THE ANONYMOUS INTERNET

Bryan H. Choi[*]

This piece 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," an attribute representing the ability of ordinary users to generate new, unanticipated uses, and thereby mold the character and constitution of the internet. Yet, if we want to leave generativity alone, we need another point of leverage with which to regulate behavior. It is not enough to recommend simply that total regulation be reduced.

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 the dominant role of the internet should be as an engine of innovation and creative output, not a vehicle of anonymous speech. Conversely, the so-called "right to anonymity" is a narrow protection that does not contemplate the unbridled use of anonymizing technology. Thus, if we must adhere to our regulatory goals online, then we should embrace limitations on anonymity as a means of averting more onerous limitations on technological functionality.

[*] Thomson Reuters Fellow in Law, Information Society Project, Yale Law School.
[Acknowledgements]

I. INTRODUCTION

The internet has made anonymity seem like an entitlement. Even when our anonymity is paper thin, 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 at all. We are not asked for identification when we browse most websites, and when we are, we select monikers that are fanciful and disposable. If real identity is required, such as to check one's bank 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.

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 added romanticism and notoriety to anonymity. The idea that anonymity can provide a check on abusive power is deeply appealing. Yet anonymity can be abused in turn. Those who criticize anonymity argue that it breeds its own form of unaccountability. Asking whether anonymity is good or bad is the wrong question, because our instincts change depending on whose anonymity it is. We know that some anonymity ought to be preserved, and we also know that anonymity is a fragile construct. The internet currently offers too much anonymity, and yet we fear that altering the balance would 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, it will squeeze out the real value of the internet.

While anonymity has been a longstanding attribute of the internet, it is not the most critical. 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."[1] In other words, a generative technology is one that is capable of being adapted to "generate" new and unforeseen uses—the more the better. As an example, paper is highly generative because it can be used for a broad variety of tasks, such as writing, wrapping fish, flying kites, storing gunpowder, and so on. The potency of the internet, and software more generally, is that it exhibits that same capacity to be molded in every conceivable manner. But by the same token, that versatility is a double-edged sword: generativity enables abuses that threaten, and occasionally

[1] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET 70 (2008); Jonathan 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* David G. Post, *The Theory of Generativity*, 82 FORDHAM L. REV. 2755 (2010).

effectuate, disastrous disruptions on personal, national, and global scales.[2] Paper can be used to libel someone's good name, set a forest fire, or start a war. By definition, the abuses of generativity cannot be separated from its benefits; the freedom to experiment required to produce good outcomes necessarily allows mistakes and abuses too. The unusually broad range of uses enabled by the internet means that it also poses an unusually broad range of potential harms.

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. 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."[3] The conclusion is sound, but he glosses over a crucial step. If generativity is the very engine that enables the harms that are considered unacceptable, then preserving generativity is not a viable option unless another point of leverage is available. All else equal, any measure that leaves generativity untouched will continue to permit those same harms.

Anonymity represents 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. But if regulation is desired, then preserving generativity requires a reduction in anonymity, and preserving anonymity requires a reduction in generativity. The fate of the generative internet depends on how we choose to regulate the anonymous internet. As long as anonymity remains inviolate, generativity will be the loser.

Part II defines the conceptions of anonymity and generativity, and expands on the proposition that one must be exchanged for the other in order to satisfy the demand to regulate harms. Anonymity and generativity are interchangeable attributes because they fulfill similar functions. Both are intermediate attributes: dependent on underlying technology, while sharing a larger purpose of maximizing the potential for change through churn. Where they differ is in how they are controlled. Disallowing anonymity discourages certain activities by certain individuals, but removing generative functionality quashes all activities by all individuals. Regulating generativity is the harsher remedy.

Part III then revisits a set of familiar cyberlaw problems in order to recast those traditional case studies in terms of the anonymity-generativity dichotomy. The failure to understand that essential tradeoff has left us with a never-ending sense that more must be done to rein in the internet. Much of that uncertainty stems from our muddled relationship with anonymity. In seeking greater clarity,

---

[2] *See, e.g.*, 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.").

[3] ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 1, at 165; *see also* Zittrain, *Generative Internet*, *supra* note 1, at 2026, 2031, 2035 (expressing hope that "we can make the grid more secure without sacrificing its essential generative characteristics" and that individual harms can be "prevented or rectified by narrow interventions").

one measure is to look to see what the courts have done. Thus, Part IV turns to the jurisprudence of anonymity. Contrary to what many liberal scholars have suggested, the analysis points to a rejection of a "right" to anonymity. Instead, the Supreme Court has embraced an actual-harm test that demands actual evidence that identification would cause harm before it will intervene on behalf of anonymity. The fact that anonymity is relatively disfavored by the courts lends further support to the idea that more should be done to protect the generative internet by reining in the anonymous internet.

Finally, Part V concludes by raising a set of problems that challenge the limits of regulating anonymity. Those examples begin with areas where we worry that laws are inadequate protections, and continue into areas where attempts to regulate anonymity are unenforceable, such as across jurisdictional borders, as well as instances where identification alone is ineffective, such as petty acts that overextend our prosecutorial resources or, at the other extreme, acts of terrorism or war. In the end, some generative compromise may be inevitable. But if we are committed to maximizing generativity, we must consider the extent to which anonymity can be curbed. If generativity represents the core value of the internet, then sacrificing anonymity may be the lesser evil. And yet, a certain degree of anonymity may remain inviolate.

II. 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 social behavior. Anonymizing technologies allow dissenting voices to replace existing social structures. Likewise, generative technologies allow new innovations to break old patterns of behavior. A society that is permissive will allow more anonymity and generativity, while a society that is restrictive will allow less of each. It is natural to expect that new technologies will 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.

As long as we accept that some enforcement is necessary, however, the relevant question is not whether generativity or anonymity can shift the balance of liberty and security, but whether the liberties afforded by generativity should be traded for the liberties afforded by anonymity. The claim that better anonymity means better liberty is seductive—and misleading. All governments are constructed out of a basic need to enforce rules, so a government that is unable to identify wrongdoers must find other ways to limit the wrongs that can be done.

> 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.[4]

Anonymity does not exist in a vacuum, and protecting it comes at direct cost to generativity. At the end of the day, better anonymity does not threaten security; it only threatens other liberties.

A. Dog Days of Anonymity

"On the internet," goes the infamous quip, "nobody knows you're a dog." 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. But of course that's not quite right; we share our identity with some parties while seeking to remain anonymous vis-à-vis everyone else. A better depiction is as a curtain that we draw between our confidants and distrusted outsiders.[5] We remain effectively anonymous to those outsiders as long as the curtain remains intact, but anyone within its curtilage can welcome others inside. Thus the security of an anonymous interaction is governed by two factors: the number of confidants, and the strength of secrecy to which they are bound. What some scholars have termed "untraceability" is the edge case where there are no known confidants.[6] "Traceable" anonymity, on the other hand, refers to cases where the confidants are already known and the only remaining variable is their discretion—which can be swayed by forces such as legal penalties, group norms,[7] and economic incentives.[8]

With online anonymity, we have remained stuck on the binary question of whether to moderate it at all.[9] Much of the reluctance to do so stems from the

---

[4] *See* Joseph William Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 WIS. L. REV. 975, 1022-23 (1983).

[5] *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.").

[6] A. Michael Froomkin, *Anonymity and Its Enmities*, 1995 J. Online L. art. 4 ¶¶ 11-40 (1995); *see also* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 416-24 (1996); John Alan Farmer, Note, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, 72 Fordham L. Rev. 725, 745-46 (2003). 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. He further notes that "the cost of obtaining a given amount of additional identification information will vary, possibly greatly, from one situation to another." *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. Chi. Legal F. 139, 150-51 (1996).

[7] The classic example is blood oaths of omerta. *See generally* MARIO PUZO, OMERTA (2000).

[8] *See, e.g.*, Reno v. Condon, 528 U.S. 141 (reviewing constitutionality of the Driver's Protection Privacy Act, which regulates the sale of drivers' records by state motor vehicle departments).

[9] The U.S. government's recent report on implementing an "Internet ID" exemplified the doublespeak that has become par for the course, insisting that its "Identity Ecosystem" would "preserve online anonymity and pseudonymity, including anonymous browsing." *See* THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE

tenacious idea that anonymity is an all-or-nothing proposition. Advocates typically alternate between rights-based rhetoric, and long lists enumerating the many beneficial purposes served by anonymity. Neither is particularly conducive to compromise. Naturally, if anonymity were a fundamental human right,[10] then one of the essential purposes of the internet would be to facilitate the exercise of that right. Any effort to obstruct that function would misapprehend the raison d'etre of the internet. Alternatively, even if we pursue the utilitarian approach, an abstract list of pros and cons tells us only whether anonymity is on balance good or bad, not how to discern when it should be preserved and when it should be relinquished.

The classic objection to anonymity, too, is often framed as a stark choice. Anonymity promotes free speech and autonomy, but undermines accountability and rule of law. When perpetrators escape detection, harms go unredressed,[11] and the aggregate incidence of harmful behavior increases as bad actors learn that penalties have no potency.[12] The internet amplifies that risk through network effects that occur at near-instantaneous speed.[13] Assessment of such evils has led some jurists to reject anonymity wholesale.[14]

Not surprisingly, the non-accountability argument has long been unpersuasive to anonymity hardliners, whose answer is that tolerating occasional

---

CHOICE, EFFICIENCY, SECURITY, AND PRIVACY 2, Apr. 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[10] *See* Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1569-70 (2007) (noting that some nations grant authors "an inalienable right to attribution, which right embraces a subsidiary right to be properly attributed as the author of that which she has created, a right not to be attributed as the author of that which she has not created, and a right to publish anonymously or under a pseudonym").

[11] *See* 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); Froomkin, *Flood Control*, *supra* note 6, at 404-05 ("Sissela Bok has argued that a society in which 'everyone can keep secrets impenetrable at will' be they 'innocuous . . . or lethal plans,' noble acts or hateful conspiracy`ies, 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.").

[12] *See* Post, *Pooling Intellectual Capital*, *supra* note 6, at 142 (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).

[13] *See* 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, 772 (2005) ("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 predicts that the power of a network grows at an exponential rate relative to the number of connected users.

[14] *See* Doe v. Reed, 561 U.S. ___, ___ (2010) (Scalia, J., concurring); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 385 (1995) (Scalia, J., dissenting).

vandals is a small price to pay for the singular ability to resist authoritarian control.[15] Some have even suggested that online abuses are more tolerable because they involve only informational harms and not physical harms.[16] And if anonymity could be revoked every time something were deemed the slightest bit displeasing, then it would be worse than useless. Under that view, brightline protection of anonymity is necessary to prevent gradual encroachments on legitimate uses of anonymity.

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 or as complex as the internet. And the trouble with using technology to elevate anonymity above the law is that it turns the enabling technology into a target. Such measures 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. But extending that tack to 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.

B. Horse Trading for Generativity

Better headway can be made by considering anonymity and generativity in tandem. Both are similar in that they represent bottom-up mechanisms for disrupting the prevailing status quo. Each permits new or alternative ideas to percolate up from any arbitrary source, be received on a level plane, and win acceptance on their merits. But they operate on different aspects of that process, a fact that is critical to our inquiry.

First, we begin by sifting through the many justifications that have been offered in defense of anonymity. Three main themes can be gleaned: privacy, participation, and truth. Together, they complete a lifecycle that permits ideas to be carried from private inception to public adoption.

---

[15] *See, e.g.*, A. Michael Froomkin, Lessons Learned Too Well, at 31, *available at* http://ssrn.com/abstract=1930017.

[16] 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."); ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 1, at 97 ("One might want to allow more room for experimentation in information technology than for physics because the risks of harm—particularly physical harm—are likely to be lower as a structural matter from misuse or abuse of information technology."). *But see* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED, July 11, 2011, 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"); Barnaby J. Feder, *A Heart Device Is Found Vulnerable to Hacker Attacks*, N.Y. TIMES, Mar. 12, 2008, http://www.nytimes.com/2008/03/12/business/12heart-web.html.

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,[17] but the one most relevant in this context is the desire to protect one's image in one context from the consequences of one's actions in another context.[18] By preventing intrusive monitoring, anonymity creates a permissive environment that allows for experimentation with ideologies and practices diverging from what we perceive to be the acceptable norm.[19] Whether one conducts a Google search on a sensitive medical condition[20] or places a listing on Craigslist's personals,[21] anonymity constructs a barrier that prevents those "private" acts from being linked to one's identity. That rationale can be extended to cover special circumstances where the sharing of personal information is unavoidable, such as the practices of medicine,[22] law,[23] and religion.[24]

---

[17] *See generally* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67 (2009).

[18] *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996) ("Anonymity refers to the power to control whether people know who you are; it is a tool of privacy."); Horn, *supra* note 13, 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."); *see also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

[19] *See* 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, 999 (2004) (noting that privacy scholars have criticized constant monitoring because it "inhibits daily activities, promotes conformity, causes embarrassment, and interferes with the creation of intimacy"); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000) (A realm of autonomous, unmonitored choice shelters experimentation with beliefs and associations, as well as "every other conceivable type of taste and behavior that expresses and defines self"). ["Arab Spring"; The Jane Collective.]

[20] *See* Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html; 33 Bits of Entropy, http://33bits.org/about/ (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); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (observing that reidentification science exposes the illusory nature of the promise that anonymization protects privacy)\.

