervene to regulate against online abuses, however, we must force ourselves to weigh carefully the costs of restricting generativity against the costs of restricting anonymity. Otherwise, the Internet will be shaped by unintended consequences, and the path of least resistance may well turn out to be an anti-generative one. Even worse, we might inadvertently restrict both anonymity and generativity far beyond what is necessary or optimal.

The claim that anonymity and generativity promote liberty is backwards. Rather, a society that is liberal will choose to allow more anonymity and more generativity, while a society that is restrictive will choose to allow less of each. All else equal—if we hold the desired level of enforcement as given and fixed—the relevant question is not whether generativity or anonymity can shift the balance between liberty and security, but instead whether the liberties afforded by generativity should be traded for the liberties afforded by anonymity.[149]

148. *See* Tien, *supra* note 112, at 151–54 ("Amplification has distributional consequences as well as communicative ones. It is not merely that more hearers may be reached, but that hearers in different places may be reached."); Scott Hammack, Note, *The Internet Loophole: Why Threatening Speech On-line Requires a Modification of the Courts' Approach to True Threats and Incitement*, 36 COLUM. J.L. & SOC. PROBS. 65 (2002) (describing how features enabled by the Internet such as widespread audiences and rapid exchange of information have an amplifying effect on threatening speech); Horn, *supra* note 143, at 772 ("Even more so than print or television media, the Internet acts as an amplifier. It likely hosts a larger number of listeners in total as well as listeners from a larger number of places. This magnifies the problems inherent in a right to anonymity . . . ."). Metcalfe's Law, a proposition developed to explain why individuals "needed more Ethernet boards than they were buying," predicts that the power of a network grows at an exponential rate relative to the number of connected users. James Hendler & Jennifer Golbeck, *Metcalfe's Law, Web 2.0, and the Semantic Web*, 6 WEB SEMANTICS: SCI. SERVS. & AGENTS ON WORLD WIDE WEB 14, 14–15 (2008), *available at* http://www.cs.umd.edu/~golbeck/downloads/Web20-SW-JWS-web Version.pdf (using Metcalfe's Law to explain the network effect of the Web).

149. *Cf.* Joseph William Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 WIS. L. REV. 975, 1022–23 (1983) ("The fact is that if people were truly prohibited from interfering with the legal liberties of others, no one would be free to do anything. We want people to be able to interfere in some ways with others, and we want to stop them from interfering in other ways. The point is to choose, not to lull people into believing that the problem does not exist.").

Those who are anonymity maximalists argue that anonymity is too easily compromised, and that tolerating occasional vandals is a small price to pay for the singular ability to resist authoritarian control.[150] Some have suggested that online abuses are more tolerable because they involve only informational harms, not physical harms.[151] If anonymity could be revoked every time it were deemed the slightest bit displeasing, then it would be worse than useless. Under that view, bright-line protection of anonymity is necessary to prevent gradual encroachments on legitimate uses of anonymity.

Yet, anonymity does not exist in a vacuum, and protecting it will come at direct cost to generativity. Some legal protection of anonymity is useful, but perfect anonymity is fool's gold. Escaping the constraints of one's physical identity requires the aid of technology—whether it is as simple as a Guy Fawkes mask[152] or as complex as the Internet. The trouble with using technology to elevate anonymity above the law is that it turns the enabling technology into a target.

150. *See, e.g.*, Froomkin, *Lessons Learned*, *supra* note 143.

151. *See* ZITTRAIN, *supra* note 1, at 97 ("One might want to allow more room for experimentation in information technology . . . because the risks of harm—particularly physical harm—are likely to be lower as a structural matter from misuse or abuse of information technology."); Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1385–86 (2008) ("Nobody has ever been killed as the result of an online attack. The Internet has never 'crashed' and never will."). *But see* Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES, Oct. 11, 2012, at A1 (reporting comments by the U.S. Defense Secretary that the United States is increasingly vulnerable to a "cyber-Pearl Harbor that would cause physical destruction and the loss of life"); Barnaby J. Feder, *Computer Security Team to Report Hacking Into Defibrillator-Pacemaker,* N.Y. TIMES, Mar. 12, 2008, at C4 (discussing how a team of computer security researchers managed to hack into and control a combination heart defibrillator and pacemaker in a way "that would potentially be fatal if the device had been in a person"); Nadya Labi, *Are You Sure You Want to Quit the World?*, GQ, Oct. 2010, at 234 (reporting on a middle-aged man who had been lurking in suicide chat rooms, and posing as a twenty-something female nurse for the thrill of encouraging others to take their lives); Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (noting that the Stuxnet worm used digital code "to physically destroy something in the real world"); *see also supra* note 113 and accompanying text .

152. *See* Tim Murphy, *The Last Laugh, 500 Years Later*, N.Y. TIMES, Oct. 30, 2011, at ST6 (reporting that a mask bearing the image of Guy Fawkes, a seventeenth-century English folk hero, was "imbued . . . with real-life symbolism" by "the 'hacktivist' collective, Anonymous," who "donned the masks whenever they appeared in public").

Such countermeasures are effective precisely because they reduce the generativity of the system. When relatively little generativity is at stake (as with masks), restricting use of that technology (such as through anti-mask laws) might have little consequence.[153] But extending that tack to a highly generative system such as the Internet exacts a more severe toll. That is not to say that all anonymity should be sacrificed in order to maximize generativity. Rather, the danger is the opposite—that perfecting anonymity will quash too much generativity.

A. Dog Days of Anonymity

"On the Internet," goes the infamous quip, "nobody knows you're a dog."[154] It is a tongue-in-cheek statement, but it embodies a common perception that anonymity is a binary on/off switch—either your real identity is known or it is not. Of course, that is not quite right; we share our identity with some parties while seeking to remain anonymous vis-à-vis everyone else.[155] A better depiction of anonymity is as a curtain that we draw between our confidants and distrusted outsiders.[156] We remain effectively anonymous to those outsiders as long as the curtain remains intact, though anyone within its curtilage has the ability to welcome others inside.

Thus, the security of an anonymous interaction is governed by two factors: (1) the number of confidants, and (2) the strength of secrecy to which they are bound. What some scholars have termed "un-

153. For a contrasting view and a comprehensive survey of judicial treatment of anti-mask laws, see Margot E. Kaminski, *Real Masks and Real Name Policies: Comparing State Anti-Mask Laws to the Doe Anonymous Online Speech Standard*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. (forthcoming 2013).

154. *See* Glenn Fleishman, *Cartoon Captures Spirit of the Internet*, N.Y. TIMES, Dec. 14, 2000, *available at* http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html (tracing the influence and popularity of the caption, which originated in a New Yorker cartoon).

155. *Cf.* Zeynep Tufekci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, 28 BULL. SCI. TECH. & SOC'Y 20, 21 (2008) ("In technologically mediated sociality, *being seen* by those we wish to be seen by, in ways we wish to be seen, and thereby engaging in identity expression, communication and impression management are central motivations.").

156. *See* Saul Levmore, *The Anonymity Tool*, 144 U. PA. L. REV. 2191, 2202 (1996) ("[A]nonymity is an accepted social practice not when it is complete but rather when there is anonymity as to some recipients or subjects but identifiability to a responsible intermediary.").

traceable anonymity" is simply the edge case where there are no known confidants.[157] "Traceable" anonymity, on the other hand, refers to cases in which the confidants are already known and the only remaining variable is their discretion,[158] which can then be swayed by external forces such as legal penalties, group norms, and economic incentives.[159]

As a practical matter, it has become clear over the past decade that most Internet users are identifiable if sufficient need is demonstrated. Mechanisms exist, or have been put in place, that can be in-

157. *See* Froomkin, *Flood Control*, *supra* note 145, at 416–24 (defining "untraceable anonymity" as "a communication for which the author is simply not identifiable at all"); John Alan Farmer, Note, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725, 745–46 (2003) (describing untraceable anonymity in similar terms).

158. *See* Zarsky, *supra* note 141, at 1031–32 ("Traceable pseudonymity enables a two-way link between the pseudonym and the physical self by allowing the individual to directly and discreetly receive messages intended for the alias."). Froomkin describes the following situation as an example of traceable electronic anonymity: "A remailer that gives the recipient no clues as to the sender's identity, but leaves this information in the hands of a single intermediary." Froomkin, *Flood Control*, *supra* note 145, at 417; *see also* Farmer, *supra* note 157, at 151 ("[T]he traceability of a message may be largely a function of the remailer's duty (or lack of a duty) to keep the information secret . . . .").

159. David Post adds nuance to Froomkin's basic framework by defining traceability as the ease with which additional identifying information can be obtained, not simply whether it can be obtained at all. Post further notes that "the cost of obtaining a given amount of additional identification information will vary, possibly greatly, from one situation to another." *See* Post, *Pooling Intellectual Capital*, *supra* note 146, at 150–51; *see also* Reno v. Condon, 528 U.S. 141, 143, 151 (2000) (upholding the constitutionality of the Driver's Protection Privacy Act, which "regulates the disclosure and resale" of drivers' personal information by state motor vehicle departments); Russell Dean Covey, *Beating the Prisoner at Prisoner's Dilemma: The Evidentiary Value of a Witness's Refusal to Testify*, 47 AM. U. L. REV. 105, 129–32 (1997) (analyzing a witness's choice to invoke the Fifth Amendment and suggesting that "[t]he force of the code of silence, or *omerta*, may spring from internal assimilation of a set of values adverse to the duties imposed by the criminal justice system"); Zarsky, *supra* note 141, at 1040–41 ("To maintain a traceable pseudonymous environment, the two walls described above—the walls (1) between the various identities and the physical persona, and (2) among the various identities themselves—must remain intact. The strength of these walls, however, will be constantly tested."); Farmer, *supra* note 157, at 151 (noting that the traceability of a message is influenced by "the ease with which disclosure can be legally compelled (by process, subpoena, warrant, or otherwise)").

voked to pierce the veil of anonymity.[160] Nevertheless, online anonymity remains relevant for at least three reasons. First, there is an overwhelming perception of anonymity among Internet users, which continues to shape their online conduct.[161] Second, the functional reality of anonymity is that it remains too burdensome to pursue identification in most cases, especially for ordinary citizens.[162] Third, there is an aspirational goal of anonymity, especially among technologists and policy advocates who remain committed to the task of building more perfect anonymizing tools for the Internet.[163]

Many justifications have been offered in defense of anonymity, but they can be organized around three major themes: privacy, participation, and truth. Together, they form an engine of change that incubates and nurtures ideas from private inception to public adoption. As we will see later, those three themes mirror parallel attributes of generativity.