[21] *See* Gary Wolf, *Why Craigslist Is Such a Mess*, WIRED MAGAZINE, Aug. 24, 2009, http://www.wired.com/entertainment/theweb/magazine/17-09/ff_craigslist; Douglas Quenqua, *Recklessly Seeking Sex on Craigslist*, N.Y. TIMES, Apr. 19, 2009, at ST1, http://www.nytimes.com/2009/04/19/fashion/19craigslist.html. *But see* Brad Stone, *Craigslist Agrees to Curb Sex Ads*, N.Y. TIMES, Nov. 6, 2008, http://www.nytimes.com/2008/11/07/technology/internet/07craigslist.html (agreeing to require phone numbers and credit card payments to confirm identities); Abby Goodnough & Anahad O'Connor, *Suspect in Hotel Killing Is Described as Honor Student Who Preyed on Women*, N.Y. TIMES, Apr. 22, 2009, at A14, http://www.nytimes.com/2009/04/22/us/22boston.html (detailing successful police work to identify the so-called "Boston Craigslist Killer").

[22] Physician-patient confidentiality is governed both by the Hippocratic oath, as well as a complex, overlapping scheme of state and federal law that now includes the Health Insurance Portability and Accountability Act ("HIPAA"). *See* Ralph Ruebner & Leslie Ann Reis, *Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege*, 77 TEMP. L. REV. 505 (2004).

But privacy does not depend on anonymity, and anonymity implies more than just passive secrecy.[25] Privacy focuses inward and seeks to keep the world out, while anonymity focuses outward and prevents the world from shutting ideas in. The main reason to invoke anonymity is to avoid repercussion for ideas or acts that are actively thrust into the public domain, and that therefore have an effect on others. Anyone can be daring in sharing with potentially unsympathetic audiences, which means not only that more ideas can be shared, but also that more people can safely signal approval or disapproval of an idea.[26] The most highly touted uses of anonymity, such as the Federalist papers, speech by persecuted groups, or whistleblowing,[27] tend to be instances of public advocacy and civic service, not private self-discovery. Democratic governance is advanced when more people are able to have their say.[28] Under that reasoning, anonymous comments are always defensible no matter how vile, and the best defense is to fight speech with more speech.[29] The pure increase in citizen participation is more important than the quality of discourse that is thereby gained.

An evolution in private norms can bubble over into public acceptance if it becomes equated with "truth." It is often claimed that the best path to truth is to allow ideas to compete freely in a "marketplace" of ideas.[30] Anonymity can serve that function in two ways. First, in a macroeconomic sense, it expands the size of the market by stimulating the production of additional speech that otherwise

---

[23] *See* Upjohn Co. v. United States, 449 U.S. 383 (1981); In re Witnesses Before the Special March 1980 Grand Jury, 729 F.2d 489 (7th Cir. 1984); Fed. R. Evid. 502.

[24] *See* Norman Abrams, *Addressing the Tension Between the Clergy-Communicant Privilege and the Duty to Report Child Abuse in State Statutes*, 44 B.C. L. REV. 1127 (2003).

[25] *See* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, [] (1995).

[26] *See* Horn, *supra* note 13, 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.").

[27] *See, e.g.*, 5 U.S.C. § 1213(h).

[28] Lidsky & Cotter, *supra* note 10, 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 more democratic."). *But see* Doe v. Reed, 130 S. Ct. 2811, 2837, 561 U.S. ___, ___ (2010) (Scalia, J., concurring) ("Requiring people to stand up in public for their political acts fosters civic courage, without which democracy is doomed."); CASS SUNSTEIN, REPUBLIC.COM 2.0 (2007); CHRIS ANDERSON, THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE (2006); Malcolm Gladwell, *Small Change*, THE NEW YORKER, Oct. 4, 2010, http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (criticizing social media activism as being ineffective because it is built on "weak ties").

[29] *See* Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 160-61 (2008) (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.'").

[30] *See* Abrams v. United States, 250 U.S. 616, 630 (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.").

would be suppressed.[31] "Thought that is not offered cannot get itself accepted into the competition of the market."[32] That rationale could justify legal protections for whistleblowers,[33] as well as extralegal operations such as Tor[34] and WikiLeaks.[35] Second, in a microeconomic sense, an individual idea becomes more competitive within the existing market when identifying information is withheld, because readers are forced to judge it on its merits without being biased by the identity or background of the author.[36] A law student can satirize the legal industry by masquerading as a world-weary law firm partner;[37] a political campaign can covertly distribute "viral" videos that undermine opposing candidates without having it be discounted as propaganda.[38] To be sure, some have rightly questioned the authenticity of "truth" delivered by anonymity.[39] Information is often more

---

[31] *See, e.g.*, Sandeen, *supra* note 11, at 541 ("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."); Post, *Pooling Intellectual Capital*, *supra* note 6, 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."); Lidsky & Cotter, *supra* note 10, 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).").

[32] Note, *Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084, 1112 (1961).

[33] *See* Whistleblower Protection Act of 1989, 101 Pub. L. No. 12, § 2, 103 Stat. 16 (1989) ("[P]rotecting employees who disclose Government illegality, waste, and corruption is a major step toward a more effective civil service."); 5 U.S.C. § 1213(h).

[34] *See* Tor: Overview, https://www.torproject.org/about/overview.html ("Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.").

[35] *See* About WikiLeaks, http://wikileaks.org/About.html ("Scrutiny requires information. Historically, information has been costly in terms of human life, human rights and economics. As a result of technical advances particularly the internet and cryptography—the risks of conveying important information can be lowered.").

[36] *See* Froomkin, *Flood Control*, *supra* note 6, at 409 ("Communications that give no hint of the age, sex, race, or national origin of the writer must be judged solely on their 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 10, at 1576 (withholding the speaker's identity may protect the public against underestimating the truth-value of the statement).

[37] *See* Sara Rimer, *Revealing the Soul of a Soulless Lawyer*, N.Y. TIMES, Dec. 26, 2004, http://www.nytimes.com/2004/12/26/fashion/26BLOG.html.

[38] *See* DANIEL KREISS, TAKING OUR COUNTRY BACK: THE CRAFTING OF NETWORKED POLITICS FROM HOWARD DEAN TO BARACK OBAMA (forthcoming 2012) (describing the use of such tactics by the Obama 2008 campaign).

[39] *Constitutional Right to Anonymity*, *supra* note 32, at 1116 ("In order to judge whether progress toward truth has been made it is necessary to know what is true."); *see also* Lidsky & Cotter, *supra* note 10, 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 . . . ."); Froomkin, *Flood Control*, *supra* note 6, at 403. That said, some facts can be self-verifying. *See* Eugene Volokh, *Crime-Facilitating Speech*, 57 STANFORD 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

reliable when the speaker's identity and credibility are verifiable,[40] while anonymity has been used in the past to spread false information about everything from financial stocks[41] to sexual relationships.[42] But the salient point here is truthiness not truthfulness. When anonymity inspires change, the strength of conviction often matters more than the conviction itself.[43]

Zittrain's theory of generativity unfolds along much the same trajectory. He 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."[44] 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 features map loosely onto the functions fulfilled by anonymity. With anonymity, the purpose is to incubate ideas that deviate from standard norms (privacy), expand the pool of individuals able to articulate those ideas (participation), and assist those ideas in achieving widespread adoption (truth). Similarly, generativity allows deviations from intended uses (leverage, adaptability), empowers ordinary users to contribute (accessibility, ease of use), and enables easy distribution of new uses to new users (transferability). A

---

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.").

[40] *See* Lidsky & Cotter, *supra* note 10, 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."); *Constitutional Right to Anonymity*, *supra* note 32, at 1109-12 ("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 because "anonymous remarks will be greatly devalued precisely because they are anonymous and easy to make").

[41] Michael Lewis, *Jonathan Lebed's Extracurricular Activities*, N.Y. TIMES MAGAZINE, Feb. 25, 2001, http://www.nytimes.com/2001/02/25/magazine/jonathan-lebed-s-extracurricular-activities.html.

[42] *See, e.g.*, Carafano v. Metrosplash.com, Inc., (9th Cir. 2003); Joanne Green, *Blind Date*, MIAMI NEW TIMES, Sept. 14, 2006, http://www.miaminewtimes.com/2006-09-14/news/blind-date/1/; Lizette Alvarez, *(Name Here) Is a Liar and a Cheat*, N.Y. TIMES, Feb. 16, 2006, http://www.nytimes.com/2006/02/16/fashion/thursdaystyles/16WEB.html; *see also* Nadya Labi, *An IM Infatuation Turned to Romance. Then the Truth Came Out*, WIRED, Aug. 21, 2007, http://www.wired.com/politics/law/magazine/15-09/ff_internetlies.

[43] *See* Suzanna Sherry, *Democracy and the Death of Knowledge*, 75 U. CIN. L. REV. 1053 (2007) (observing that "democratization of knowledge" can lead to the "death of knowledge"); *Constitutional Right to Anonymity*, *supra* note 32, at 1123-24 (anonymity should be promoted in order to "bring about a general climate in which modification [of beliefs] is most likely to be encouraged"); *see also* JARON LANIER, YOU ARE NOT A GADGET: A MANIFESTO 48-50, 55-64, 122-23 (2010) (criticizing the wisdom of crowds and arguing that "quantity can overwhelm quality in human expression").

[44] ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 1, at 71.

reduction in any of those attributes stunts the system's potential to generate progress through churn.

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 one, in which a few gatekeepers control all the cards.[45] Zittrain offers two supporting narratives: 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. Generativity does not replace the top-down model of research and development, but serves as a supplementary source of do-it-yourself invention. Likewise, the participation rationale is that citizens have more opportunities to participate meaningfully in the creation of culture, rather than being passive consumers of culture produced by others.[46] Again, the point is not to replace the content created by mainstream media, but rather to add more citizen-produced content.

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."[47] Curiously, he then downplays that unruliness, and claims instead that generativity can promote better security by equipping communities with better tools and capabilities to self-police their collective norms.[48] Perhaps he anticipates that it would be difficult to lobby for generativity if it is seen as dangerous. But that paradox—that generativity can simultaneously advance liberty and security—is held together by an illusory thread of communitarianism.[49] The successes of Zittrain's anecdotal examples—a Dutch traffic experiment[50] and Wikipedia[51]—

---

[45] *Id.* at 80-90. In his book, Zittrain uses the terms "polyarchy" and "hierarchy" interchangeably with the terms "bottom-up" and "top-down" to describe the contrast between development by many versus development by few. *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."). In a follow-on article, he characterizes those two sets of terms as being orthogonal to each other, with "polyarchy" and "hierarchy" expressing the more accurate concept of availability of choice to join one governing system or another. *See* Jonathan Zittrain, *The Fourth Quadrant*, 78 FORDHAM L. REV. 2767, 2768 (2010) ("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.").

[46] ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 1, at 90-94.

[47] *Id.* at 105-06.

[48] *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, *Fourth Quadrant*, *supra* note 45, at 2770.

[49] 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." *See* Post, *Theory of Generativity*, *supra* note 1, at 2764.

[50] Zittrain highlights the success of a traffic experiment conducted by the Dutch town of Drachten that improved safety through the elimination of all traffic signs—verkeersbordvrij. ZITTRAIN,

are easily distinguished and refuted. The gist of his argument is not better enforcement through generativity, but instead the familiar libertarian hope that eliminating odious rules will eliminate the need for enforcement.[52] The catch is that no matter how reasonable a rule may seem to the larger community, minds differ and generativity qua liberty allows any single "subversively minded techie" to collapse the illusion of security.

A trivial example is networked games, where easily installed cheats allow an individual player to enjoy temporary dominance over others—a selfish thrill that persists despite strong indignation from other players and extensive efforts by game designers to disable such exploits. More notoriously, splintering happens within communities of skilled hackers, such as when LulzSec broke off from the larger group Anonymous. When the members of LulzSec became interested in gaining publicity by committing more conspicuous "ops," they were able to do so despite efforts by other members of Anonymous to self-police against cheap vandalism.[53] Nor were those attacks stopped by sophisticated defenses, or because of LulzSec's noble ideals; instead, the main deterrent appears to have been the increasing risk of being exposed and caught.[54]

It is precisely because generativity is a destabilizing force with as much potency as anonymity that there has been a strong impulse to moderate its excesses. In particular, Zittrain highlights the move toward "tethered appliances," i.e., devices like DVRs or mobile phones that can be reprogrammed from afar by

---

FUTURE OF THE INTERNET, *supra* note 1, at 127. But that town had been experiencing an average of only 8 accidents a year, none of which had been fatal. NOORDELIJKE HOGESCHOOL LEEUWARDEN, THE LAWEIPLEIN: EVALUATION OF THE RECONSTRUCTION INTO A SQUARE WITH ROUNDABOUT 26, *available at* http://www.fietsberaad.nl/library/repository/bestanden/Evaluation%20Laweiplein.pdf. In addition, the town did not rely simply on good will; it also converted the intersection into a roundabout, a traffic structure that inherently functions well without signs.

[51] *See, e.g.*, 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, 199-201 (2010) (describing Wikipedia's governance as "not purely bottom-up," and that a handful of appointed "bureaucrats" possess authority over all other users). [John Siegenthaler, rate of errors, number of actual editors, etc.]

[52] ZITTRAIN, FUTURE OF THE INTERNET, *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.").

[53] *See* Eric Mack, *Hacker Civil War Heats Up*, PCWORLD, June 24, 2011, http://www.pcworld.com/article/231078/hacker_civil_war_heats_up.html; Kim Zetter, *Researchers: Anonymous and LulzSec Need to Focus Their Chaos*, THREAT LEVEL, Aug. 6, 2011, http://www.wired.com/threatlevel/2011/08/defcon-anonymous-panel/

[54] *See* Matthew J. Schwartz, *LulzSec Leader Sabu Details Exploits*, INFORMATIONWEEK, Oct. 11, 2011, http://informationweek.com/news/security/cybercrime/231900535; Riva Richmond & Nick Bilton, *Saying It's Disbanding, Hacker Group Urges New Cyberattacks*, N.Y. TIMES, June 27, 2011, at B1, http://www.nytimes.com/2011/06/27/technology/27hack.html.

a controlling interest.[55] Zittrain worries that the trend toward tethered appliances is anti-generative because it makes regulation too easy, permitting regulators to stifle experimental uses before they have a chance to prove their worth.[56] When enforcement is costly, regulators must economize their resources, and are therefore forced to tolerate activities that are technically illegal but below a certain threshold of priority.[57] That leniency "allow[s] for experimentation of all sorts and later reining in [of] excesses and abuses as they happen, rather than preventing them from the outset."[58] But as regulatory costs approach zero, regulators can achieve perfect enforcement, thereby eliminating the latitude to disagree and decide for oneself whether an activity is truly harmful.[59]

Yet, we should be careful to distinguish tethering from appliancization. As other commentators have observed, "tethering and appliancization sometimes flow from common pressures, [but] one can exist without the other."[60] Appliancization inflicts generative loss to prevent future violations, but tethering relies on a different mechanism—identification—to embed the potential for future regulation. A critique of tethered applications therefore sheds light on the larger dilemma between anonymity and generativity.

Of the two, appliancization is more troubling precisely because it bypasses the individual. In part, the problem is one of peremptory application. Instead of having to petition a court or other arbitrator, and abide by all the procedural protections and costs attendant to such a petition, a controlling interest with direct access to a device can simply compel the results it wants on its own terms. A company like Amazon can spontaneously delete electronic copies of books like George Orwell's "1984" and "Animal Farm";[61] Apple can regularly reprogram its devices in order to thwart efforts to "jailbreak" them, even when jailbreaking is

---

[55] ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 1, at 101-04.

[56] *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."); *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.").

[57] *Id.* at 119 (citing Tim Wu, *Does YouTube Really Have Legal Problems?*, SLATE, Oct. 26, 2006, http://www.slate.com/id/2152264).

[58] *Id.* The argument for 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* Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 254-55 (2006).

[59] ZITTRAIN, FUTURE OF THE INTERNET, *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."); Christina M. Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH. L.J. & TECH. 12 (2008).

[60] *See* James Grimmelmann & Paul Ohm, *Dr. Generative or: How I Learned to Stop Worrying and Love the iPhone*, 69 MD. L. REV. 910, 938 (2010) ("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.").

[61] Brad Stone, *Amazon Erases Orwell Books from Kindle*, N.Y. TIMES, July 17, 2009, http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

not illegal;[62] and Google can reprogram its secret search algorithm to favor certain websites and disfavor others. The network neutrality debate has also captured that concern—that allowing private ISPs to throttle network traffic on a discriminatory basis would authorize them to act as silent and sole arbiters of content delivery.[63] Nor is such power limited to proprietary hardware: the creators of the Stuxnet worm were able to seize hostile control in the course of sabotaging a key nuclear facility in Iran.[64] Likewise, the U.S. government has been considering legislation that would allow it to shut down foreign websites by modifying the internet's domain name routing system.[65] When the permission settings are changed from "read-only" to "read-write," any party can resort to self-help without acknowledging the interests of adverse parties.

But even when the use of appliancization is mediated by a neutral court of law, it remains ripe for being applied for convenience rather than for cause. We have seen that temptation arise in cases like Viacom v. YouTube,[66] in which a copyright owner sought to shut down a video-sharing platform because of third-party uses rather than because of a fault with the technology itself. Although the district court dismissed that case because of statutory immunities, Viacom's intention was to obtain a single decision that would substitute for individual determinations of each video shared on YouTube. When a similar situation was presented in Grokster v. MGM, the Supreme Court acquiesced and reached the opposite result. There, the Court reasoned that the ill intent of the technology developer was sufficient to stand in as proxy for all individual uses of that technology.

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.[67] 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,[68] then that rule is absolute and can be challenged only if enterprising owners find ways to circumvent the limitation. On the other hand, remedies that act directly on the individual, such as imposing a fine or revoking a driver's license, must survive repeated scrutiny because they

---

[62] Jailbreaking is a process by which an iPhone user can access hidden functionality that Apple has purposefully deactivated. *See* Dan Goodin, *Apple Eyes Kill Switch for Jailbroken iPhones*, THE REGISTER, Aug. 20, 2010, http://www.theregister.co.uk/2010/08/20/apple_jailbreak_patent/; Jenna Wortham, *In Ruling on iPhones, Apple Loses a Bit of Its Grip*, N.Y. TIMES, July 26, 2010, http://www.nytimes.com/2010/07/27/technology/27iphone.html.

[63] *See generally* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2010).

[64] *See* Zetter, *supra* note 16.

[65] *See* David G. Robinson, Following the Money: A Better Way Forward on the PROTECT IP Act, 24-26 (Sept. 18, 2011), http://ssrn.com/abstract=1930013.

[66] Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

[67] *Cf.* Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601, 1613-, 1627-28 (1986) (arguing that awareness that legal judgments cause death and pain must remain central to legal interpretation).

[68] *Compare* Mulligan, *supra* note 59, at ¶¶ 14-15 (describing a Hawaiian initiative in 2000 to use cameras to catch anyone driving six or more miles over the speed limit).

can be contested and evaluated each time they are applied.[69] Forced repetition has uncovered judicial unease even in areas as seemingly settled as narcotics,[70] child pornography,[71] and death penalty sentencing.[72] Appliancization short-circuits that iterative process.

That is not to say that every instance of court-mandated appliancization is problematical. A court might reasonably prohibit a specific individual from using computers or accessing the internet, after determining that the individual's use of such technologies poses an unreasonable risk to public safety.[73] Nor should we be so distressed by cases like TiVo v. EchoStar,[74] where the dispute is limited entirely to the parties before the court. In that case, the district court ordered EchoStar to remotely deactivate patent-infringing DVR devices that were already in the physical possession of EchoStar's customers. But the injunction was not directed at prohibiting DVR usage by those customers. The conflict was between horizontal competitors over an intended and patented use, not between vertical entities threatening novel or unintended uses. As long as the imposition of appliancization is limited to parties who have an opportunity to represent themselves before the court, it does not invoke the same concerns of superficial treatment.[75]

---

[69] The federal government repealed the national speed limit in 1995. National Highway System Designation Act of 1995, 104 Pub. L. No. 59 § 205(d), 109 Stat. 568, 577.

[70] The sentencing guidelines were amended to reduce the 100-to-1 disparity in crack cocaine sentencing compared with powder cocaine sentencing. *See* Fair Sentencing Act of 2010, 111 Pub. L. No. 220, 124 Stat. 2372; Amendment 706, U.S. SENTENCING GUIDELINES MANUAL supplement to app. C 228-30 (2007) http://www.ussc.gov/Guidelines/2007_guidelines/Manual/appc2007.pdf. Much of the evolving resistance described above 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 (2010).

[71] 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 severe harshness of the remedy. A.G. Sulzberger, *Defiant Judge Takes on Child Pornography Law*, N.Y. TIMES, May 21, 2010, at A1, http://www.nytimes.com/2010/05/22/nyregion/22judge.html; *see also* Sen. 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 (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").

[72] *See, e.g.*, William Yardley, *Oregon Governor Says He Will Block Executions*, N.Y. TIMES, Nov. 22, 2011, at A14, http://www.nytimes.com/2011/11/23/us/oregon-executions-to-be-blocked-by-gov-kitzhaber.html (noting that only 34 states now allow the death penalty, and that only 27 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").

[73] *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.'").

[74] *See* ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 1, at 103-04 (citing TiVo, Inc. v. EchoStar Commc'ns Corp., 446 F. Supp. 2d 664 (E.D. Tex. 2006), *aff'd*, 516 F.3d 1290 (Fed. Cir. 2008)).

[75] Thus, the reasons for disallowing the aggregation of multiple defendants differs from cases such as mass torts and class actions, where multiple plaintiffs are aggregated because they are hoping to

Meanwhile, it is easy to point to tethering as the culprit that facilitates appliancization: after all, the authorities must be able to find the party before they can spoil it. But attempting to preserve generativity by severing connections with the networked environment is itself weirdly anti-generative. Tethering can promote generativity by encouraging underpolished "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, expecting early developmental releases to be replaced iteratively by newer stable releases.[76] 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 functions by providing devices at the end of the network with continuous access to data and services in the middle of the network. While cloud computing still faces important challenges, it is an extraordinarily innovative step made possible because of tethering not despite it.

Even if we were to set aside the affirmative benefits of tethering, however, there is another reason to endorse it: without tethering, the use of appliancization necessarily becomes more prevalent. Because any identifying characteristic can serve as a tether—a face, a fingerprint, a home address, or even an old essay[77]—the argument against tethering is in essence a call for untraceable anonymity. When no tethers are naturally present, any regulation must be asserted instead through functional restrictions. To take an offline example, Sudafed was a popular decongestant available for unrestricted over-the-counter sale, until the government recognized that large quantities were being purchased to produce methamphetamine. Since the pills did not contain a built-in tracking system,[78] the government resorted to other methods to ensure that Sudafed was not being purchased for wrongful purposes. In 2005, Congress passed the Combat Methamphetamine Epidemic Act, which required pharmacies to keep a log of sales, and limited the total quantity that could be sold to any given individual.[79] The end result was a restraint on all uses of Sudafed whether legitimate or illegitimate. 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, including checkpoints, fences,[80] patrols,

---

collect from a common pot of funds. [also, offensive collateral estoppel vs defensive collateral estoppel?]

[76] *See* ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR (2000).

[77] *See* David Johnston, *17-Year Search, an Emotional Discovery and Terror Ends*, N.Y. TIMES, May 5, 1998, http://www.nytimes.com/1998/05/05/us/17-year-search-an-emotional-discovery-and-terror-ends.html.

[78] Such tracking technologies have since been developed and implemented. *See* Randy Dotinga, *Viagra Tag Could Be Bitter Pill*, WIRED, Jan. 18, 2006, http://www.wired.com/science/discoveries/news/2006/01/70033.

[79] Pub. L. No. 109-177, tit. VII, 120 Stat. 192, 256. In response, Pfizer released a modified product called Sudafed PE that could not be transformed into methamphetamine. *See* Fox Butterfield, *States May Restrict Cold Pills with Ingredient in Meth*, N.Y. TIMES, Jan. 30, 2005, http://www.nytimes.com/2005/01/30/national/30meth.html.

[80] Julia Preston, *Some Cheer Border Fence as Others Ponder the Cost*, N.Y. TIMES, Oct. 20, 2011, at A17, http://www.nytimes.com/2011/10/20/us/politics/border-fence-raises-cost-questions.html.

and even citizen-manned surveillance cameras.[81] While efforts to create better identification schemes have been protested as violations of civil liberties,[82] we should at least be cognizant that the costs of enforcement are not being abandoned but are being shifted elsewhere.

That effect also extends to software. Because each copy is identical, any differentiation must be determined on the basis of extrinsic factors. When that test can be performed through a centralized mechanism—either because the software requires a shared environment (e.g., collaborative workflow programs or multiplayer games) or simply because it is designed to check in periodically—then verification is straightforward. Each purchaser can be issued a unique identifier, such as a username or license key, and any unauthorized use of that identifier is readily investigated and remedied.[83] Some spoofing and identity theft may occur, as it does offline, but that problem is relatively contained, as it is offline. On the other hand, when authentication is entrusted entirely to the software, we can expect to see a corresponding push to develop mechanisms that lock functionality, since each copy 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 change is committed by the rightful owner.[84] Other software programs have been designed so that they cannot be operated unless a physical object such as a CD-ROM or USB dongle is inserted into the computer.[85] That method provides better portability but is subject to loss or theft.

With the internet, the choice to favor appliancization over tethering is especially puzzling because it fights against the natural orientation of the system. On one hand, the network protocols were designed to guarantee robust connectivity between any two arbitrary peer nodes. Not surprisingly, it turns out that it is difficult, if not impossible, to impose functional restrictions without compromising that basic tenet. Taxes on email, the Great Firewall, 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. On the other hand, the internet lends itself to always-on connectivity,

---

[81] John Burnett, *A New Way to Patrol the Texas Border: Virtually*, NPR, Feb. 23, 2009, http://www.npr.org/templates/story/story.php?storyId=101050132.

[82] *See, e.g.*, Crawford v. Marion County Election Bd., 553 U.S. 181 (2008) (rejecting facial challenge of statute requiring photo identification for voter registration); Randall C. Archibold, *Arizona Enacts Stringent Law on Immigration*, N.Y. TIMES, Apr. 24, 2010, at A1, http://www.nytimes.com/2010/04/24/us/politics/24immig.html; Kim Zetter, *No Real Debate for Real ID*, WIRED, May 10, 2005, http://www.wired.com/politics/security/news/2005/05/67471.

[83] *See, e.g.*, Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593 (E.D. Pa. 2007). *But see* Joshua A.T. Fairfield, *The God Paradox*, 89 B.U. L. REV. 1017, 1023 (2009).

[84] *See* Technical Details on Microsoft Product Activation for Windows XP, Aug. 13, 2001, http://technet.microsoft.com/en-us/library/bb457054.aspx.

[85] *See* Wikipedia, Software Protection Dongle, http://en.wikipedia.org/wiki/Software_protection_dongle.

especially as bandwidth improves and costs diminish.[86] Tracing the activities of computing devices thus becomes a simple matter of assigning a unique identifier and ensuring that the identifier remains reasonably persistent over time. If we accept with certainty that at least one of those two tactics must be pursued, then we should find tethering 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.