For most of us, of course, being anonymous is not about changing the world. All we want is shelter from prying eyes to conduct our personal business. The term "privacy" encompasses many concepts,[164]

160. *See, e.g.*, Stored Communications Act, 18 U.S.C. § 2703(c) (2006) (enacting provisions for the "[r]equired disclosure of customer communications or records"); Council Directive 2006/24/EC, 2006 O.J. (L 105/54) (EC) (relating to "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks"); Dendrite Int'l, Inc. v. Doe, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001) (offering judicial guidelines for unmasking a "John Doe" defendant).

161. *See* Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 835 (2010) (noting that people "feel anonymous amidst the millions of [other] users").

162. *See, e.g.*, Margolick, *supra* note 128.

163. *See, e.g.*, Jim Dwyer, *Using His Software Skills with Freedom, Not a Big Payout, in Mind*, N.Y. TIMES, Apr. 18, 2012, at A20 (reporting on the development of Cryptocat, a tool that allows up to ten people to speak privately to one another in encrypted chat rooms); James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES, June 12, 2011, at A1 (reporting that the U.S. State Department has been funding the development of anonymizing software); *see also* STRYKER, *supra* note 128, at 174–84 (explaining that it is possible to remain totally anonymous on the Internet, "but it's *very* hard"). *But see* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL FORUM 1, 18–20 (2008) (praising the "struggle" for perfection, though not the achievement of perfection, as a valuable way to balance the interests between transparency and privacy).

164. *See generally* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) ("[P]rivacy is a sweeping concept, encompassing (among other things) freedom of thought, control over

but the one most often associated with "anonymity" is the desire to protect one's reputation and well-being in one context from the consequences of one's actions in another context.[165] By providing that separation, anonymity creates a permissive environment that allows for greater incubation of thought and experimentation with ideologies and practices diverging from what is perceived to be the acceptable norm.[166] With an anonymous Internet, we can be bolder in searching the Web for sensitive information or keeping an online diary, because anonymity constructs a barrier that prevents those "private" acts from being linked back to our identities.[167]

---

one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67 (2010) (noting that "privacy is a messy and complex subject" and that "[t]he landscape of theoretical work on privacy is vast, spanning disciplines from philosophy to political science").

165. *See* Cohen, *supra* note 143, at 1038–39 (arguing that "reading is so intimately connected with speech, and so expressive in its own right, that the freedom to read anonymously must be considered a right that the First Amendment protects"); Horn, *supra* note 143, at 765 ("[A] right to anonymity ensures that an individual will have control over how he or she chooses to reveal him or herself, and control over the circumstances in which his or her speech is given."); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 876 (1996) ("Anonymity refers to the power to control whether people know who you are; it is a tool of privacy."). *But see* Lidsky & Cotter, *supra* note 143, at 1568–70 (suggesting an intrinsic rationale, deriving "internal satisfaction from not having their true identity revealed").

166. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000) (writing that a "realm of autonomous, unmonitored choice" permits experimentation "with beliefs and associations, [as well as] with every other conceivable type of taste and behavior that expresses and defines self"); Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008) (articulating a normative theory of "intellectual privacy" that protects "the ability . . . to develop ideas and beliefs away from the unwanted gaze or interference of others"); Zarsky, *supra* note 141, at 999 (noting that privacy scholars have criticized constant monitoring as an intrusion on privacy because monitoring "inhibits daily activities, promotes conformity, causes embarrassment, and interferes with the creation of intimacy"); *see also Jane: An Abortion Service*, FEMINIST WOMEN'S HEALTH CTR., http://www.fwhc.org/jane.htm (last visited Jan. 11, 2013) (describing JANE, an anonymous abortion service founded in Chicago in the late 1960s that provided "over 12,000 safe, affordable abortions" until it was disbanded after *Roe v. Wade*).

167. *See, e.g.*, Cohen, *supra* note 143, at 1010 ("The right to read anonymously . . . is predicated on the likely chilling effect that exposure of a reader's tastes would have on

Yet, "anonymity" implies much more than just private self-discovery. The most highly touted uses of anonymity—such as the Federalist papers,[168] speech by persecuted groups,[169] or whistleblowing[170]—are instances of public advocacy and civic action. The classic invocation of anonymity is as an act of public participation, not seclusion, and is usually used to convey an unpopular or controversial idea.[171] In other words, privacy focuses inward and seeks to keep the

expressive conduct, broadly understood—not only speech itself, but also the information-gathering activities that precede speech."); Zarsky, *supra* note 141, at 1038–39 ("With pseudonymity, . . . users can get a taste of different cultures and ideas, while reserving their ability to switch back to their real life unnoticed. . . . [W]hen a user grows tired of a specific virtual personality, or is unhappy with the feedback it generates, he or she can simply set it aside, and move on . . . ."); Douglas Quenqua, *Recklessly Seeking Sex on Craigslist*, N.Y. TIMES, Apr. 19, 2009, at A1 (describing the "Casual Encounters" section of Craigslist as "allow[ing] for a wide range of personal meeting and relationship options," and "an accurate inside look at how people like to connect these days"). Evidence of that boldness is sometimes put on prominent display when anonymity is unexpectedly breached. *See* Christopher Soghoian, *The Problem of Anonymous Vanity Searches*, 3 I/S J.L. & POL'Y INFO. SOC'Y 299 (2007) (describing how a murder suspect had searched for the words "neck," "snap," and "break" before allegedly killing his wife); Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1 (discussing how an AOL user was identified by her Internet searches, which included multiple queries for medical conditions ranging from "numb fingers," to "dry mouth," to "bipolar"); April Witt, *Blog Interrupted*, WASH. POST, Aug. 15, 2004, at W12 (detailing the "Washingtonienne" scandal involving an anonymous online sex diary that was outed); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) (explaining reidentification science and the flaws of anonymizing techniques); *About 33 Bits*, 33 BITS OF ENTROPY, http://33bits.org/about/ (last visited Jan. 11, 2013) (noting that with "only 6.6 billion people in the world, [we] only need 33 bits . . . of information about a person to determine who they are").

168. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 360–69 (1995) (Thomas, J., concurring) (recounting the extensive use of anonymous political expression in early American history).

169. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute a[n] effective . . . restraint on freedom of association . . . . This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.").

170. *See, e.g.*, 5 U.S.C. § 1213(h) (2006).

171. *See, e.g.*, Melissa Bell & Elizabeth Flock, *Sometimes You Want to Go Where Nobody Knows Your Name*, WASH. POST, June 19, 2011, at B3 ("Anonymity has allowed bloggers in

world "out," while anonymity focuses outward and prevents the world from keeping ideas "in." The very reason to invoke anonymity—rather than privacy—is to avoid repercussions for ideas or acts that one feels compelled to thrust into the public consciousness despite knowing that they may be unpopular.[172] Because of that reassurance, more ideas can be shared, and more people can safely signal approval or disapproval of those ideas.[173]

One school of thought holds that democratic governance is advanced whenever more people have more opportunities to participate in the process and have their say—regardless of what is actually said.[174]

---

the Middle East to safely tell the world what is happening in their countries during the Arab Spring. Anonymity allows everyone online . . . a creativity and a breadth of discussion that might not occur if a name had to be attached.").

172. *See, e.g.*, Doe v. Reed, 130 S. Ct. 2811, 2823 (2010) (Alito J., concurring) ("The widespread harassment and intimidation suffered by supporters of California's Proposition 8 provides strong support for an as-applied exemption [from disclosure of the identities of petition signers] in the present case."). *But see id.* at 2829 (Sotomayor, J., concurring) ("Disclosure of the identity of petition signers . . . in no way directly impairs the ability of anyone to speak and associate for political ends either publicly or privately.").

173. *See* Lidsky & Cotter, *supra* note 143, at 1573 ("[A]nonymity encourages contributions to the marketplace of ideas by eliminating barriers both to speaking (such as age, social status, or ethnicity) and to listening (such as fear of social censure or geographical isolation)."); Post, *Pooling Intellectual Capital*, *supra* note 146, at 143 ("By permitting individuals to communicate without fear of compromising their personal privacy and without fear of retribution, anonymity permits information to be injected into public discourse that might otherwise remain undisclosed."); Sandeen, *supra* note 145, at 541–42 ("The main benefit of anonymity, at least based upon the Supreme Court's reasoning in *Talley* and its progeny, is its potential role in promoting unfettered speech."); Horn, *supra* note 143, at 765–66 ("If an individual is forced to disclose his or her identity, he or she may be deterred from speaking. However, while the chilling effect is largely concerned with what government action will be taken in response to a particular speech, anonymity is concerned with the way the speech will be received by an audience generally, irrespective of governmental reprisal.").