III. FREE AS IN GENERATIVITY NOT AS IN ANONYMITY

With that framework in mind, it is worth revisiting a few familiar cyberlaw problems in order to illustrate how a better understanding of the inherent tension between anonymity and generativity might modify the way we would choose to approach those problems. The four examples addressed here are copyright piracy, defamation, age verification, and spam.

While each context has its idiosyncrasies, all efforts to reach resolution are reducible to variations on the central theme of restricting either generativity or anonymity. One trend worth highlighting is the unprecedented degree to which the Supreme Court has been willing to overrule Congress in defense of online anonymity—at the cost of generativity. As we will see later, that bias deviates from the standard presumptions the Court has applied against offline anonymity.

A. File Sharing and Copyright Infringement

The arc of the music industry's fight to enforce its copyrights exhibits a marked shift from efforts targeting generativity to efforts targeting anonymity. Although that shift has been heavily criticized, the intuition is sound: if generativity and anonymity are regulatory substitutes, then one can choose to assert control over either the technologies that enable abuse or the individuals who commit it. As long as copyrights are to be enforced, the question is whether to place the temptation of infringement firmly out of reach, or whether to detect and punish violations after the fact. A choice to do neither is a constructive forfeiture of the right.

Early regulatory efforts focused on attacking, from multiple angles, the generative technology that facilitated illicit file sharing. Most notably, the Recording Industry Association of America ("RIAA") sought to shut down the file-sharing networks by suing all the major operators and distributors of peer-to-peer platforms. In a series of high-profile lawsuits, the RIAA won favorable results against entities such as MP3.com,[87] Napster,[88] Aimster,[89] AudioGalaxy,

[86] *See* BRIAN X. CHEN, ALWAYS ON: HOW THE IPHONE UNLOCKED THE ANYTHING-ANYWHERE FUTURE—AND LOCKED US IN (2011).
[87] UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000).
[88] A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

Kazaa, Morpheus, Grokster,[90] iMesh, Limewire, and The Pirate Bay. At the same time, the music industry also pursued technological attempts to cripple peer-to-peer technology, such as flooding networks with fake music files,[91] and creating digital rights management ("DRM") systems that limited the capacity to copy music files. Those tactics enjoyed some success, but with diminishing returns. The legal attacks strained the limits of copyright protection,[92] while the technological attacks were thwarted by superior countermeasures.[93]

In frustration, the RIAA switched gears to identifying and suing individual file sharers—a tactic that was widely condemned at the time.[94] Even before the advent of peer-to-peer filesharing, the content industries had persuaded Congress to include in the Digital Millennium Copyright Act ("DMCA") a provision to expedite the identification of suspected copyright infringers. Just by filing a request for subpoena with the clerk of a federal district court, copyright holders could easily compel an internet service provider to furnish the identity of any alleged infringer.[95] After successfully persuading a few district courts to accept the use of this procedural shortcut,[96] the RIAA issued more than 1,500 subpoenas,

---

[89] In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

[90] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[91] *See* Ruben Cuevas et al., *Is Content Publishing in BitTorrent Altruistic or Profit-Driven*, ACM CoNEXT (2010), *available at* http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/11-Cuevas.pdf (fake publishers are responsible for 30% of content and 25% of downloads on BitTorrent portals).

[92] *See generally* Bryan H. Choi, *The Grokster Dead-End*, 19 HARV. J.L. & TECH. 393 (2006).

[93] *See* Timothy O'Brien, *Norwegian Hacker, 19, Is Acquitted in DVD Piracy Case*, N.Y. TIMES, Jan. 8, 2003, http://www.nytimes.com/2003/01/08/technology/08HACK.html (reporting acquittal in DeCSS case); 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; Daniel Roth, *The Pirates Can't Be Stopped*, PORTFOLIO.COM, Jan. 14, 2008, http://www.portfolio.com/news-markets/national-news/portfolio/2008/01/14/Media-Defenders-Profile. Those problems eventually led the industry to abandon DRM schemes. *See* Brad Stone, *Want to Copy iTunes Music? Go Ahead, Apple Says*, N.Y. TIMES, Jan. 6, 2009, at B1, http://www.nytimes.com/2009/01/07/technology/companies/07apple.html; Brad Stone & Jeff Leeds, *Amazon to Sell Music Without Copy Protection*, N.Y. TIMES, May 17, 2007, http://www.nytimes.com/2007/05/17/technology/17amazon.html.

[94] *See* Amy Harmon, *261 Lawsuits Filed on Internet Music Sharing*, N.Y. TIMES, Sept. 9, 2003, http://www.nytimes.com/2003/09/09/technology/09MUSI.html ("The [RIAA] said it selected the defendants by employing simple search techniques . . . ."); John Schwartz, *More Lawsuits Filed in Effort to Thwart File Sharing*, N.Y. TIMES, Mar. 24, 2004, http://www.nytimes.com/2004/03/24/technology/24music.html; *see also* EFF, RIAA v. The People: Five Years Later, Sept. 2008, http://www.eff.org/wp/riaa-v-people-years-later (noting that peer-to-peer traffic comprises 45 percent of internet traffic); RIAA Watch, http://sharenomore.blogspot.com (tallying 17,587 individual lawsuits filed as of February 2006, after which the RIAA stopped releasing official numbers).

[95] *See* 17 U.S.C. § 512(h); Kristina Groennings, Note, *Costs and Benefits of the Recording Industry's Litigation Against Individuals*, 20 BERKELEY TECH. L.J. 571, 574 (2005) ("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.").

[96] RIAA v. Verizon Internet Servs., 257 F. Supp. 2d 244 (D.D.C. 2003); RIAA v. Verizon Internet Servs., 240 F. Supp. 2d 24 (D.D.C. 2003); RIAA v. Charter Commc'ns, Inc., ; *see also* Pac. Bell Internet Servs. v. RIAA, No. C03-3560, 2003 WL 22862662 (N.D. Cal. Nov. 26, 2003).

filed suit against several hundred individuals, and sent settlement offers to the rest.[97]

The industry's liberal use of DMCA subpoenas was soon overturned on appeal, however. Based on a technical reading, the appeals court exempted all ordinary internet service providers from the DMCA subpoena provision, claiming that only certain providers (those that actively stored infringing materials on their servers) could be served proper notice under the meaning of the statute.[98] While the decision did not rule out the possibility of acquiring user identities through other means, it removed from the table the most convenient option available.

Stripped of its statutory right to obtain the identities of alleged infringers, the RIAA was left to bargain for access the traditional way. It could petition the courts by filing "John Doe" lawsuits—a process made prohibitively expensive by the refusal of several courts to allow mass filings.[99] In one recent case, the district court further added that ISPs could seek reimbursement for the costs of identifying subscribers and limit the number of requests to 25 per month.[100] Alternatively, the RIAA could contract directly with the ISPs to obtain user information, thereby bypassing the friction and uncertainty of litigation. And in fact, a U.S. deal was recently announced in which participating ISPs would give copyright infringers four warnings before initiating an escalating series of punitive measures.[101] A similar arrangement was reached in Britain, though later abandoned, in which a music label would have offered unrestricted music downloads to an ISP's customers in exchange for the ISP's assistance with enforcing copyrights otherwise.[102]

---

[97] David W. Opderbeck, *Peer-to-Peer Networks, Technological Evolution, and Intellectual Property Reverse Private Attorney General Litigation*, 20 BERKELEY TECH. L.J. 1685, 1705-07 (2005); John Borland, *Record Industry Warns of New Lawsuits*, CNET NEWS.COM, Oct. 17, 2003, http://news.cnet.com/Record-industry-warns-of-new-lawsuits/2100-1027_3-5093078.html.

[98] RIAA v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003); *accord* RIAA v. Charter Commc'ns, Inc., 393 F.3d 771 (8th Cir. 2005).

[99] *See* Opderbeck, *supra* note 97, at 1707–08; Mike Masnick, *RIAA Spent $17.6 Million in Lawsuits . . . to Get $391,000 in Settlements?*, TECHDIRT, July 14, 2010, http://www.techdirt.com/articles/20100713/17400810200.shtml. As a result, the RIAA announced in December 2008 that it was ending its official campaign of mass lawsuits. Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, http://online.wsj.com/article/SB122966038836021137.html.

[100] DigiProtect USA Corp. v. Does 1-240, No. 10-8760, 2011 WL 4444666 (S.D.N.Y. Sept. 26, 2011) (dismissing for lack of personal jurisdiction). *But see* Call of the Wild Movie, LLC v. Smith, 274 F.R.D. 334 (May 12, 2011) (denying individual motions for severance); Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332 (D.D.C. 2011) (denying motions by ISPs to quash mass subpoenas).

[101] David Kravets, *ISPs to Disrupt Internet Access of Copyright Scofflaws*, WIRED.COM, July 7, 2011, http://www.wired.com/threatlevel/2011/07/disrupting-internet-access.

[102] Eric Pfanner, *Universal Music and Virgin Reach a Download Deal*, N.Y. TIMES, June 15, 2009, at B2, *available at* http://www.nytimes.com/2009/06/16/technology/internet/16music.html. That deal has since been eclipsed by a new agreement between Virgin Media and Spotify. David Meyer, *Virgin Media: Spotify Deal Will Bring Down Piracy*, ZDNET UK, July 6, 2011, http://www.zdnet.co.uk/news/networking/2011/07/06/virgin-media-spotify-deal-will-bring-down-piracy-40093328/.

As a policy matter, the question of whether the copyright system needs substantive reform has become highly contentious in recent years, and this is not an attempt to revisit that debate. The point is simply that as long as any part of the copyright system is to remain enforceable, the path of regulation must travel through either anonymity or generativity. The prospect of censuring individual infringers seems oppressive, but the alternative is equally heavy-handed: crippling the technologies that facilitate the exchange of data.

B. Defamation and the Communications Decency Act

More distressing to the public have been acts of cyberbullying. Individuals have been devastated[103] and communities outraged[104] over malicious barbs aired on web forums and social networking sites. Those who have sought to fight back have encountered two hurdles: the internet's architectural protocols do not reliably identify users, and internet intermediaries have no legal incentive to assist, because section 230 of the Communications Decency Act immunizes all "interactive computer services" from civil liability for third-party content.[105]

Many scholars have pointed the finger at section 230, characterizing it as a well-meaning but mistaken relic of the early internet era.[106] 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, they are granted blanket immunity.[107] As a result of that discrepancy, it is exceedingly difficult to expunge defamatory statements

---

[103] *See* Choe Sang-Hun, *South Korea Links Web Slander to Celebrity Suicides*, N.Y. TIMES, Oct. 12, 2008, http://www.nytimes.com/2008/10/12/technology/12iht-kstar.3.16877845.html; Tamara Jones, *A Deadly Web of Deceit*, WASH. POST, Jan. 10, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/09/AR2008010903367.html.

[104] *See* Heather Timmons, *'Any Normal Human Being Would Be Offended'*, N.Y. TIMES INDIA INK, Dec. 6, 2011, http://india.blogs.nytimes.com/2011/12/06/any-normal-human-being-would-be-offended/; A.G. Sulzberger, *In Small Towns, Gossip Moves to the Web, and Turns Vicious*, N.Y. TIMES, Sept. 19, 2011, at A1, http://www.nytimes.com/2011/09/20/us/small-town-gossip-moves-to-the-web-anonymous-and-vicious.html; Tamar Lewin, *On Formspring, an E-Vite to Teenage Insults*, N.Y. TIMES, May 5, 2010, http://www.nytimes.com/2010/05/06/us/06formspring.html.

[105] *See* 47 U.S.C. § 230(c)(1); Doe v. GTE Corp., 347 F.3d 655, 659–70 (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)"); Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383 (2009) (unavailability of easy remedies has created a market for reputation defense services); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 159 (2007).

[106] *See* Kahn, *supra* note 51, at 189-93 & n.86 (collecting commentary).

[107] *See* H. Brian Holland, *In Defense of Online Intermediary Liability: Facilitating Communities of Modified Exceptionalism*, 56 KAN. L. REV. 369, 374–75 (2008); Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 197–98 (2006); Zittrain, *Online Gatekeeping*, *supra* note 58, at 257–63; 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); Paul Ehrlich, Note, *Communications Decency Act § 230*, 17 BERKELEY TECH. L.J. 401, 404–05 & n.29 (2002)

from the record once they are published on the internet—a problem that is further compounded by the internet's broad reach. Nevertheless, the courts have consistently upheld that interpretation as a faithful reflection of Congressional intent.[108]

But it is not clear that section 230 has outlived its usefulness. The motivation behind section 230 was to protect the generative potential of the internet. Congress was concerned that, in offering new services, online providers were trapped between needing to remain family-friendly, and being exposed to crippling liability whenever such efforts fell short. Congress therefore made a deliberate choice to prioritize the development of internet services over the enforcement of intermediary liability. The gambit has paid off handsomely: countless innovative offerings have thrived in large part because of that immunity.

Narrowing the scope of section 230 would certainly aid in deterring defamation, but it would do so by forcing intermediaries to become more circumspect about their services. Few entities, if any, would be able to absorb the cost of indemnifying user-generated content—and even those that could would want to minimize it. Any reduction in defamation would be purchased at direct cost to generative functionality, rather than by encouraging better behavior among individual users.

If we do not want to stunt the availability of user-content services, then the only alternative is to use identification measures to reinstate offline laws and norms. The courts have been amenable to that approach, issuing orders to assist victims in identifying their antagonizers as long as good cause is shown and due process is satisfied.[109] But those efforts have not been wholly effective, foiled by simple workarounds such as the use of public computers, shared network connections, and proxy servers.[110] As a result, some regulators have sought to take even more proactive steps such as imposing "real-name" requirements as a preemptive measure. Among nations, the most visible efforts have come from China and South Korea,[111] and in the private sector, from social network site

---

[108] *See* Grace v. eBay Inc., 16 Cal. Rptr. 3d 192, 198–99 (Cal. Ct. App. 2004), *dismissed by* 101 P.3d 509 (Cal. 2004); Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 153–54 (Cal. Ct. App. 2004), *rev'd*, 51 Cal. Rptr. 3d 55 (Cal. 2006).

[109] *See generally* 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 (2009); Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM. L. & POL'Y 405 (2003); *see also* Cohen v. Google, 887 N.Y.S.2d 424 (N.Y. Sup. Ct. Aug. 17, 2009) (slip op.); Amir Efrati, Subpoenas Allowed in AutoAdmit Suit, Wall St. J., Jan. 30, 2008, http://blogs.wsj.com/law/2008/01/30/subpoena-allowed-in-autoadmit-suit/.

[110] *See* David Margolick, *Slimed Online*, PORTFOLIO.COM, Feb. 11, 2009, http://www.portfolio.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying (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").

[111] *See* Chris Buckley, *China Seeks to Tether the Microblog Tiger*, REUTERS, Sept. 16, 2011, http://www.reuters.com/article/2011/09/16/us-china-internet-idUSTRE78F04D20110916;
Jonathan Ansfield, *China Web Sites Seeking Users' Names*, N.Y. TIMES, Sept. 5, 2009, at A4,

operators such as Facebook and Google.[112] Those policies have drawn heavy criticism, for reasons ranging from wrongful enforcement and loss of privacy to physical endangerment of activists and dissidents,[113] but they may point the best way to the "future of the internet" that Zittrain and others seek.

While some would argue that anonymity should not be compromised at any cost, attempting to save anonymity on an unconditional basis may turn out to be a pyrrhic victory. By making anonymity inviolate, we paint ourselves into a corner where the only way to regulate offensive speech is to motivate intermediaries to reassert editorial control over user content. Already, many websites have voluntarily responded by hiding user comments or disabling the functionality entirely, demonstrating that the generative cost of anonymity is non-negligible. That trend would quickly accelerate if section 230 were sacrificed too. By making it costly for technological platforms to support user expression, we risk reverting to a world in which all speech is mediated by large publishers—and consequently one in which anonymity is greatly limited.

C. Age Verification and the Child Online Protection Act

Meanwhile, when Congress sought to shield minors from online pornography, it focused from the outset on regulating anonymity. Both the Communications Decency Act ("CDA")[114] and the Child Online Protection Act ("COPA")[115] were attempts to require distributors of online pornography to identify users by age. The Supreme Court was skeptical of applying an identity-based approach to the internet, however, and rebuffed those efforts.

The CDA sought to reinstate the offline norm of requiring proof of proper age in order to obtain sexually explicit materials. The statute imposed criminal penalties on anyone who used an interactive computer service to transmit obscene, indecent, or patently offensive materials to persons under 18 years of

---

http://www.nytimes.com/2009/09/06/world/asia/06chinanet.html; 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, at 43 (2009). *But see* ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997).

[112] *See* Kahn, *supra* note 51.

[113] *See* Eric Pfanner, *Naming Names on the Internet*, N.Y. TIMES, Sept. 4, 2011, http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html; Alexis Madrigal, *Why Facebook and Google's Concept of 'Real Names' is Revolutionary*, THE ATLANTIC, Aug. 5, 2011, http://www.theatlantic.com/technology/archive/2011/08/why-facebook-and-googles-concept-of-real-names-is-revolutionary/243171/; Audrey Watters, *No Pseudonyms Allowed: Is Google Plus's Real Name Policy a Good Idea?*, READWRITEWEB, July 12, 2011, http://www.nytimes.com/external/readwriteweb/2011/07/12/12readwriteweb-no-pseudonyms-allowed-is-google-pluss-real-na-316.html; Tini Tran, *Activist Michael Anti Furious He Lost Facebook Account—While Zuckerberg's Dog Has Own Page*, HUFFINGTON POST, Mar. 8, 2011, http://www.huffingtonpost.com/2011/03/08/michael-anti-facebook_n_832771.html

[114] Telecommunications Act of 1996 (Communications Decency Act), Pub. L. No. 104-104, § 502, 110 Stat. 133–34 (1996), *invalidated by* Reno v. ACLU (*CDA II*), 521 U.S. 844 (1997).

[115] Pub. L. No. 105-277, 1403, 112 Stat. 2681-736 to 2681-739 (1998) (codified at 47 U.S.C. § 231 (2006)), *invalidated by* ACLU v. Mukasey (*COPA VII*), 534 F.3d 181 (3d Cir. 2008).

age. But the true substance 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.[116]

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."[117] Because the coverage was overbroad, and the sanctions so severe, the Court feared that the statute would unintentionally silence constitutionally protected speech.[118]

More importantly, though, the Court concluded that there was no good way to authenticate the ages of internet users.[119] 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."[120]

By the time Congress redrafted the legislation and enacted it as COPA, the culture of anonymity had become so embedded in the internet that the Court was loath to uproot it. The Court acknowledged that COPA successfully fixed the problems of statutory scope that had plagued the CDA.[121] Yet the Court

---

[116] *CDA II*, 521 U.S. at 860-61 & n.26. *But see* Ashcroft v. ACLU (*COPA V*), 542 U.S. 656, 674 (2004) (Stevens, J., concurring) (complaining that affirmative defenses "cannot guarantee freedom from prosecution," and that speakers 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, using similar language to protect those who, "in good faith, ha[ve] 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." Ashcroft v. ACLU (*COPA III*), 535 U.S. 564, 570 (2002) (quoting 47 U.S.C. §231(c)(1)). *But see* Lessig & Resnick, (arguing that the affirmative defenses in COPA were sufficiently broader than those contained in the CDA).

[117] *Id.* at 871 & n.35, 877.

[118] *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 the CDA "is a criminal statute. . . . Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection.").

[119] *Id.* at 876-77.

[120] *Id.* at 881-82.

[121] *See COPA III*, 535 U.S. at 578-79; *COPA V*, 542 U.S. at 665 (rejecting the lower court's finding of unconstitutionality based on statutory grounds); *see also id.* at 660 ("In enacting COPA, Congress gave consideration to our earlier decisions on this subject, in particular the decision in Reno v. ACLU."); *id.* at 690 (2004) (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; 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 17 years. *See COPA III*, 535 U.S. at 569-70.

invalidated COPA anyway, on the basis that there now were less restrictive alternatives than identification. According to the Court, new methods such as filtering software were preferable precisely because they did not require adults to reveal identifying information in order to gain access to explicit materials.[122] That explanation seemed to pretend that something could be gained for nothing, without acknowledging the generative tradeoff: by rejecting the approaches that relied on identification, the Court was naturally forced to turn to approaches that would restrict functionality.

In a perfect world, of course, age verification systems and filtering systems would be indistinguishable: both would correctly distinguish adults from minors, and separate explicit content from safe content. But both systems are inevitably imperfect; the difference is in how they fail. When an age verification system errs, it is because a child is able to masquerade as an adult using false credentials.[123] Seldom is the case where an adult is denied access to a bar or club upon showing proof of age. On the other hand, when a filtering system errs, it interferes with the internet's normal functionality. 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.

To the Court, the harm of overfiltering seemed lesser because it was a "selective" restriction, visited only upon those children whose parents opt in and choose to install the software.[124] Anyone not using the filtering software would be unaffected. On the other hand, the Court claimed, COPA was a "universal" restriction applied at the source. All adults would be affected by having to disclose identifying information that otherwise could remain secret. But the opt-in/opt-out distinction is misleading. Although age verification can be managed centrally at the server layer, it too can be configured as software installed locally on end-user devices.[125] COPA contemplated and afforded immunity for both methods.

Furthermore, the Court's calculation of restrictiveness should have compared apples to apples. For children, an error in an age verification system allows them to see more than they should—like sneaking a peek at a pinup magazine found in the garage. By contrast, an error in a filtering system results in

---

[122] *COPA V*, 542 U.S. at 667-68 ("Under 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.").

[123] The Court expressed some concern that 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 it should have been even more critical of opt-in filtering schemes, which allow all children to pass as adults by default.

[124] *Id.* at 667 ("[Filters] impose selective restrictions on speech at the receiving end, not universal restrictions at the source.").

[125] 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* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 416–22 (1999); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 517–19 (1999).

a severe burden: innocuous content that should be viewable is censored for no reason other than overzealousness. For adults, meanwhile, the only difference is that the age verification system requires an extra validating step. Even if identification has to be sent to the provider—which is not necessarily the case—that process is a well-established social ritual, even in the context of sensitive speech. Faces are observed and IDs are checked when entering gentlemen's clubs, and when purchasing adult magazines. Certainly, care must be taken to prevent unwarranted disclosures,[126] but the use of identity as a validating credential is not presumptively harmful.

The real issue at stake was whether content providers could be required to flag their own content, or whether that task would be left entirely to third parties. One concern with placing the burden on content providers was that the threat of liability might deter them from exercising protected speech. But the Court did not object to COPA's scope of coverage as vague or overbroad, and there was already some precedent for developing workable guidelines in other contexts such as print publications and broadcast media. The other concern was that compliance with COPA might be inconsistent, particularly by foreign entities, and that filtering software would therefore be more effective since it does not rely on extrinsic data. But considering effectiveness before restrictiveness places the cart before the horse. The risk of overfiltering should have been seen as far more restrictive than the risk of undercompliance.

If we abandon identification as a regulatory tool, then there is only one direction in which to travel: further encroachments on technological functionality. Since the demise of COPA, advocates have been pushing 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.[127] Such a proposal could successfully screen content for minors without forcing adults to reveal any identifying information. But the cost to generativity would be high.[128] Requiring explicit content to remain technologically segregated at all times would make it difficult to create or do anything online that might blur or cross the lines.[129]

---

[126] *See generally* Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710). *But see COPA V*, 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)

[127] The first step in 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, http://www.wired.com/epicenter/2011/03/icann-approves-xxx. Other methods of segregating content have been proposed as well. *See, e.g.*, Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 B.Y.U. L. REV. 1417 (2007) (recommending the use of separate ports).

[128] *See* ZITTRAIN, FUTURE OF THE INTERNET, *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).

[129] 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-

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 continue to consume pornography anonymously—but perhaps it would be simpler just to use identification.

D. Spam and the CAN-SPAM Act

With spam, the identity-centric approach has been least controversial. In 2003, Congress passed the CAN-SPAM Act, which neatly divided the problem into two parts: 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.[130] In the civil section, Congress mandated an opt-out mechanism that would allow recipients to refuse future messages;[131] senders were required to identify themselves accurately and conspicuously so that recipients would not be misled when choosing to opt out. The criminal section, then, was directed to the remaining parties who would ignore the civil regulations by hiding behind false mail headers, open relays, zombie computers, and other anonymizing means.[132] Framed in that manner, it is not surprising that the identification requirements went unchallenged: the affected parties were either legitimate companies unwilling to be associated with anonymous spam, or illegitimate groups with little interest in petitioning the courts of law.

The main criticism of CAN-SPAM has been that it is anemic and ineffective. Much of that discussion has focused on criticizing the opt-out framework as being too lenient,[133] and by extension the federal preemption provision that prevents individual states from adopting stricter, opt-in schemes.[134]

---

releases/neustar-announces-significant-wholesale-price-reductions-for-kidsus-registrars-58226767.html.

[130] *See* 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."); Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 5 ¶¶ 66-72 (2005).

[131] CAN-SPAM Act of 2003, Pub. L. No. 108-187, § 5, 117 Stat. 2699, 2706 (codified at 15 U.S.C. § 7704). *See also* FEDERAL TRADE COMMISSION, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT: A REPORT TO CONGRESS 8 (2005), http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf ("CAN-SPAM has established a framework for lawful commercial email, and legitimate marketers are largely complying with it . . . .").

[132] CAN-SPAM Act § 4, 117 Stat. at 2703 (codified at 18 U.S.C. § 1037 and 15 U.S.C. § 7703);

[133] cite various proposals – SPAM Act, REDUCE Spam Act, RID Spam Act, Anti-Spam Act; see also EU Directive, South Korea law, Australia?. Critics of preemption provision also point to California? Washington?

[134] *See, e.g.*, Katherine Wong, *The Future of Spam Litigation After Omega World Travel v. Mummagraphics*, 20 HARV. J.L. & TECH. 459, 469, 473 (2007) (arguing that state experimentation would be more effective at reducing spam than a uniform, national liability standard).

Such debates are frivolous, however, since most spam comes from sources that would refuse to comply either way.[135] The merits of a civil regulation cannot be evaluated based on harms that are being committed by anonymous actors.

If spam is to be curbed, it is the criminal provisions that are key. Spam activities are conducted almost entirely through a small number of "botnets"—vast networks of computers owned and operated by legitimate users but covertly controlled by spammers. One recent study found that just eight botnets were responsible for more than 90 percent of detected spam.[136] In recent years, takedowns of major botnets such as Rustock,[137] Mega-D,[138] and McColo,[139] have led to meaningful dips in spam activity, demonstrating that shutting down the botnets is the right strategy. But those reprieves have been temporary, as operators remaining at large have been able to resurrect and regrow their networks, or take over territory left behind by others. Because complex computer code inevitably contains errors, and sophisticated botnet technology is designed to perpetuate itself even when initial vulnerabilities are patched, the likelihood of eradicating infiltrations through technological means is slim.[140] More permanent success depends on tracking down and prosecuting those botnet operators. 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.[141] Adding other avenues of regulating online anonymity would further expedite the elimination of spam.

---

[135] Cite study re how much spam was compliant with CAN-SPAM

[136] M86 SECURITY LABS, SECURITY LABS REPORT: JANUARY – JUNE 2011 RECAP 6-7, July 2011, http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_1h2011.pdf.