174. *See* Cohen, *supra* note 143, at 1007 ("To object that comparatively few people conduct in-depth research before sharing their views on a particular topic is to miss the point."); Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 893–904 (2000) (discussing the ways in which online anonymity tests the high theory of the First Amendment); Lidsky & Cotter, *supra* note 143, at 1573–74 ("[A]nonymous speech promotes democratic self-governance . . . . The inclusion of voices in public debate that might not otherwise be heard, particularly the voices of those with less power and influence, makes public discourse and ultimately our system of government

Under that reasoning, anonymous comments are always defensible in public discourse, no matter how vile, and the best defense is to fight speech with more speech.[175] The pure expansion in ability to speak and participate is more important than judging the quality of discourse that is thereby gained.[176]

more democratic."); Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 477, 484-85 (2011) [hereinafter Post, *Participatory Democracy*] ("It is this [equal autonomy of speakers] that underwrites the First Amendment doctrine's refusal to distinguish between good and bad ideas, true or false ideas, or harmful or beneficial ideas. The equality of status of ideas within public discourse follows directly from the equality of political status of citizens who attempt to make the government responsive to their views. Outside public discourse, by contrast, the state typically distinguishes true from false ideas, as when physicians or lawyers are held liable for false or misleading opinions."); *see also* CHRIS ANDERSON, THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE 62–65 (2006) (discussing the democratization of the tools of production and noting that "[t]oday, millions of ordinary people have the tools and the role models to become amateur producers," which makes "the talented and visionary ones . . . a force to be reckoned with"). *But see Doe*, 130 S. Ct. at 2836 (Scalia, J., concurring) ("The long history of public legislating and voting contradicts plaintiffs' claim that disclosure of petition signatures having legislative effect violates the First Amendment."); CASS R. SUNSTEIN, REPUBLIC.COM 2.0, at 137 (2007) ("[A] system of limitless individual choices with respect to communications is not necessarily in the interest of citizenship and self-government."); Malcolm Gladwell, *Small Change*, NEW YORKER, Oct. 4, 2010 (criticizing social media activism as being ineffective because it is built on "weak ties").

175. *See* Ciolli, *supra* note 140, at 160–61 ("The Internet, though contributing to an increased amount of speech of lower relative value, makes 'public discourse more democratic and inclusive' and 'less subject to the control of powerful speakers' by 'eliminating structural and financial barriers to meaningful public discourse.'"); *cf.* Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("This right to receive information and ideas, regardless of their social worth, is fundamental to our free society." (citation omitted)).

176. *See* Robert C. Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 603, 626–33 (1990) [hereinafter Post, *Public Discourse*] (exploring the theoretical justification for allowing outrageous speech within public discourse, despite the inherent tensions with community norms and rules of civility); *see also* Charles Fried, *Speech in the Welfare State: The New First Amendment Jurisprudence: A Threat to Liberty*, 59 U. CHI. L. REV. 225, 233 (1992) (arguing that "[f]reedom of expression is properly based on [Kantian] autonomy," and that "[o]ur ability to deliberate, to reach conclusions about our good, and to act on those conclusions is the foundation of our status as free and rational persons").

The more mainstream view, however, holds that the purpose of public discourse is to seek "truth."[177] Under that view, anonymity is valuable because it galvanizes the vocalization of fringe views, allowing them opportunities to become accepted as truth and evolve into dogma. It is often asserted that the best path to truth is to allow speech to compete freely in the "marketplace" of ideas.[178] Anonymity can serve that function in two ways. First, in a macroeconomic sense, it can expand the size of the market by stimulating the production of additional speech that otherwise would have been chilled.[179] "Thought that is not offered cannot get itself accepted in the competition of the market."[180] That rationale can be used to justify legal protections for whistleblowers,[181] as well as extralegal operations such as Tor[182] and WikiLeaks.[183] Second, in a microeconomic sense, an individual idea can become more competitive within the existing market when identifying information is withheld, because readers are forced to judge the idea on its merits without being biased by the identity or background of the author.[184] A law student can satirize the legal in-

177. *Cf.* Elena Kagan, *Private Speech, Public Purpose: The Role of Governmental Motive in First Amendment Doctrine*, 63 U. CHI. L. REV. 413, 423–25 (1996) (summarizing two approaches to the First Amendment: "one focuse[d] on expanding the expressive opportunities open to speakers," and "another focuse[d] on improving the sphere of discourse encountered by the public 'audience'").

178. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market . . . .").

179. *See supra* note 173 and accompanying text.

180. Comment, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084, 1111–12 (1961).

181. *See* 5 U.S.C. § 1213(h) (2006) (noting that the identity of whistleblowers may not be disclosed unless "necessary because of an imminent danger to public health or safety or imminent violation of any criminal law"); Post, *Pooling Intellectual Capital*, *supra* note 146, at 143 (noting that anonymity enables "'whistleblower' information that may help uncover the existence of illegal activity" to enter the public discourse and that without the protections of anonymity, the information may not be made public) .

182. *See* Eric J. Stieglitz, Note, *Anonymity on the Internet: How Does It Work, Who Needs It, and What Are Its Policy Implications?*, 24 CARDOZO ARTS & ENT. L.J. 1395, 1402–03 (2007).

183. *See generally* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311 (2011).

184. *See* Froomkin, *Flood Control*, *supra* note 145, at 409 ("Communications that give no hint of the age, sex, race, or national origin of the writer must be judged solely on their

dustry by masquerading as a world-weary law firm partner;[185] a political campaign can covertly distribute "viral" videos that undermine opposing candidates without having it be discounted as propaganda.[186]

To be sure, many scholars have rightly questioned the authenticity of the "truth" delivered by anonymity.[187] They suggest that information is often more reliable when the speaker's identity and credibility are verifiable,[188] and that anonymity has been used to spread

content as there is literally nothing else to go by. This makes bigotry and stereotyping very difficult, and also should tend to encourage discussions that concentrate on the merits of the speech rather than the presumed qualities of the speakers."); Lidsky & Cotter, *supra* note 143, at 1577 (stating that, in some cases, withholding the speaker's identity "may protect the public against underestimating the truth-value of the statement"); Post, *Public Discourse*, *supra* note 176, at 640 n.213 (describing the principle that withholding the identity of an author can allow "impartial evaluation" of the contents of the author's speech rather than a reflection of the author's status).

185. *See* Sara Rimer, *Revealing the Soul of a Soulless Lawyer*, N.Y. TIMES, Dec. 26, 2004, (telling the behind-the-scenes story of the blog "Anonymous Lawyer").

186. *See* Daniel Kreiss, *Acting in the Public Sphere: The 2008 Obama Campaign's Strategic Use of New Media to Shape Narratives of the Presidential Race*, 33 RES. SOC. MOVEMENTS CONFLICTS & CHANGE 195, 210–11 (2012) (describing the use of such tactics by the 2008 Obama campaign).

187. *See* Lidsky & Cotter, *supra* note 143, at 1581–89 ("[I]f truth . . . is to emerge from the marketplace of ideas, the consumers of ideas must be capable of exercising their critical faculties to separate the wheat from the chaff . . . ."); Helen Norton, *Secrets, Lies, and Disclosure*, 27 J.L. & POLITICS 641, 644-46 (2012) (noting the distinction between "a speaker's interest in keeping her identity secret because she is vulnerable to abuse by power from a speaker's interest in keeping her identity secret to better wield her own power to shape others' choices"); Post, *Participatory Democracy*, *supra* note 174, at 487 ("The purpose of fostering a marketplace of ideas is an implausible goal of First Amendment doctrine because new knowledge cannot be created without the concomitant power to judge ideas as true or false, as better or worse."); Comment, *supra* note 180, at 1116 ("The assertion that free discussion will lead to truth is unverifiable. In order to judge whether progress toward truth has been made it is necessary to know what is true."). That said, facts (as opposed to ideas) can be self-verifying. *See, e.g.*, Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1120–21 (2005) ("If we know that hundreds of security experts from many institutions have been able to discuss potential problems in some security system, that journalists are free to follow and report on these debates, and that the experts and the press seem confident that no serious problems have been found, then we can be relatively confident that the system is sound.").

188. *See* Froomkin, *Flood Control*, *supra* note 145, at 402–03 (summarizing arguments by other scholars that anonymity is inefficient because it makes it more difficult to identify

false information about everything from financial stocks[189] to dating relationships.[190] Yet, perhaps the salient point here is "truthiness," not "truth." When anonymity spurs changes in public opinion, the strength of conviction in those changes may matter more than actual validity.[191]

---

self-interest or bias and shifts the costs of that information acquisition onto those who are not the least-cost avoiders); Lidsky & Cotter, *supra* note 143, at 1559–63 ("Anonymous speech persists despite the fact that it is, on average, *less* valuable than nonanonymous speech to speech consumers (audiences) who often use speaker identity as an indication of a work's likely truthfulness, artistic value, or intellectual merit. Without attribution, audiences must necessarily rely upon other indicia, which can be less reliable than speaker identity."); Comment, *supra* note 180, at 1111 ("Anonymous propaganda makes it more difficult to identify the self interest or bias underlying an argument or the qualifications of its exponent. . . . It is therefore argued that exposure of the source of propaganda will advance the search for truth by permitting a more critical evaluation of facts, figures, and arguments presented."); *see also* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1049 (1994) (discounting the harmful effect of anonymous defamation on the grounds that "anonymous remarks will be greatly devalued precisely because they are anonymous and easy to make").