[137] *Id.* at 21; Nick Wingfield, *Spam Network Shut Down*, WALL ST. J., Mar. 18, 2011, http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html.

[138] Joe Barrett, *Accused Spam King to Be Arraigned*, WALL ST. J., Dec. 3, 2010, http://online.wsj.com/article/SB10001424052748704377004575651232273336218.html; Jeremy Kirk, *FireEye Moves Quickly to Quash Mega-D Botnet*, REUTERS, Nov. 10, 2009, http://www.reuters.com/article/2009/11/10/urnidgns852573c4006938800025766a-idUS343920408120091110; M86 SECURITY LABS, SECURITY LABS REPORT: JULY – DECEMBER 2010 RECAP 9, Feb. 2011, http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_2h2010.pdf.

[139] Brian Krebs, *Major Source of Online Scams and Spams Knocked Offline*, WASH. POST, Nov. 11, 2008, http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html; MARSHAL8E6 TRACELABS, MARSHAL8E6 SECURITY THREATS: EMAIL AND WEB THREATS, Jan. 2009, http://www.m86security.com/newsimages/trace/Marshal8e6_TRACE_Report_Jan2009.pdf.

[140] *See, e.g.*, Brian Krebs, *'Stuxnet' Worm Far More Sophisticated than Previously Thought*, KREBS ON SECURITY, Sept. 14, 2010, http://krebsonsecurity.com/2010/09/stuxnet-worm-far-more-sophisticated-than-previously-thought/; John Markoff, *Computer Experts Unite to Hunt Worm*, N.Y. TIMES, Mar. 18, 2009, at A17, http://www.nytimes.com/2009/03/19/technology/19worm.html.

[141] See Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY L.J. 1037 (2010); John Markoff, *Study Sees Way to Win Spam Fight*, N.Y. TIMES, May 19, 2011, at B1, http://www.nytimes.com/2011/05/20/technology/20spam.html.

In the meantime, we should be highly skeptical of proposals that seek to modify email technology to fit the problem of spam. Economics-minded commentators have pointed out that the profitability of spam depends on the zero marginal cost of email,[142] and therefore have proposed a range of solutions to inject artificial cost into the equation. 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.[143] Making people pay for email might be problematical in the immediate term because the additional cost would be absorbed by botnet victims rather than spammers. 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. It would be a giant symbolic 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.

IV. UNTANGLING THE DOCTRINE OF ANONYMITY

Our inconsistent attitudes toward online anonymity can be explained in part by the fact that the legal doctrine of anonymity has been waylaid by a handful of errant judicial statements. In particular, the notion of a "right" to anonymity has been revitalized in recent years by the Supreme Court's 1995 decision in McIntyre v. Ohio Elections Commission.[144] Those interested in championing such a right have seized on tantalizing excerpts from *McIntyre* and other outlier cases such as Talley v. California[145] to theorize that the Court established a limited right to anonymity that is especially potent for "core" political speech, and that is potentially extensible to other areas of speech as well.[146] But that portrait depends on a stilted view of the case law, with the heaviest lifting done by the most

---

[142] *See, e.g.*, 45 HARV. J. LEGIS. 165, 169 (2008); Accountable Net, 9 Va. J.L. & Tech. ¶ 18.
[143] *See* Bambauer, *supra* note 130, at ¶¶ 164-69; Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319, 346 (2005).
[144] 514 U.S. 334 (1995).
[145] 362 U.S. 60 (1960).
[146] *See, e.g.*, Calvert et al., *supra* note 109, at 12 ("It is important to note that *Talley* and *McIntyre* did not create an absolute right to engage in an anonymous speech, but rather the cases are cabined by their unique facts and political contexts."); Horn, *supra* note 13; Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2 (2002) (citing examples where "the Court has recognized a right to anonymity that is broader than simply political anonymity"); Jennifer B. Wieland, Note, *Death of Publius: Toward a World Without Anonymous Speech*, 17 J. L. & POLITICS 589 (2001); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) (claiming that the Court's cases "suggest the glimmerings of judicial recognition of a broad right of anonymity extending to all of the constitutive activities of communication").

sparsely reasoned cases. It is hardly an accident that the most strident rhetoric is found in the cases with the least evidence of actual harm.

In *Talley*, the majority's oft-cited colloquy about the "important role" that anonymity has "sometimes" played "in the progress of mankind"[147] was not a declaration of right, but instead an eloquent but vain effort to paper over a conspicuous gap in the record regarding actual harm. The city of Los Angeles had passed an ordinance requiring every handbill to print the true names and addresses of its authors and distributors. The Court stated baldly that "[t]here can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[148] No further elaboration was given, not even to speculate who might be deterred or why.[149] The dissenting opinion rightly objected that the record lacked any evidence to support a claim of deterrent effect, and that such evidence should have been demanded before invalidating the statute.[150] Invoking the historical contributions of anonymity was simply a last-ditch effort to add grist to an empty factual record.

That *McIntyre* escalated the rhetoric was telling. The statute at issue there was like the one in *Talley,* in that it required proper identification to be printed on handbills, except that its scope was limited to political literature. After quoting extensively from *Talley*, the majority added that anonymous pamphleteering is an "honorable tradition of advocacy and of dissent"[151] and that "an author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment."[152] But again when it came to identifying the actual harm posed by the statute, the Court was curiously silent. As a factual matter, the Court was unable to claim that Mrs. McIntyre—who had distributed her leaflets in person, and had signed her name to some leaflets but not others—would have been deterred in any way by having to comply with the statute. Nor did the Court claim that other dissenting voices were being suppressed by the statute. Instead, the majority simply asserted that the statute was a content-based regulation of political speech, and reflexively applied strict scrutiny without explaining precisely how the regulation—one that admittedly "applie[d] evenhandedly to advocates of different viewpoints"[153]—harmed the free exercise of speech.

---

[147] *See* 362 U.S. at 64-65.
[148] *Id.* at 64.
[149] The Court mentioned in passing that the NAACP cases had held that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance." *Id.* at 65. But the NAACP cases were materially different, as explained later, because those were cases in which the government sought to use identification to attack a specific viewpoint.
[150] *See id.* at 69 (Clark, J., dissenting) ("The record is barren of any claim, much less proof, that [Talley] will suffer any injury whatever by identifying the handbill with his name. . . . Talley makes no showing whatever to support his contention that a restraint upon his freedom of speech will result from the enforcement of the ordinance. The existence of such a restraint is necessary before we can strike the ordinance down.").
[151] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).
[152] *Id.* at 342.
[153] *Id.* at 345.

If we set aside *Talley* and *McIntyre*, however, the remaining cases tell a different story. The Court's rulings can be grouped into two classes: those involving prophylactic measures that request identification before harms occur, and those involving investigative measures that apply after the fact. Far from upholding anonymity as an individual right, both contexts reveal that identification requirements have been presumptively favored unless a specific showing of harm can be provided to rebut that presumption. The underlying assumption is that the state should always have the *capacity* to force identification—just as the state always has the capacity to conduct a physical search—even if that power is then subject to legal and prudential constraints when the risk of harm is too great. The Court's case law decidedly rejects the notion of a generalized right to anonymity.

A. Prophylactic Measures

As an abstract matter, the claim to anonymity ought to be strongest at the outset when it has not yet been exercised or caused any harm. But even there the Court's embrace of anonymity has been lukewarm at best. Some statutory identification requirements have been invalidated, but many others have been upheld, leading some observers to conclude that the jurisprudence of anonymity is "murky."[154] The standard of review has remained frustratingly indeterminate,[155] and even the Court has admitted that it lacks a good grasp of what the dividing line is.[156]

The best way to organize these cases, it seems, is to look past the loss of anonymity and to focus on the nature of the harms at stake, i.e., potential deterrence of speech. In fact, it is possible to explain the disparity in outcomes by observing that not all deterrence is alike. Some forms are far less troubling than others, and so simply lumping them all together as "deterrence" is unhelpful. Cataloging the different forms of deterrence provides a better map to the Court's intuitions on anonymity—and also exposes where the Court has occasionally gone astray.

---

[154] *See* Lidsky & Cotter, *supra* note 10, at 1541.

[155] *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 164 (2002) (declaring it "unnecessary" to decide what standard of review should be used to assess the constitutionality of the registration requirement in question). In another instance, Justice Thomas wrote separately to complain that the Court should have applied strict scrutiny, Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 206 (1999) ("*Buckley II*") (Thomas, J., concurring), even though the majority insisted that its opinion was "entirely in keeping" with that heightened standard, *id.* at 192 n.12, 204 (majority opinion).

[156] *See Buckley II*, 525 U.S. at 192 (stating that there is "no litmus-paper test" and "no substitute for the hard judgments that must be made").

1. Suppression Through Identification

The simplest cases have been those in which the government has looked to use identification to directly suppress speech that it finds undesirable. Singling out a viewpoint for censorship is the classic case of oppressive government and is heavily disfavored under First Amendment jurisprudence. That said, the Court has consistently left room for exception, acknowledging that some speech is so harmful that precautionary suppression is justified.

The question presented in early handbill cases such as Lovell v. City of Griffin,[157] Schneider v. State,[158] and Cantwell v. Connecticut,[159] was whether local governments could control the distribution of all handbills, pamphlets, and similar items by requiring an express license from a governmental authority. The governments offered various neutral justifications—such as protecting citizens from fraudulent solicitations, or preventing litter in the streets—but one purpose of such ordinances was to prevent the distribution of religious literature by unpopular sects like the Jehovah's Witnesses.[160] In striking down those ordinances, the Court stated that municipalities could not "require all who wish to disseminate ideas to present them first to police authorities for their consideration and approval."[161] Such broad, discretionary review would "restore the system of license and censorship in its baldest form,"[162] and was precisely the sort of arbitrary oversight that the First Amendment had been established to protect against.

With the same breath, however, the Court indicated that its rule was not absolute, and that identification could be used to block certain classes of handbills, such as those that were obscene or that were solicitations for money. "Without a doubt," the Court declared in *Cantwell*, "a state may protect its citizens from fraudulent solicitation by requiring a stranger in the community, before permitting him publicly to solicit funds for any purpose, to establish his

---

[157] 303 U.S. 444 (1938).
[158] 308 U.S. 147 (1939).
[159] 310 U.S. 296 (1940).
[160] *See, e.g.*, Niemotko v. Maryland, 340 U.S. 268, 272 (1951) ("The conclusion is inescapable that the use of the park was denied because of the City Council's dislike for or disagreement with the Witnesses or their views."); *cf.* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 645 (1994) ("Our cases have recognized that even a regulation neutral on its face may be content based if its manifest purpose is to regulate speech because of the message it conveys."). *But see* City Council of Los Angeles v. Taxpayers for Vincent, 466 U.S. 789, 804-05 (1984) (upholding a similar interest in "advanc[ing] esthetic values" because "there is not even a hint of bias or censorship in the City's enactment or enforcement of th[e] ordinance").
[161] *Schneider*, 308 U.S. at 164; *see also Cantwell*, 310 U.S. at 307 ("But to condition the solicitation of aid for the perpetuation of religious views or systems upon a license, the grant of which rests in the exercise of a determination by state authority as to what is a religious cause, is to lay a forbidden burden upon the exercise of liberty protected by the Constitution."); *Lovell*, 303 U.S. at 451 ("The struggle for the freedom of the press was primarily directed against the power of the licensor.").
[162] *Lovell*, 303 U.S. at 452.

identity and his authority to act for the cause which he purports to represent."[163] Similarly, the *Schneider* Court made clear that its holding did not apply to "commercial soliciting and canvassing,"[164] and the *Lovell* Court indicated that it would reach a different conclusion if the ordinance were limited to literature that was "obscene or offensive to public morals or that advocates unlawful conduct."[165] Such exceptions were deemed acceptable because the suppression was of proscribable content, unprotected by the Constitution.[166]

If the Court felt obliged to protect the ability of religious groups to distribute proselytizing literature, it was even more sympathetic to protecting black activists from hateful retribution during the Civil Rights Movement. In two companion cases, NAACP v. Alabama ex rel. Patterson[167] and Bates v. City of Little Rock,[168] the Southern states attempted to oust the NAACP through intimidation by forcing the group to reveal its membership list. The Court credited evidence that "on past occasions revelation of the identity of [the NAACP's] rank-and-file members ha[d] exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility."[169] Not surprisingly, the Court concluded that the Southern states lacked a legitimate interest in obtaining those membership lists.

But the NAACP cases should not be misunderstood as immunizing all organizations from having to reveal the names of their members, particularly when the organization is considered to be violent or otherwise dangerous. For example, the Court distinguished an earlier case, Bryant v. Zimmerman,[170] in which the Court had upheld a New York registration statute as applied to a local chapter of the Ku Klux Klan. Because the organization was responsible for committing "acts of unlawful intimidation and violence,"[171] rather than being

---

[163] *Cantwell*, 310 U.S. at 306; *see also Martin v. City of Struthers*, 319 U.S. 141, 148 (1943) ("A city can punish those who call at a home in defiance of the previously expressed will of the occupant and, in addition, can, by identification devices, control the abuse of the privilege by criminals posing as canvassers."); *Murdock v. Pennsylvania*, 319 U.S. 105, 116 (1943) (suggesting that it would be permissible to have "merely a registration ordinance calling for an identification of the solicitors so as to give the authorities some basis for investigating strangers coming into the community").

[164] *Schneider*, 308 U.S. at 165 ("We are not to be taken as holding that commercial soliciting and canvassing may not be subjected to such regulation as the ordinance requires.").

[165] *Lovell*, 303 U.S. at 451.