189. *See, e.g.*, Michael Lewis, *Jonathan Lebed's Extracurricular Activities*, N.Y. TIMES MAG., Feb. 25, 2001 (reporting on the story of Jonathan Lebed, a teenager from New Jersey, who was "the first minor ever to face proceedings for stock-market fraud" after he anonymously "posted hundreds of messages on Yahoo Finance message boards recommending . . . stock to others").

190. *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1120–22 (9th Cir. 2003) (concluding that a computer match-making service was immune from liability under section 230 of the CDA "for false content in a dating profile provided by someone posing as another person"); Lizette Alvarez, *(Name Here) Is a Liar and a Cheat*, N.Y. TIMES, Feb. 16, 2006, at G1 (highlighting various dating websites such as DontDateHimGirl.com and TrueDater.com that allow women to write anonymous, unverified stories identifying men they dated); *see also* Nadya Labi, *An IM Infatuation Turned to Romance. Then the Truth Came Out*, WIRED, Aug. 21, 2007 (recounting the story of a middle-aged man who created a fake online dating profile and, after becoming involved with a middle-aged woman posing as her eighteen-year-old daughter, allegedly murdered another man with whom the woman was also having an online relationship).

191. *See* Comment, *supra* note 180, at 1123 (arguing that anonymity should be promoted to "bring about a general climate in which modification [of beliefs] is most likely to be encouraged"); Suzanna Sherry, *Democracy and the Death of Knowledge*, 75 U. CIN. L. REV. 1053, 1056–69 (2007) (observing that "democratization of knowledge" can lead to the "death of knowledge"); *see also* JARON LANIER, YOU ARE NOT A GADGET: A MANIFESTO 48–50, 55–64, 122–23 (2010) (criticizing the "wisdom of crowds" and the "disdain for the idea

B. Horse Trading for Generativity

Zittrain's theory of generativity unfolds along much the same trajectory. Zittrain defines generativity as consisting of five factors:

> (1) how extensively a system or technology leverages a set of possible tasks;
> (2) how well it can be adapted to a range of tasks;
> (3) how easily new contributors can master it;
> (4) how accessible it is to those ready and able to build on it; and
> (5) how transferable any changes are to others—including (and perhaps especially) nonexperts.[192]

In other words, a system is generative when it allows individuals to repurpose its functionality toward new uses, and then share those innovations with others.

Those five features map loosely onto the attributes of anonymity. Anonymity incubates ideas that deviate from standard norms (privacy), expands the pool of individuals able to articulate those ideas in public (participation), and assists those ideas in achieving widespread adoption (truth). Similarly, generativity allows deviations from intended uses (leverage, adaptability), empowers more users to perform that tinkering (accessibility, ease of use), and facilitates easy distribution of new uses to new users (transferability). A reduction in any of those attributes stunts the system's potential to generate progress through disruptive churn.[193]

Like anonymity, generativity increases entropy by championing a bottom-up model of development, in which many ideas can be pursued independently, over a top-down model, in which a few gatekeepers control all the cards.[194] Zittrain offers two supporting narratives:

---

of quality within the culture of web 2.0 enthusiasts," and arguing that "quantity can overwhelm quality in human expression"); Rebecca Wexler, *Integrity vs. Authenticity in Video Journalism*, CPJ JOURNALIST SEC. BLOG (Dec. 13, 2012, 2:20 PM), https://www.cpj.org/security/2012/12/integrity-vs-authenticity-in-video-journalism.php (describing heated controversy over the authenticity of a video allegedly showing Sri Lankan soldiers executing Tamil Tiger rebels).

192. ZITTRAIN, *supra* note 1, at 71.

193. *See id.* at 96 ("Generative technologies need not produce forward progress, if by progress one means something like increasing social welfare. Rather, they foment change.").

194. *See id.* at 93 ("In hierarchies, gatekeepers control the allocation of attention and resources to an idea. In polyarchies, many ideas can be pursued independently."); *cf.* Jon-

innovation and participation. The innovation rationale is that by allowing amateurs to solve their own idiosyncratic needs, generative systems fill a crucial gap that otherwise would go unfulfilled by the "firm-mediated market model."[195] Generativity does not replace the top-down model of research and development, but serves as a supplementary source of do-it-yourself invention.[196] Likewise, the participation rationale is that generative systems provide citizens with more opportunities to participate actively in the creation of "cultural meaning," rather than be "passive consumers" of culture produced by others.[197] Again, the point is not to replace the content created by mainstream media, but instead to add more citizen-produced content.[198]

That latitude also means generativity represents an immunity from regulation very nearly like that which is provided by anonymity. "[S]o long as the *endpoints* [of a network] remain generative," Zittrain writes, "subversively minded techies can make applications that offer a way around network blocks."[199]

Curiously, after developing that story of unruliness, Zittrain downplays it and turns instead to building the argument that generativity promotes better security.[200] Perhaps he sees that strategy as the best hope of persuading security-minded regulators to leave generativity alone.[201] But that vision—that generativity can simultaneously ad-

athan Zittrain, *The Fourth Quadrant*, 78 FORDHAM L. REV. 2767, 2768 (2010) [hereinafter Zittrain, *The Fourth Quadrant*] ("The term 'hierarchy' . . . connotes a system for which there is no alternative, either because it does not exist, because it would be too costly, or because law precludes it. . . . Polyarchy is defined by choice. . . . [C]hoice is the ability to choose among various regimes or systems in which you might exist.").

195. ZITTRAIN, *supra* note 1, at 80–90 ("Generativity-enabled activity by amateurs can lead to results that would not have been produced in a firm-mediated market model.").

196. *Id.* at 86–90.

197. *Id.* at 90–94.

198. *See id.* at 93 (explaining that "more people [can] have a hand at contributing to the system, regardless of the quality of the contribution").

199. *Id.* at 105–06.

200. *See id.* at 125–48 (explaining how "some enterprises that are generative at the content level have managed to remain productive without requiring extensive lockdown or external regulation" and arguing that "those lessons [can be applied] to the future of the Internet").

201. *Cf.* Grimmelmann & Ohm, *supra* note 7, at 931–32 ("[Zittrain] actually recommends very little in the way of legal intervention. . . . The very spirit of verkeersbordvrij

vance liberty and security—is an illusion that depends on the proverbial "bad man" being won over by the goodness of humanity.[202] The gist of Zittrain's argument is not that generativity improves enforcement, but instead the familiar libertarian hope that the elimination of odious rules will obviate the need for intentional rule-breaking—and thus the need for any enforcement at all.[203] The catch, however, is that no matter how reasonable a rule may seem to the larger community, rational minds can differ, and generativity qua liberty allows any single "subversively minded techie" to collapse the illusion of security.

Zittrain's anecdotal examples of communitarian success—a Dutch town's experiment to improve traffic safety by removing all traffic signs[204] and Wikipedia, a free online encyclopedia that allows any visitor to edit its articles[205]—are easily distinguished and refuted. In the Dutch example, the town was small enough that the preexisting harm from potential accidents was minimal, and never malicious, such that installing a roundabout was enough to nudge driver behavior and reduce accidents.[206] As for Wikipedia, the communitari-

[Dutch for "free of traffic signs"], it might seem, precludes more ambitious regulatory interventions.").

202. David Post hints at that over-optimism, characterizing Zittrain's agenda as a "decidedly eighteenth-century program" that seeks to construct a society having "civic virtue." Post, *The Theory of Generativity*, *supra* note 7, at 2764.

203. ZITTRAIN, *supra* note 1, at 128 ("When we face heavy regulation, we see and shape our behavior more in relation to reward and punishment by an arbitrary external authority, than because of a commitment to the kind of world our actions can help bring about."); *cf.* Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J.L. & COM. 509, 511 (1996) ("Early cyberspace—by which I mean the Internet as it functioned before the mass influx of new users and commercial hopefuls—was closer to the world the critics of intellectual property would like to see. . . . Cooperative creation was prevalent, and a collective creativity was recognized and celebrated.").

204. ZITTRAIN, *supra* note 1, at 127–30.

205. *Id.* at 131–48.

206. Zittrain highlights the success of a traffic experiment conducted by the Dutch town of Drachten that improved safety by counterintuitively removing nearly all road signs. *Id.* at 127. Prior to the experiment, however, that town had been experiencing an average of only nine accidents a year, none of which had been fatal. NOORDELIJKE HOGESCHOOL LEEUWARDEN, THE LAWEIPLEIN: EVALUATION OF THE RECONSTRUCTION INTO A SQUARE WITH ROUNDABOUT 5, 26–27 (2007), *available at* http://www.fietsberaad.nl/library/repository/bestanden/Evaluation%20Laweiplein.pdf (noting eighty-three accidents between 1994 and 2002). Drachten did not rely simply on good will; it also converted the Laweiplein intersection into a roundabout, a traffic structure that functions inherently well

an aspects have survived only because an authoritarian bureaucracy has been installed to impose order as needed.[207]

Many other examples exist in which group norms fail to check generative mischief. Splintering can be expected within any large, dispersed community that has enough generative ability to go around. In networked multiplayer games, easily installed cheats allow an individual player to enjoy temporary dominance over others—a selfish thrill that persists despite strong indignation from other players.[208] Inevitably, the remedies involve a combination of efforts by game designers to disable such exploits, and the use of identifiers so that cheaters can be censured or permanently banned.[209] Likewise, it was unsurprising when LulzSec broke off from the larger hacker group Anonymous.[210] The members of LulzSec became interested in gaining publicity by committing more conspicuous "ops," and they were successful in doing so despite efforts by other members of Anony-

without signs. *Id.* at 5; *see also* FED. HIGHWAY ADMIN., DEP'T TRANSP., ROUNDABOUTS 4 (2010) ("Numerous studies have shown significant safety improvements at intersections converted from conventional forms to roundabouts."); *cf.* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008) (describing the powerful influence of default settings on human behavior).

207. *See* Kahn, *supra* note 111, at 199–201 (describing Wikipedia's governance as "not purely bottom-up," because "a handful of [appointed] 'bureaucrats' . . . possess authority above all other users"); *see also* Daniel Kreiss, Megan Finn & Fred Turner, *The Limits of Peer Production: Some Reminders from Max Weber for the Network Society*, 13 NEW MEDIA & SOC'Y 243, 243–245, 255 (2011) (advocating the virtues of bureaucratic governance within systems of peer production).

208. *See* Steven Daniel Webb & Seiteng Soh, *Cheating in Networked Games—A Review* 105–12 (Proceedings of the 2nd International Conference on Digital Interactive Media in Entertainment and Arts, Sept. 19–21, 2007) *available at* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.83.9005 (highlighting the various methods of cheating in networked games and arguing that such actions "degrade[] the experience" for other players).

209. *See, e.g.*, *id.* at 110–11 (describing "protocols [that] have been proposed to prevent cheating"); Joel Zetterström, A Legal Analysis of Cheating in Online Multiplayer Games 71 (Mar. 2005) (unpublished LL.M. thesis, Göteborg University), *available at* https://gupea.ub.gu.se/bitstream/2077/1948/1/200528.pdf ("Anti-cheating efforts focus on eliminating that anonymity, so that caught cheaters can be identified and banned.").

210. For background information on Anonymous, see generally STRYKER, *supra* note 128, at 35–70; Quinn Norton, *Anonymous 101: Introduction to the Lulz*, WIRED (Nov. 8, 2011, 5:30 AM), http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1.

mous to dissuade and shame them.[211] Ultimately, LulzSec's attacks were stopped not because of loyalty to the community's ideals and norms, but because the members were exposed and caught.[212]

More problematically, by claiming that generativity can *increase* security, Zittrain avoids having to grapple with the dilemma of how to choose regulations that do the least harm to generativity. Instead, his main policy recommendation is to *increase* generativity on the rationale that security is best improved when restrictions come from the community, bottom up, rather than from authoritarian leaders, top down.[213] Zittrain argues that generativity equips communities with better tools and capabilities to build walls and other mechanisms to self-police their collective norms.[214] Yet those tools and capabilities al-

211. *See* Ravi Somaiya & Steve Lohr, *British Police Charge Teenager in Connection With Hacking Attacks*, N.Y. TIMES, June 24, 2011, at B1 ("The two hacker groups [Anonymous and a splinter group, LulzSec] certainly strike different poses. LulzSec's statements and its actions display a spirit of exuberant anarchic glee. Lulz, in essence, means mean-spirited laughter . . . . There seems to be far less glee in the Anonymous culture. In a YouTube video describing the group, a voice intones . . . that Anonymous's actions have 'brought justice to our world.'"); Eric Mack, *Hacker Civil War Heats Up*, PCWORLD (June 24, 2011, 7:13 AM), http://www.pcworld.com/article/231078/hacker_civil_war_heats_up.html (discussing the ongoing battle between hacker groups, particularly the "emerging hacker insurgency" against LulzSec, which "could be motivated by a sincere sense of retribution–to teach Lulzsec a lesson for 'going too far'"); *see also* Kim Zetter, *Researchers: Anonymous and LulzSec Need to Focus Their Chaos*, WIRED (Aug. 6, 2011, 10:44 PM), http://www.wired.com/threatlevel/2011/08/defcon-anonymous-panel/ (reporting on the views of computer security experts that "[t]he loosely affiliated groups" of "Anonymous and LulzSec are weakening their cause with scattershot attacks and need to get more intelligent and focused" because they do "not hav[e] real goals [other than] simply wanting 'to smash things'").

212. *See* Somini Sengupta, *Arrests Sow Mistrust Inside a Clan of Hackers*, N.Y. TIMES, Mar. 7, 2012, at A1.

213. *See* ZITTRAIN, *supra* note 1, at 150–52 (suggesting that saving the generative spirit of the Internet will require finding ways to encourage more generative participation at the technical layers, as has been done at the social layer, to tap the power of groups to distinguish good code from bad code).

214. *Id.* at 129 ("When people can come to take the welfare of one another seriously and possess the tools to readily assist and limit each other, even the most precise and well-enforced rule from a traditional public source may be less effective than that uncompelled goodwill."); *see also* Zittrain, *The Fourth Quadrant*, *supra* note 194, at 2770, 2777–81 (suggesting that communitarian concepts, which are "supposed to embody participation in a much richer way," provide the solution for managing cyber-security regulation because they

so allow subversive elements to build the same walls and mechanisms to evade a community's policing efforts. At bottom, Zittrain's proposal is an endorsement of self-regulation and vigilantism all around. It is not a principle for selecting generative compromise.

C. Tethered Generativity and Anonymous Appliancization

Zittrain's predicament is illustrated by his critique of "tethered appliancization."[215] He observes that devices like digital video recorders ("DVRs") and cellphones are "tethered," because they can be monitored from afar by a controlling interest, while devices like refrigerators and televisions are "appliances," because they are locked down and closed to user modifications.[216] Combining the terms, he refers to "tethered appliancization" as the capacity to lock down devices from afar via remote command, allowing dangerous or subversive uses to be disabled long after the point of sale. Zittrain acknowledges that the feature is attractive to many sellers and consumers because it offers reliability and safety. Yet, he also worries that the trend toward tethered appliancization is anti-generative because it makes enforcement too easy, permitting regulators to stifle experimental uses before those uses have a chance to prove their worth.[217] When enforcement is costly, regulators are forced to tolerate activities that are technically illegal but below a certain threshold of priority.[218] That leniency "allow[s] for experimentation of all sorts and later rein-

---

"draw directly upon . . . those who operate in good faith, to try to make the Internet a better place").

215. ZITTRAIN, *supra* note 1, at 103.

216. *Id.* at 106 ("Tethered appliances . . . are *appliances* in that they are easy to use, while not easy to tinker with [and] are *tethered* because it is easy for their vendors to change them from afar, long after the devices have left warehouses and showrooms.").

217. *Id.* at 103 ("With tethered appliances, the dangers of excess come . . . from the much more predictable interventions by regulators into the devices themselves, and in turn into the ways that people can use the appliances."); *id.* at 112 ("Challenging the rise of tethered appliances helps maintain certain costs on the exercise of government power—costs that reduce the enforcement of objectionable laws."); *see also id.* at 118 ("The rise of tethered appliances significantly reduces the number and variety of people and institutions required to apply the state's power on a mass scale. It removes a practical check on the use of that power.").

218. *Id.* at 119 & n.84 (citing Tim Wu, *Does YouTube Really Have Legal Problems?*, SLATE (Oct. 26, 2006, 4:28 PM), http://www.slate.com/id/2152264) (describing the concept of "tolerated uses").

ing in [of] excesses and abuses as they happen, rather than preventing them from the outset."[219] But as regulatory costs approach zero, regulators can achieve "perfect enforcement," thereby eliminating the latitude to dissent and decide for oneself whether an activity is truly harmful.[220]

The trouble with Zittrain's critique of tethered appliancization is that it does not grapple with the middle ground between self enforcement and perfect enforcement. Perfect enforcement is a legitimate concern anytime there is a centralized system of detection and prevention; but Zittrain's response is to fight the centralized enforcement model itself. He does not offer guiding principles for how regulators might create barriers or stickiness so that a rule can be enforced with appropriate moderation.

One helpful move is to distinguish tethering from appliancization. Tethering can be understood mainly as a detection mechanism, i.e., an anonymity restriction. The actual generative loss is inflicted by appliancization, which describes any modifications done to the device (before or after manufacture) to prevent future violative uses. As James Grimmelmann and Paul Ohm have astutely observed, "tethering and appliancization sometimes flow from common pressures, [but] one can exist without the other."[221] Thus, a proper critique of tethered appliances should include consideration of the interplay between anonymity and generativity. For example, if tethering is less harmful to generative potential than appliancization is, then we can envision more palatable regulatory combinations in which tethering is

219. *Id.* The argument in favor of such leniency draws its strength from the distinction between malum prohibitum and malum in se, the notion that prohibition by law does not make an act inherently immoral or evil. *See* Zittrain, *Online Gatekeeping*, *supra* note 117, at 254–55.

220. ZITTRAIN, *supra* note 1, at 122 ("Perfect enforcement collapses the public understanding of the law with its application, eliminating a useful interface between the law's terms and its application. Part of what makes us human are the choices that we make every day about what counts as right and wrong, and whether to give in to temptations that we believe to be wrong."); *see generally* Christina M. Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH. J.L. & TECH. 13 (2008) (discussing the concerns of perfect enforcement raised by the use of technology to enforce law, including perfect prevention, perfect surveillance, and perfect correction).

221. *See* Grimmelmann & Ohm, *supra* note 7, at 938 ("Even with its auto-update tether, the PC is still profoundly more generative than the fully appliancized GPS unit. And yet, we suspect that Zittrain loses more sleep over the tethered PC than over appliancized GPS units.").

paired with traditional legal remedies rather than with appliancization remedies.