[166] *See* Brown v. Entm't Merchants Ass'n, 564 U.S. ___ (2011); R.A.V. v. City of St. Paul, 505 U.S. 377, 382-84, 388 (1992) ("When the basis for the content discrimination consists entirely of the very reason the entire class of speech at issue is proscribable, no significant danger of idea or viewpoint discrimination exists."); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 372 (1995) (Scalia, J., dissenting) ("There is no doubt, for example, that laws against libel and obscenity do not violate 'the freedom of speech' to which the First Amendment refers.").

[167] 357 U.S. 449 (1958).

[168] 361 U.S. 516 (1960).

[169] *NAACP*, 357 U.S. at 462; *see also Bates*, 361 U.S. at 523-24 ("There was substantial uncontroverted evidence that public identification of persons in the community as members of the organizations had been followed by harassment and threats of bodily harm.").

[170] 278 U.S. 63 (1928).

[171] *NAACP*, 357 U.S. at 465.

subjected to the same, the *Bryant* Court ruled that the right of free association must "yield to the rightful exertion of the police power."[172]

Likewise, in a case decided contemporaneously with *Bates*, during the height of McCarthyism, the Court affirmed an executive order requiring the Communist Party to register and disclose a roster of its rank-and-file members.[173] The Court acknowledged the severe consequences that could attach for both the organization and its members: tax exemptions could be denied, use of mail and broadcast services could be restricted, and members could be disqualified from obtaining passports and from certain employment opportunities[174]—not to mention the attendant "private community pressures" that the Court had found so offensive in the NAACP cases.[175] Nevertheless, the Court held that those individual harms were trumped by "the magnitude of the public interests which the registration and disclosure provisions are designed to protect," namely "to prevent the world-wide Communist conspiracy from accomplishing its purpose in this country."[176]

In those latter examples, the Court allowed the government to use identification measures to single out the KKK and the Communist Party because their messages and actions were sufficiently dangerous that deterrence was appropriate.[177] Doing so was equivalent to restricting obscene or fraudulent handbills—content that is so offensive that removing it from the public sphere causes no cognizable harm. Although the Court eventually recanted its views on communism, it was not until two decades later when fears of a communist takeover had subsided and no longer seemed menacing.[178] Without a doubt, such cases are rare exceptions to the rule that efforts by the government to identify and suppress specific viewpoints are invalid. Nevertheless, they demonstrate that even in the most speech-protective context, the protection of anonymity yields when the need is sufficiently great.

---

[172] *Bryant*, 278 U.S. at 72; *see also* Church of the Am. Knights of the Ku Klux Klan v. Kerik, 356 F.3d 197 (2d Cir. 2004) (upholding anti-mask statute as applied to the KKK); Hernandez v. Superintendent, 800 F. Supp. 1344 (E.D. Va. 1992) (same).

[173] Communist Party of the U.S. v. Subversive Activities Control Bd., 367 U.S. 1 (1961); *see also* Barenblatt v. United States, 360 U.S. 109, 126 (1959) (individual may be compelled to disclose his membership in the Communist Party).

[174] *Communist Party*, 367 U.S. at 15-18, 70-71.

[175] *See NAACP*, 357 U.S. at 463 ("It is not sufficient to answer . . . that whatever repressive effect compulsory disclosure of names of petitioner's members may have . . . follows not from state action but from private community pressures. The crucial factor is the interplay of governmental and private action, for it is only after the initial exertion of state power represented by the production order that private action takes hold.").

[176] *Communist Party*, 367 U.S. at 93.

[177] *Cf. Constitutional Right to Anonymity*, *supra* note 32, at 1124 (noting that, to the extent that the right to anonymity derives from the First Amendment, "in those circumstances in which a speaker could constitutionally be silenced by direct governmental action, he could also be silenced by a disclosure provision.").

[178] *See* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 95 (1982) (noting that the government's interest in identification was reduced "because minor party candidates are unlikely to win elections").

2. A Modicum of Self-Restraint

Where the government's imposition of an identification requirement is neutral, the analysis becomes more complex. No longer can the government be faulted for actively blocking content from reaching the public domain. Instead, any deterrence of speech must be attributed to self-censorship, i.e., refusal on the part of the citizen to comply with the neutral regulation. Self-censorship might occur for an assortment of reasons, including (1) fear of retaliation, (2) inconvenience or lack of forethought, and (3) principled objection to the act of identification. Because those reasons are so different, viewing the Court's cases without that lens makes them appear scattershot.

Cases in the first set are the most concerning because a credible threat of retaliation is as potent as direct viewpoint discrimination. Strict scrutiny is appropriate in that context to prevent the government from using indirect means to commit repressive censorship that would be intolerable if it were effectuated directly. On the other hand, cases in the other two sets do not raise the same concerns. To be sure, some spontaneous speech may be curbed, and some speech may be voluntarily refused as an act of protest. But a regulation of spontaneous speech is a regulation of time, place, or manner; it is not a restriction of content. And when the only reason for refusal is one's conscience, that provides even less basis for elevating the standard of review. Ordinarily when one refuses to provide identification, the result is a loss of the associated privilege (e.g., driving, voting, hunting, borrowing books, purchasing alcohol, marching in a parade), not invalidation of the statute.

That framework is intuitive in straightforward cases involving only one type of deterrence, such as Shelton v. Tucker,[179] United States v. Harriss,[180] and Thomas v. Collins.[181] In *Shelton*, the Court invalidated an identification requirement that was facially nondiscriminatory but that seemed ripe for improper retaliation as applied. Arkansas had enacted a statute requiring its public school teachers to disclose all organizational memberships before being renewed for employment each year. The NAACP membership list cases, which had been decided just a few terms earlier, lay heavy on the Court's mind. But this time, Arkansas had cleverly tied its request to the seemingly legitimate interest of ensuring the character and fitness of its teachers, and so the Court conceded that the NAACP cases were not dispositive.[182] Nevertheless, the majority remained aware of the political reality that the state would likely retaliate against individual teachers who were discovered to be members of the NAACP. It observed that the

[179] 364 U.S. 479 (1960).
[180] 347 U.S. 612 (1954).
[181] 323 U.S. 516 (1945).
[182] *See Shelton*, 364 U.S. at 485 ("This controversy is thus not of a pattern with such cases as N.A.A.C.P. v. Alabama, 357 U.S. 449, and Bates v. Little Rock, 361 U.S. 516 . . . [where] there was no substantially relevant correlation between the governmental interest asserted and the State's effort to compel disclosure of the membership lists involved."); *id.* at 490 (Frankfurter, J., dissenting); *id.* at 498 (Harlan, J., dissenting).

state could in "any year terminate the teacher's employment without bringing charges, without notice, without a hearing, without affording an opportunity to explain," which therefore placed constant and heavy "pressure upon a teacher to avoid any ties which might displease those who control his professional destiny."[183] Although the dissenting justices protested that the statute had not yet been discriminatorily administered, and that there would be time enough to hold the application of the statute unconstitutional if such use were made,[184] the majority was not willing to wait for retaliation that was so foreseeable.

On the other end of the spectrum, where it is clear that the only basis for complaint is a simple aversion to identification, the Court has recognized the absurdity of permitting such a specious demand for anonymity to trump an otherwise reasonable regulation. In *Harriss*, for example, the Court was dismissive of the claim that professional lobbyists would be deterred by having to submit periodic disclosures—including relevant names, addresses, and dollar sums—of the money they received and expended in the pursuit of influencing federal legislation. According to the Court, the statute did not prevent anyone from engaging in lobbying activities, but "merely provided for a modicum of information from those who for hire attempt to influence legislation."[185] The only restraint was "at most, an indirect one resulting from self-censorship," which the Court found to be "too remote" to require striking down the statute.[186] Lobbyists might dislike having to disclose their financial statements, but few were likely to quit a business so lucrative, even if the disclosures were political in nature.

Finally, in *Thomas*, the Court fixated on the deterrence of spontaneous speech.[187] Texas had passed a statute requiring labor organizers to register and obtain an organizer's card before soliciting members for labor unions. The Court objected to that registration requirement primarily because it would exert pressure on unregistered individuals to remain silent or risk prosecution under the statute. The fact that registration was easy or routine was irrelevant; because the statute applied broadly to all contexts, the Court worried that its proscriptions would hang over every conversation at every moment:

---

[183] *Id.* at 486 (majority opinion).

[184] *Id.* at 496 (Frankfurter, J., dissenting); *id.* at 497 (Harlan, J., dissenting).

[185] *Harriss*, 347 U.S. at 625; *cf.* Heller v. District of Columbia, 698 F. Supp. 2d 179, 190 (D.D.C. 2010) ("[B]ecause registration requirements only regulate, rather than prohibit[], the possession of firearms, they do not infringe the Second Amendment right.").

[186] *Harriss*, 347 U.S. at 626.

[187] Although labor unions were disfavored at the time, the Court accepted the state's argument that the registration requirement was only "ministerial, not discretionary," and not a device to dissuade the activities in question. *See Thomas*, 323 U.S. at 538, 541 & n.24 ("[W]e have no occasion to consider whether the restraint as imposed goes beyond merely requiring previous identification or registration."); *see also id.* at 550 (Roberts, J., dissenting) ("The act confers no unbridled discretion on the Secretary of State to grant or withhold a registration card at his will, but makes it his mandatory duty to accept the registration and issue the card to all who come within the provisions of the Act upon their good-faith compliance therewith."). Furthermore, the petitioner's refusal to comply with the registration requirement was more a matter of expediency than principle, because he was informed of the requirement only six hours before he was scheduled to speak to an audience of factory workers. *See id.* at 521-22 (majority opinion).

> No speaker, in such circumstances, safely could assume that anything he might say upon the general subject would not be understood by some as an invitation [to join a labor union]. . . . In these conditions, it blankets with uncertainty whatever may be said. It compels the speaker to hedge and trim. He must take care in every word to create no impression that he means, in advocating unionism's most central principle, namely, that workingmen should unite for collective bargaining, to urge those present to do so.[188]

Perhaps the Court might have been more sympathetic to the state's interests if Texas had presented a substantial reason to identify labor organizers. Instead, as a strategic matter, the government chose to argue that the registration requirement was just a routine regulation of business practice that did not implicate any free speech concerns. Faced with no evidence that labor solicitations were harmful or unlawful, the Court concluded that the government had no basis to burden the speech—even with a perfunctory registration requirement.[189]

More challenging to evaluate have been regulations that blur the lines. With only a shallow theory of self-censorship, the Court has fumbled its way through those hybrid situations. Three examples are illustrative:

1. The Court has been slow to distinguish between actual retaliation and potential retaliation. In two companion cases—Buckley v. Valeo ("*Buckley I*")[190] and McConnell v. Federal Election Commission[191]—the Court eventually worked its way to the right result, that is to say, that mere allegations of potential retaliation is not enough. Those cases involved facial challenges to the Federal Election Campaign Act of 1971 ("FECA"), which had placed maximum limits on political contributions and expenditures in an effort to reduce the influence of money on elections. Significantly, the Act had also enacted detailed recordkeeping requirements in order to enforce those limits. In both cases, the Court was remarkably unified in upholding those disclosure provisions despite deep ambiguity as to what standard of review was appropriate.[192]

In *Buckley I*, the Court began by declaring, as a "general principle," that strict scrutiny is necessary whenever compelled disclosure has the "potential" to

---

[188] *Id.* at 535.

[189] *Id.* at 540 ("If the exercise of the rights of free speech and free assembly cannot be made a crime, we do not think this can be accomplished by the device of requiring previous registration as a condition for exercising them."). That said, the Court went on to state that where the speaker "goes further" and "engages in conduct which amounts to more than the right of free discussion comprehends, . . . he enters a realm where a reasonable registration or identification requirement may be imposed." *Id.*

[190] 424 U.S. 1 (1976).

[191] 540 U.S. 93 (2003).

[192] In *Buckley I*, only Chief Justice Burger dissented from the portion of the opinion upholding the disclosure provisions, quibbling that the dollar thresholds were too low to serve a legitimate informational interest. 424 U.S. at 236-41 (Burger, C.J., concurring in part). In *McConnell*, Justice Thomas was the only dissenter. 540 U.S. at 275-77 (Thomas J., dissenting in part).

"expose contributors to harassment or retaliation."[193] But the ensuing discussion quickly revealed the impracticality of applying exacting scrutiny when there is no evidence of *actual* retaliation.[194] Once the Court concluded that "[n]o record of harassment . . . was found in this case," and that "any serious infringement on First Amendment rights brought about by the compelled disclosure of contributors is highly speculative,"[195] it predictably dismissed the unsubstantiated fear of deterrence in favor of the tangible public interest in information and disclosure. The Court left open the possibility that unconstitutional harm might be proved in other cases,[196] but it refused to invalidate the disclosure provisions on the basis of hypothetical harms.

Three decades later, Congress amended FECA and expanded the disclosure provisions to cover new electioneering tactics. In *McConnell*, the Court reaffirmed the test it had first advanced in *Buckley I*, that evidence must be offered showing a "reasonable probability" that the compelled disclosure would result in actual "threats, harassment, or reprisals."[197] Once again, the Court upheld the disclosure provisions because it found that there was a "lack of specific evidence" that anyone would be prevented from speaking.[198] While the Court avoided committing to a specific standard of review, the implication was that unfounded assertions of *potential* retaliation were insufficient to trigger exacting scrutiny.[199]

Requiring evidence of harm was clearly contrary to the conclusory approach of *McIntyre* and *Talley*. In dissent, Justice Thomas argued that the latter position should have prevailed.[200] That he was not joined by any other member of the Court—the same members who had decided *McIntyre*—was a firm repudiation of the natural-rights theory of anonymity.[201]

2. While the Court has recognized the different forms of self-censorship across individual cases, it has had difficulty maintaining those

---

[193] *Buckley I*, 424 U.S. at 66, 68.