Of the two, appliancization is more troubling because it acts as a true prior restraint.[222] Targeting the technology in lieu of the individual makes regulation too facile—not in the quantitative sense that too many violations are prevented or corrected, but in the qualitative sense that it avoids the discomfort of having to grapple individually with each case.[223] Consider the example of speeding. If a city relies on technological means to artificially cap the maximum speed of cars driving within a designated zone, then that rule is absolute and cannot be violated even for good cause. By contrast, remedies that act directly on the individual, such as imposing a fine or revoking a driver's license, must survive repeated scrutiny because they can be contested and evaluated each time they are applied.[224] Recurrent review has uncovered societal unease even in areas as seemingly settled as narcotics,[225] child pornography,[226] and death penalty sentencing.[227] Appliancization short-circuits that iterative process.[228]

222. Law-based "prior restraints" can be breached as long as one is willing to assume the risk of penalty, whereas technology-based restraints can be breached only if one has the ability and expertise to circumvent them. *Cf.* Steven Alan Childress, *The Empty Concept of Self-Censorship*, 70 TUL. L. REV. 1969, 1972–73 (1996) (arguing that "the entire distinction between prior restraint and ex post facto punishment is a false one . . . because most systems identified as prior restraints actually achieve that goal merely by imposing costs on those who avoid the administrative scheme or fail to get a license").

223. *Cf.* Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601, 1613, 1627–28 (1986) (arguing that awareness and consideration of death and pain must remain central to legal interpretation).

224. *See, e.g.*, Mulligan, *supra* note 220, ¶¶ 14–15 (describing opposition to a Hawaiian initiative in 2000 to use cameras to ticket everyone driving six or more miles over the speed limit). Similarly, opposition to the national speed limit led to its repeal in 1995. National Highway System Designation Act of 1995, Pub. L. No. 104-59, § 205(d), 109 Stat. 568, 577.

225. The federal sentencing guidelines for cocaine-related offenses were amended in 2010 to reduce the 100-to-1 disparity in crack cocaine sentencing compared with powder cocaine sentencing. Fair Sentencing Act of 2010, Pub. L. No. 111-220, § 2, 124 Stat. 2372; *see also* U.S. SENTENCING GUIDELINES MANUAL, Supp. App. C amend. 706 (2007), *available at* http://www.ussc.gov/Guidelines/2007_guidelines/Manual/appc2007.pdf. Much of the evolving resistance to various sentencing guidelines may stem from common reservations regarding the wisdom of mandatory minimum sentencing laws. *See* Erik Luna & Paul G. Cassell, *Mandatory Minimalism*, 32 CARDOZO L. REV. 1, 15 (2010) (comparing mandatory minimum sentences to a "tariff" on the least culpable criminals).

That is not to say that every instance of appliancization is problematic, provided that it is not being used to bypass due process considerations. A court may prohibit a specific individual from using computers or accessing the Internet if it determines that the individual's use of such technologies poses an unreasonable risk to public safety.[229] Nor should we be disturbed by cases like *TiVo, Inc. v. EchoStar Communications Corp.*,[230] the leading example selected by Zittrain to demonstrate the problems of appliancization.[231] There, EchoStar's DVR devices were found to have infringed TiVo's patents, and Zittrain's concern was that the district court had ordered EchoStar to remotely deactivate infringing devices that were still in the physical

226. Criminal sentences for possession of child pornography is another example where we have seen resistance develop over time, as judges have had to grapple repeatedly with the severity of the penalty. *See* A.G. Sulzberger, *Defiant Judge Takes on Child Pornography Law*, N.Y. TIMES, May 21, 2010, at A1 (describing how judges around the country have begun to criticize amendments to sentencing guidelines that nearly quadrupled the average prison sentence for individuals convicted of possessing child pornography); *see also* Arlen Specter & Linda Dale Hoffa, *A Quiet but Growing Judicial Rebellion Against Harsh Sentences for Child Pornography Offenses—Should the Laws Be Changed?*, CHAMPION, Oct. 2011, at 12 (observing that a 2010 survey of federal judges found that "70 percent of respondents said the possession ranges were too high, 69 percent said the same for receipt, and 30 percent said the ranges for distribution were excessive").

227. *See, e.g.*, William Yardley, *Oregon Governor Says He Will Not Allow Executions*, N.Y. TIMES, Nov. 23, 2011, at A14 (noting that only thirty-four states currently allow the death penalty and that only twenty-seven have performed executions in the past decade); *see also* Callins v. Collins, 510 U.S. 1141, 1145 (1994) (Blackmun, J., dissenting) (declaring, famously, that "[f]rom this day forward, I no longer shall tinker with the machinery of death").

228. *See* Mulligan, *supra* note 220, at ¶ 102 ("The ability of individuals to disobey or refuse to enforce laws can provide lawmakers with the pressure and incentive to re-evaluate the wisdom of laws.").

229. *See* United States v. Love, 593 F.3d 1, 12 (D.C. Cir. 2010) ("Consensus is emerging among our sister circuits that Internet bans, while perhaps unreasonably broad for defendants who possess or distribute child pornography, may be appropriate for those who use the Internet to 'initiate or facilitate the victimization of children.'" (citations omitted)).

230. 446 F. Supp. 2d 664 (E.D. Tex. 2006), *aff'd in part, rev'd in part*, 516 F.3d 1290 (Fed. Cir. 2008).

231. *See* ZITTRAIN, *supra* note 1, at 103–04.

possession of customers.[232] But the result was no different than if the district court had ordered EchoStar to cease broadcasting to those devices. The only offender in question, EchoStar, was fully represented in court. The injunction did not address any customers individually or direct them to destroy or surrender their devices; nor did it prohibit customers from obtaining DVR service elsewhere.[233] The conflict in *TiVo* was between horizontal competitors over a known and intended use, not between vertical entities threatening newly generative uses.[234]

It is easy to point to tethering as the culprit that facilitates appliancization. After all, a controlling interest with direct access to a device can simply compel the results it wants on its own terms.[235] We have seen Amazon spontaneously delete electronic copies of books from subscribers' Kindles,[236] while Apple regularly reprograms its devices in order to thwart efforts to "jailbreak" them, even when jailbreaking is not illegal.[237] That power is not limited to proprietary hardware. Sony BMG used "rootkit" software to disable customers' computers from copying its CDs,[238] and the creators of the Stuxnet

232. *See TiVo*, 466 F. Supp. 2d. at 669–70 ("Defendants do not dispute that, with software updates transmitted directly to the infringing products, the DVR capabilities of the infringing products can be disabled.").

233. *Id.* at 670 (stating that one reason for granting the injunction is that DVR customers are "sticky customers," and that continued infringement would lead to long-term loss of market share).

234. *Id.* ("The hardship of disabling DVR capabilities to Defendants' DVR customers is a consequence of Defendants' infringement and does not weigh against an injunction.").

235. *See* ZITTRAIN, *supra* note 1, 107–10 (discussing the ways in which "[t]hose who control the tethered appliance can control the behavior undertaken with the device," including reprogramming a device "*after* it is in consumer hands, to reflect changed circumstances").

236. Brad Stone, *Amazon Erases Two Classics from Kindle. (One Is '1984.')*, N.Y. TIMES, July 18, 2009, at B1.

237. Jailbreaking is a process by which an iPhone user can access hidden functionality that Apple has purposefully deactivated. *See* Jenna Wortham, *In Ruling on iPhones, Apple Loses a Bit of Its Grip*, N.Y. TIMES, July 27, 2010, at B3 (noting that the Library of Congress determined that an exception to the DMCA allowing for "the so-called jailbreaking of iPhones and other devices" was legally permissible); Dan Goodin, *Apple Eyes Kill Switch for Jailbroken iPhones*, REGISTER (Aug. 20, 2010, 10:38 PM), http://www.theregister.co.uk/2010/08/20/apple_jailbreak_patent/ (discussing Apple's attempts to prevent jailbreaking).

238. *See* Bruce Schneier, *Real Story of the Rogue Rootkit*, WIRED (Nov. 17, 2005), htpp://wired.com/politics/securitymatters/2005/11/69601?currentPage=all.

worm were able to seize hostile control of centrifuges at a key nuclear facility in Iran.[239] In each of those cases, however, the objection is to the specific use of appliancization, not to the general fact of tethering.

Attempting to preserve generativity by severing connections with the networked environment is itself weirdly anti-generative. In fact, tethering can promote generativity by encouraging under-polished "beta" products to be released early with the understanding that final touches can be added later. That is the model by which open source software development has always operated, with the expectation that early developmental releases will be replaced regularly by newer, more stable releases.[240] Tethering is also vital to applications like search engines and GPS devices, which depend on information sets that are regularly updated with new data. More generally, cloud computing operates by providing devices at the ends of the network with continuous access to data and services in the middle of the network.[241] While cloud computing still faces important challenges, it is an extraordinarily innovative step made possible because of tethering, not in spite of it.

Even if we were to set aside the affirmative benefits of tethering, however, there is another reason to endorse it. Tethering provides a means of identification; without it, regulation would be conducted instead through restrictions on functionality and access.

To take an offline example, 9/11 created an enormous desire to protect airplanes from being used in another terrorist attack. Yet, the inability to easily identify terrorists has resulted in overbroad restrictions on ordinary items permitted through security checkpoints—liquids, scissors, aerosols, sporting equipment, snowglobes, and more.[242] Those restrictions have been rightly called "security thea-

239. *See* David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (discussing how President Obama authorized secret attacks on the computer systems that controlled Iran's nuclear processing facilities); *see also* Gross, *supra* note 99.

240. *See* ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY 28–33 (2000) (describing why "[e]arly and frequent releases are a critical part of the Linux development model").

241. *See generally* Michael Armbrust et al., *A View of Cloud Computing*, 53 COMM. ACM 50, 50–55 (2010).

242. *See Prohibited Items*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/traveler-information/prohibited-items (last updated Feb. 12, 2013). Those restrictions were re-

ter,"[243] but they can also be viewed as the natural outgrowth of attempting to achieve a desired regulatory outcome in the absence of a good identification system.

A similar story can be told about border control. The inability to easily distinguish illegal immigrants from legal residents has led to efforts to restrict free movement across borders using checkpoints, fences, patrols, and citizen-manned surveillance cameras.[244] Efforts to create better identification schemes have been protested as violations of civil liberties,[245] yet we should at least be cognizant that enforce-

---

cently relaxed to allow pocketknives, golf clubs, and other sports items. Jad Mouawad, *U.S. Relaxes Air Travel Carry-On Prohibitions*, N.Y. TIMES, Mar. 6, 2013, at B3.

243. *See, e.g.*, Candice L. Kline, Comment, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 443, 443 (2008) ("The government's pursuit of 'Security Theater' following September 11, 2001 ('9/11') leverages anti-terrorism techniques that appear 'high tech' and effective, but in reality are highly flawed."); Jeffrey Goldberg, *The Things He Carried*, ATLANTIC, Nov. 2008, *available at* http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/ ("Airport security in America is a sham—'security theater' designed to make travelers feel better and catch stupid terrorists. Smart ones can get through security with fake boarding passes and all manner of prohibited items—as our correspondent did with ease.").

244. *See, e.g.*, Julia Preston, *Some Cheer Border Fence as Others Ponder the Cost*, N.Y. TIMES, Oct. 20, 2011, at A17 (reporting on proposals to expand the border fence that has been built along 650 miles of the border between the United States and Mexico); John Burnett, *A New Way to Patrol the Texas Border: Virtually*, NPR (Feb. 23, 2009, 12:56 PM), http://www.npr.org/templates/story/story.php?storyId=101050132 (stating that over 43,000 people have become "virtual Texas deputies" by logging on to www.blueservo.net and monitoring border cameras). *But see* Arizona v. United States, 132 S. Ct. 2492, 2507–10 (2012) (lifting the injunction on a provision of an Arizona statute that authorizes state officers to determine the immigration status of any person they stop, detain, or arrest).

245. *See, e.g.*, Crawford v. Marion Cnty. Election Bd., 553 U.S. 181, 185–89 (2008) (plurality opinion) (rejecting a facial challenge to an Indiana statute requiring photo identification to vote on election day); Randal C. Archibold, *Arizona Enacts Stringent Law on Immigration*, N.Y. TIMES, Apr. 24, 2010, at A1 (noting President Obama's opposition to an Arizona immigration law that would criminalize the failure to carry immigration documents and give police the power to detain an individual suspected of being in the country illegally); Kim Zetter, *No Real Debate for Real ID*, WIRED (May 10, 2005), http://www.wired.com/politics/security/news/2005/05/67471 (noting that hundreds of civil liberties groups oppose the Real ID Act, a piece of federal legislation that would establish a national identification card).

ment efforts are not being abandoned but are being shifted elsewhere.

The substitution effect also extends to software. Because each copy of a software program is identical, any differentiation must be determined on the basis of extrinsic factors. When that differentiation can be performed by "calling home"—i.e., through a tethering mechanism—then verification is straightforward.[246] Each customer can be issued a unique identifier, such as a username or license key, and any unauthorized use of that identifier can be readily investigated and remedied.[247] Some spoofing and identity theft may occur, as it does offline, but the problem is relatively contained, as it is offline. On the other hand, when the software cannot rely on an external verification system, we can expect to see a corresponding push to develop mechanisms to lock functionality, since each copy of the software must fend for itself. Microsoft Windows, for example, generates a special hash code based on the specific hardware configuration of the computer, and it automatically disables itself if it detects that the underlying hardware has changed—even if that switch was made by the rightful owner.[248] Other software programs have been designed to be inoperable unless a physical object such as a CD-ROM or USB dongle is inserted into the computer.[249] The dongle solution provides better portability but is subject to loss or theft.

---

246. *Cf.* ZITTRAIN, *supra* note 1, at 101 (identifying "mobile phones, video game consoles, TiVos, iPods, and Blackberries" as tethered information appliances because they "assure[] users that functionality and security improvements can be made as new problems are found").

247. *See, e.g.*, Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 597 (E.D. Pa. 2007) (describing a dispute in which the plaintiff signed up for and paid to participate in a multiplayer role-playing game and the game administrators froze his account after he allegedly cheated); Joshua A.T. Fairfield, *The God Paradox*, 89 B.U. L. REV. 1017, 1023 (2009) (observing that the companies that run virtual worlds can exercise technological control to suspend or ban players).

248. *See Technical Details on Microsoft Product Activation for Windows XP*, MICROSOFT TECHNET, http://technet.microsoft.com/en-us/library/bb457054.aspx (last updated Aug. 13, 2001) (outlining Microsoft's development of product activation to help reduce software piracy).

249. *See, e.g.*, Noah J. Wald, Note, *Don't Circumvent My Dongle! Misinterpretation of the Digital Millennium Copyright Act Threatens Digital Security Technology*, 33 T. JEFFERSON L. REV. 325, 328–30 (2011) ("A dongle acts like a tangible key to a digital lock. . . . High-end software purchases often include a dongle. Use of the software will require that the dongle plug

With the Internet, a choice to favor appliancization over tethering would be especially puzzling because it fights against the natural orientation of the system. On one hand, the Internet lends itself to always-on connectivity, especially as bandwidth improves and costs diminish.[250] Assigning unique identifiers to computing devices, and ensuring that those identifiers remain reasonably fixed over time, would be trivial as a technological matter. By contrast, the network protocols were designed to guarantee robust connectivity between any two arbitrary peer nodes.[251] As a result, it is difficult if not impossible to impose functional or access restrictions on the Internet without violating that basic tenet.[252] Taxes on email, the Great Firewall of China, deep-packet inspection for quality of service, takedowns of peer-to-peer networks—each targets a different aspect of the ability to send data freely from one node to another.[253]

As long as we treat tethering as inseparable from appliancization, we will see only a false dichotomy between a networked world and a generative world. But once we see that a different choice can be made—anonymity versus generativity—then we should find tethering

---

into the computer, most commonly through a USB port. . . . [The software] will be useless without an authorized dongle capable of accessing the software.").

250. *See* BRIAN X. CHEN, ALWAYS ON: HOW THE IPHONE UNLOCKED THE ANYTHING-ANYTIME-ANYWHERE FUTURE—AND LOCKED US IN 47 (2011) ("Just imagine the possibilities when the incredibly capable Internet-powered devices we carry in our pockets increase in power and decrease in price while cellular networks mature to handle massive amounts of data at blazingly fast speeds.").

251. *See* David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, AGM SIGCOMM COMPUTER COMM. REV., Aug. 1988, at 106 (explaining that "since this network was designed to operate in a military context, which implied the possibility of a hostile environment, survivability was put as a first goal, and accountability as a last goal. . . . An architecture primarily for commercial deployment would clearly place these goals at the opposite end of the list.").

252. ZITTRAIN, *supra* note 1, at 185 (noting that "new platforms of Web services . . . depend on Internet connectivity to function"); *see also id.* at 123-24. ("[T]he features that make tethered appliances worrisome—that they are less generative and that they can be so quickly and effectively regulated—apply with equal force to the software that migrates to become a service offered over the Internet.").

253. *See, e.g.*, Richard Clayton et. al., *Ignoring the Great Firewall of China* 3 I/S J.L. & POL'Y INFO. SOC'Y 273, 274–78, 284–86 (2007) (describing "methods available to countries that wish to prevent their citizens from accessing particular Internet content," which include content inspection and packet dropping schemes, as well as the Great Firewall, China's Internet filtering system).

to be the lesser harm, because it works in consonance with the existing attributes of the network, rather than being at odds with the core function of the network.

IV. CONCLUSION

For years, we have accepted as gospel the notion that nourishing the innovative potential of the Internet depends on minimizing restrictive controls over the network. What we have seen instead is a game of whack-a-mole, where resistance to controls in one place only causes other controls to pop up elsewhere.[254] Rather than resisting those controls reactively, wherever they appear, we should think more prudently about prioritizing the disorderly aspects of the Internet that matter most. Zittrain has argued persuasively that generativity should top that list.[255] But a list of priorities must offer more than one option to be practicable to regulators interested in achieving specific regulatory outcomes. If we want regulators to leave generativity intact, we must lead them away with some other bait. A willingness to embrace restrictions on online anonymity would provide that flexibility.[256]

One place to begin is to embed network identification into the computer hardware, such as through the use of IPv6.[257] The current Internet addressing system, IPv4, is transitioning to IPv6 because we are running out of IPv4 addresses.[258] By providing a greatly expanded

254. *See supra* Parts II–III.

255. *See supra* Part III.B.

256. *See supra* Part III.

257. *See* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 532, 543 (2012), *available at* http://harvardnsj.org/wp-content/uploads/2011/03/vol.-2_Clark-landau_Final-Version1.pdf (noting that "[n]etwork-level addresses (IP addresses) are more useful than is often thought as a starting point for attribution, in those cases where attribution is relevant," since any form of personal-level attribution is ineffective when dealing with compromised computers).

258. *See* Dylan Tweney, *No Easy Fixes as Internet Runs Out of Addresses*, WIRED (Feb. 3, 2011, 9:58 AM), http://www.wired.com/business/2011/02/internet-addresses/ ("IP addresses are like telephone digits, in that there's a finite number of them. . . . It's as if every possible area code from 001 to 999 had already been utilized or reserved."); *see also* Hollis, *supra* note 114, at 399 n.172 (describing the benefits and flaws of transitioning to IPv6); Terrence K. Kelly & Jeffrey Hunker, *Cyber Policy: Institutional Struggle in a Transformed World*, 8 I/S: J.L. & POL'Y INFO. SOC'Y 210, 238–41 (2012) (noting the policy challenges of transitioning from IPv4 to IPv6, because IPv6 is not backward compatible with IPv4); IEEE-USA, NEXT GENERATION INTERNET: IPV4 ADDRESS EXHAUSTION, MITIGATION STRATEGIES AND

address space, IPv6 eliminates the need for dynamic addressing and shared addressing—two outgrowths of the current address shortage that have contributed greatly to hindering the reliable identification of Internet users.[259] Dynamic addressing allows efficient recycling of a limited set of addresses by assigning addresses on a rolling basis as each device connects to the network, rather than assigning static addresses that never change.[260] Shared addressing employs a different scheme that allows a single, assigned address to be used simultaneously by multiple users and devices.[261] Both workarounds rely on maintaining imprecise relationships between user devices and IP addresses. By contrast, using IPv6 to assign a unique and static IP address to each device would go a long way toward achieving device-level attribution.

Under the device-ID model, at least three vulnerabilities would remain: (1) the potential inaccuracy of network activity logs (forgetting or mistaking an identity); (2) the use of intermediary devices to mask the originating IP address (concealing an identity); and (3) the spoofing of IP addresses (falsifying an identity).[262] Those vulnerabilities can be mitigated, though not eliminated.

Of the three, the first presents the most difficult logistical challenge, because it requires numerous private parties to maintain massive data logs and protect them from unauthorized access or tamper-

---

IMPLICATIONS FOR THE U.S. 9–11 (2009), *available at* http://www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-IPv62009.pdf.

259. *See* Frederick Lah, Note, *Are IP Addresses "Personally Identifiable Information"?*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 681, 699–704 (2008) (describing the debate over whether IP addresses are reliable enough at identifying individuals that they should be protected as personal data); IEEE-USA, *supra* note 258, at 9–11 (describing common methods of sharing scarce IP addresses, including Network Address Translation (NAT), Classless Inter Domain Routing (CIDR), and dynamic IPv4 address assignment (DHCP)).

260. IEEE-USA, *supra* note 258, at 11 ("One method of IPv4 address exhaustion mitigation is to allow different clients to share the same IP address at different times. . . . When the client disconnects, the ISP puts the previously allocated IP address into a pool.").

261. *See* ICANN, BEGINNER'S GUIDE TO INTERNET PROTOCOL (IP) ADDRESSES 4 (2011), *available at* http://www.icann.org/en/about/learning/beginners-guides/ip-addresses-beginners-guide-04mar11-en.pdf ("If your computer is assigned a private address but you can still access services over the Internet, then your computer is probably behind a Network Address Translator (NAT), which lets lots of computers share a single unique IP address.").

262. *See* Hollis, *supra* note 114, at 399 n.172 (noting that "record-keeping, stepping stones, [and] botnets" will continue to create attribution problems even after a transition to IPv6).

ing.[263] Enacting statutory recordkeeping duties would help,[264] but errors and security breaches would likely persist. The second presents the most difficult technological and legal challenge, because it entails preventing or uprooting any proxy networks that assist—voluntarily or involuntarily—in passing around Internet traffic to "launder" it of identifying information.[265] Above-the-board operations like Tor might be more easily dissuaded, but a determined criminal operation would use every means possible to protect itself.[266] The third is the simplest to address, as it can be foiled mainly by performing server-side validation to verify that the packet's stated origin matches its real origin.[267] Nevertheless, it still deserves mention because it can be exploited for distributed denial of service ("DDoS") attacks.[268]

Each of those vulnerabilities is compounded by the problem of international borders. If a foreign government refuses to cooperate, it can obstruct identification efforts in each of the three ways described above: (1) by withholding or failing to keep appropriate records; (2) by allowing its network traffic to be scrubbed of identifying details; and (3) by improperly validating spoofed credentials. A for-

263. *See id.* at 399 ("Attackers routinely destroy or modify system logs so victims lack information (or receive misinformation) on what happened.").

264. *See supra* note 160.

265. *See* Clark & Landau, *supra* note 257, at 533 ("The most challenging and complex attacks to deter are those we call multi-stage attacks, where the attacker infiltrates one computer to use as a platform to attack a second, and so on."); Hollis, *supra* note 114, at 399 ("[A botnet] will install several 'stepping stones' between the attacking computer and the system used to control and command it. In effect, attackers can 'launder' the packets so that the attack's true origins will be difficult, if not impossible, to find.").

266. *But see* Roger Dingledine & Nick Mathewson, *Anonymity Loves Company: Usability and the Network Effect*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 547, 549 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005) (explaining that "[n]o organization can build [an anonymizing network] for its own sole use," because "any connections entering or leaving that network would be obviously linkable to the controlling organization").

267. *See* Clark & Landau, *supra* note 257, at 534–35 (explaining that "the source address found in [Internet data] packets often provides a valid form of source attribution," even though it could potentially be forged or falsified by the sender, because "the source address of the packet has to be valid for the reply to arrive back").

268. *See id.* at 556 ("[T]he only sort of attack where a forged IP address is effective is a DDoS attack, where the goal is just to flood the destination with useless traffic. Any more sophisticated exchange, for example in support of espionage, will necessitate a two-way exchange of information; this requires the use of valid source addresses.").

eign government could also obfuscate its own military activities[269] or refuse to extradite identified criminals residing within its territory.[270] The challenge of international cooperation is a longstanding one, and unlikely to be resolved anytime soon, but one option would be to conduct an "Internet embargo" by establishing a cooperative network of Internet allies, and assigning tariffs or prohibiting all traffic from non-cooperating countries.[271]

Another option is to deploy reliable validation at the application layer.[272] Previous efforts such as digital signatures have been unsuccessful,[273] but two possibilities seem particularly promising. The first is peer-based validation through social networks such as Facebook.[274] Ninety percent of the work toward peer-based validation has been done; the remaining ten percent requires finding a way to cull out the fake accounts without alienating the real ones. The second possibility is government-based validation through an agency-issued credential. The U.S. Army already registers every soldier and provides online access to military benefits and services.[275] Digital management of civilian

269. *But see id.* at 554 (noting that for national security issues, the degree of attribution needed is "perhaps only at the level of the state actor responsible").

270. *See id.* at 552–53 ("[E]ven if we were to push for a variant of the Internet that demanded very robust identity credentials to use the network, tracing would remain subject to barriers that would arise from variation in jurisdictions.").

271. *See, e.g.*, Gregory S. McNeal, *Cyber Embargo: Countering the Internet Jihad*, 39 CASE W. RES. J. INT'L L. 789 (2007).

272. *See id.* at 556–57 (arguing that an application-specific approach to attribution offers a better tradeoff between accountability and freedom than a network-based approach).

273. *See* Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 IDAHO L. REV. 353, 358–59 (2001) (refuting claims that digital signatures are widely used, and arguing furthermore that usage is unlikely to increase in the near future, because "trying to use asymmetric cryptography as a signature on a contract is like trying to fit a square peg into a round hole . . . with few tangible payoffs in sight").

274. *See supra* note 137 and accompanying text.

275. *See* Louise Knapp, *Army Intranet: World's Largest*, WIRED (Nov. 15, 2001), http://www.wired.com/science/discoveries/news/2001/11/48183 (reporting that "[a]ll soldiers on active duty have already been ordered to sign up" to Army Knowledge Online ["AKO"], which "acts as a portal to hundreds of the Army's internal websites" and "centralizes all the information the Army has, so the soldier does not have to search through to find them all"); *see also* Gary Winkler, *Winkler: AKO Is So Much More than E-Mail*, FED. COMPUTER WK., June 14, 2011, *available at* http://fcw.com/articles/2011/06/20/

benefit entitlements is the next logical step. The challenge there is in finding appropriate ways to adapt a military solution to the civilian sector.

Beyond the technological challenges, there is also a set of specific situations where identity-based measures are an ill-suited mode of regulation. Some activities are so hazardous (such as nuclear technology) that we do not want to allow any form of public access, anonymous or otherwise. Other identity-based measures of regulation may not work for the following reasons: (1) the remedies may be nonexistent (because the laws are unwritten or unjust); (2) the remedies may be unenforceable (as with international crimes that cross jurisdictional borders); (3) the remedies may be under-enforced (as with petty crimes that overextend our prosecutorial resources); or (4) the remedies may be non-factors (as with crimes of passion and acts of terrorism or war).

Where the problems associated with identification are too intractable, we should acknowledge the need for some generative compromise, and return to preventive, appliancized solutions. The point is not to vilify anti-generative measures, or to exalt anti-anonymity measures. Whatever balance we ultimately accept, we should recognize that there is a choice to be made, and that the choice should reflect the exceptionalism we want the future Internet to have.

---

comment-gary-winkler-army-ako-email.aspx ("AKO has become the Army's 'secret sauce.' . . . AKO provides identity, authentication and help-desk services for more than 1,000 applications."). *But see* Joe Gould, *GIs, Officials Disagree on Effectiveness of AKO*, ARMYTIMES (Nov. 28, 2010, 8:33 AM), http://www.armytimes.com/news/2010/11/army-soldiers-disagree-on-army-knowledge-online-112810w/ (reporting on frustrations with the system's cumbersome authentication requirements).