[194] *Cf. Buckley II*, 525 U.S. 182, 214 (Thomas, J., concurring) ("I recognize that in *Buckley [I]*, although the Court purported to apply strict scrutiny, its formulation of that test was more forgiving than the traditional understanding of that exacting standard.").

[195] *Buckley I*, 424 U.S. at 69-70.

[196] In a subsequent case, the Court did find sufficient evidence of hostility and harassment to exempt the Communist Party from equivalent state disclosure requirements. *See* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 98-101 (1982).

[197] McConnell v. Fed. Election Comm'n, 540 U.S. 93, 198 (2003).

[198] *Id.* at 199, 201.

[199] The few textual clues from the opinion suggest that the Court did apply lesser scrutiny. *See id.* at 196 (stating that the disclosure provisions were supported by "important" state interests); *see also id.* at 140 n.42 ("It is . . . simply untrue in the campaign finance context that all 'burdens on speech necessitate strict scrutiny review.'").

[200] *Id.* at 275-76 (Thomas J., dissenting in part) ("[T]his Court has explicitly recognized that 'the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry.'") (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995)).

[201] *But see* Lidsky & Cotter, *supra* note 10, at 1541-55. Lidsky and Cotter argue that the conflict between *McIntyre* and *McConnell* is attributable to inconsistent theoretical assumptions about audience sophistication, rather than a procedural disagreement about evidentiary burden.

distinctions once multiple identification requirements are joined in one statute. In Buckley v. American Constitutional Law Foundation, Inc. ("*Buckley II*"),[202] Colorado had imposed a number of restrictions on the circulation of ballot-initiative petitions. Petition circulators had to (1) be at least 18 years old, (2) be registered voters, (3) wear identification badges, and (4) disclose their names and addresses on an affidavit attached to the final copy of the petition. In addition, petition sponsors were required to disclose their names and the individual amounts of money paid to each petition circulator. The Court applied the same level of scrutiny to the entire statute.

In the most cogent portion of its opinion, the *Buckley II* Court expressed concern that the statute might deter the participation of petition circulators by exposing them to physical threats and other retaliation while engaged in the immediate act of advocacy. Thus, the Court invalidated the badge requirement because it applied during the face-to-face interaction between petition circulators and private citizens. The Court credited testimony that forcing petition circulators to wear name badges discouraged them from participating on "volatile" issues because they feared "recrimination and retaliation," particularly in the "heat of the moment" when "reaction to the circulator's message is immediate and may be the most intense, emotional, and unreasoned."[203] By contrast, the Court found that the affidavit requirement was not problematical because it was "separated from the moment the circulator speaks" and applied only "after circulators have completed their conversations with electors."[204] One might question why wearing a name badge increases the risk of retaliation when the circulator is already standing there in person, but the Court's decision was at least plausibly tied to evidence that additional retaliation and deterrence would occur. In that context it was arguably reasonable to apply strict scrutiny.

The rest of the opinion extended strict scrutiny without similar support from the record. In one part, the majority objected that requiring circulators to be registered voters would drastically reduce the number of people eligible to circulate petitions. Although registering to vote was easy and automatic, the majority reasoned that people should not be compelled to register because that choice "implicates political thought and expression."[205] But deterrence through voluntary choice cannot be equated to deterrence through duress. Both dissents reached that same conclusion. Justice O'Connor classified the registration requirement as a "neutral qualification" that did not "directly prohibit otherwise qualified initiative petition circulators from circulating petitions" or "silence those who are 'able and willing' to circulate ballot initiative petitions."[206] Chief Justice Rehnquist put it more bluntly: "political dropouts" who "make the conscious decision not to register to vote on the grounds that they reject the democratic process" have "no right to complain that they cannot circulate initiative petitions

[202] 525 U.S. 182 (1999).
[203] *Buckley II*, 525 U.S. at 198-99 (quotation marks omitted).
[204] *Id.* at 198, 200.
[205] *Id.* at 195-96.
[206] *Id.* at 218-19 (O'Connor, J., dissenting in part).

to people who *are* registered voters."[207] Refusal to participate because of a disagreement with the principle of registration was more akin to *Harriss* than *Shelton*, and was not the sort of deterrence that called for elevated scrutiny.

The other provision invalidated by the Court was the requirement that petition sponsors disclose the individual amounts paid to each circulator. Here the subject of deterrence was skipped altogether. The majority opinion stated that disclosure would "forc[e] paid circulators to surrender the anonymity enjoyed by their volunteer counterparts."[208] But it did not follow that up with the necessary assertion that paid circulators would therefore refuse to participate in petition campaigns. Again, both dissents were attuned to that flaw, pointing out that neither logic nor evidence in the record supported any finding of deterrence.[209] Without a showing of colorable harm to the exercise of free speech, the Court should not have held the provision invalid.

3. If *Buckley I* paid false heed to potential deterrence, and *Buckley II* conflated the different forms of deterrence, a hybrid of those two problems plagued the Court's decision in Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton.[210] There, the Court refused to choose a proper theory of harm on the premise that all were potentially plausible. The case was brought by Jehovah's Witnesses who challenged a village ordinance that made it a misdemeanor to engage in door-to-door advocacy without a permit. Although the involvement of Jehovah's Witnesses was suggestive of the early handbill cases, the lower courts here had found the ordinance to be content-neutral and of general applicability.

Where the *Watchtower* Court excelled was in articulating clearly the three theories of deterrence. First, it observed that the permit requirement might lead to "economic or official retaliation" and "social ostracism," and prevent some individuals from canvassing for unpopular causes. The second reason for deterrence was that "religious or patriotic views" could cause some citizens to refuse to apply for a license, because they "prefer silence to speech licensed by a petty official." And the last reason given by the Court was that a significant amount of spontaneous speech would be effectively inhibited if citizens had to obtain permits before going across the street to talk with their neighbors about ordinary matters.[211]

Where the Court fell short was in failing to explain which if any of those theories justified its decision to strike down the statute. It punted instead, stating

---

[207] *Id.* at 230-31 (Rehnquist, C.J., dissenting).
[208] *Id.* at 204 (majority opinion).
[209] *See id.* at 222 (O'Connor, J., dissenting in part) ("[T]he Court does not suggest that there is any record evidence tending to show that such remote disclosure will deter the circulation of initiative petitions."); *id.* at 232-33 (Rehnquist, C.J., dissenting) (observing that all petition circulators were already required to surrender their anonymity under the affidavit requirement, which was upheld, and that the "only additional piece of information for which the disclosure requirement asks is thus the amount paid to each circulator").
[210] 536 U.S. 150 (1999).
[211] *See id.* at 166-67.

that the ordinance "cover[ed] so much speech" that it was "unnecessary" to decide which standard of review to apply.[212] But that skipped the crucial step of identifying the constitutional harm; the appeal to breadth of scope was a red herring.

If the Court had carried forward its analysis, it could have started by dismissing the charge of deterrence via retaliation. Applying the rule established in *Buckley I* and *McConnell*, the Court should have recognized that the record failed to show a likelihood of threats, harassment, or reprisal. In fact, although the Witnesses had tried to argue that the ordinance was a product of hostility against their ministry, the trial court had rejected that charge.[213] Nor was this a case like *Buckley II*—as the Court suggested in passing—where forcing canvassers to reveal their names would deter participation because of a bona fide fear of retaliation. In *Buckley II*, the Court had relied on testimonial evidence; in *Watchtower*, the Court's descriptions of retaliation were solely in the abstract.

The Court also could have dismissed the claim of religious objection. As the Witnesses explained at trial, they had refused to apply for the permit "because they derive their authority to preach from Scripture," and seeking a permit to preach "would almost be an insult to God."[214] But the Court has emphatically established in prior precedents that religious objection is not a basis for striking down an otherwise valid and neutral law of general applicability.[215] That rule should have foreclosed the second line of argument. In any event, it was unlikely that the Witnesses would have been deterred at all, since "door-to-door canvassing is mandated by their religion."[216]

The final—and most credible—basis for invalidity was that the ordinance would deter spontaneous speech. That threat was not tied directly to the activities of the Jehovah's Witnesses, which were hardly spontaneous. Nevertheless, the Court's concern was that any citizen would have to "first inform the government of her desire to speak to her neighbors and then obtain a permit to do so."[217] Any conversation initiated near a villager's residence would have to be carefully circumscribed to avoid inadvertent violations—the same concern that pervaded the Court's decision in Thomas v. Collins. But *Thomas* was distinguishable in that

---

[212] *Id.* at 164, 165. There were at least three votes for intermediate scrutiny, but no indications as to how the other five Justices in the majority would have voted.
[213] *Id.* at 158.
[214] *Id.* at 157-58.
[215] *See* City of Boerne v. Flores, 521 U.S. 507, 535 (1997) ("When the exercise of religion has been burdened in an incidental way by a law of general application, it does not follow that the persons affected have been burdened any more than other citizens, let alone burdened because of their religious beliefs."); Employment Div. v. Smith, 494 U.S. 872, 879 (1990) ("Subsequent decisions have consistently held that the right of free exercise does not relieve an individual of the obligation to comply with a 'valid and neutral law of general applicability on the ground that the law proscribes (or prescribes) conduct that his religion prescribes (or proscribes).'" (internal citation omitted)); *see also Watchtower*, 536 U.S. at 171 (Scalia, J., dissenting) ("If a licensing requirement is otherwise lawful, it is in my view not invalidated by the fact that some people will choose, for religious reasons, to forgo speech rather than observe it.").
[216] *Watchtower*, 536 U.S. at 160.
[217] *Id.* at 166.

the only justifying state interest invoked there was the routine regulation of business practices; in *Watchtower*, the Court conceded that the village had provided several important interests—prevention of fraud, prevention of crime, and protection of residents' privacy.[218] Furthermore, although the Court suggested that the village should have considered alternatives that were more narrowly tailored, such as the posting of "No Solicitation" signs, a restriction of spontaneous speech triggers only intermediate scrutiny, which does not require the government to use least restrictive means.[219]

In the end, perhaps the Court's gut instinct was correct, and the ordinance was overly restrictive of protected speech. But a more discerning explanation would have illuminated the contours of the relationship between anonymity and speech. By refusing to explore those subtleties, the Court planted its signpost before reaching the fork in the road and steered observers off the path.

B. Investigatory Measures

Less effort is needed to reconcile the cases in which the identification request is tied to a specific criminal investigation. Generally, in such cases, the state interest is well-established, and so a person seeking to guard his anonymity must claim either that the request is in bad faith (if challenging before the fact) or that the methods used to obtain his identity were procedurally unsound (if challenging after the fact). Two contexts are especially instructive: investigations by police officers, and investigations by courts.

While police investigations are limited by the ordinary bounds that govern searches and seizures, the act of asking for identification does not carry independent constitutional significance. In other words, merely asking a person for his identity does not automatically convert that police interaction into an illegal search or seizure.[220] Providing one's name, for example, is so routine and relevant to investigative purposes that a refusal to answer may be penalized by arrest or even prosecution.[221] When courts have excluded identifying evidence, it has been because the police committed a separate violation, such as conducting a dragnet search and detaining multiple individuals without suspicion in order to obtain their fingerprints or DNA samples. An otherwise-illegal detention cannot be legitimized by the fact that its sole purpose is to ascertain an individual's identity.[222] Even then, however, the courts have made clear that it is not the

---

[218] *See id.* at 164-65. Even if the interest in crime prevention were omitted, *see id.* at 169-71 (Breyer, J., concurring), the other goals of protecting residents from fraud and undue annoyance would remain important interests.

[219] *See, e.g.*, Wengler v. Druggists Mut. Ins. Co., 446 U.S. 142, 150 (1980) (the means employed must be "substantially related" to the achievement of the important governmental objectives).

[220] Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004) ("'[I]nterrogation relating to one's identity or a request for identification by the police does not, by itself, constitute a Fourth Amendment seizure.'" (quoting INS v. Delgado, 466 U.S. 210, 216 (1984))).

[221] *Id.* at 186-88.

[222] Davis v. Mississippi, 394 U.S. 721, 727 (1969) ("Detentions for the sole purpose of obtaining fingerprints are no less subject to the constraints of the Fourth Amendment.").

collection of identifying information that is problematical, but rather the undue inconvenience and harassment that can occur if the collection is performed clumsily.[223] The upshot is that one's identity is not subject to the same procedural protections from police search and seizure that are granted to physical bodies or ordinary, tangible objects.

Judicial investigations have adhered to the same approach: once a court determines that the identity of a party or witness is material to a case, the public interest in adjudication invariably trumps any individual interest in anonymity.[224] That presumption is negated only if the subpoena request is issued in bad faith, in that the court has no legitimate interest in obtaining the information.[225] Although the bad-faith loophole has enjoyed some popularity among the courts of appeal, especially in the context of reporters or newsmen, it is a situational exception that does not translate into a generalized right to anonymity.[226] If the court has good reason to seek the identifying information, then it is always entitled to that information.

Two other exceptions are worth noting. The first is the "informer's privilege," which allows the government to assert a limited protection of anonymity for its own confidential witnesses. Here, the courts have been more tolerant of anonymity because encouraging informants to cooperate with the government furthers the public welfare, and also because exposing their identities to potentially dangerous criminals represents a clear risk of harm.[227] And although

---

[223] *See* Hayes v. Florida, 470 U.S. 811, 816-17 (1985) (noting that a "brief detention in the field for the purpose of fingerprinting" might be permissible as long as it is carried out with dispatch); *see also* United States v. Mitchell, 652 F.3d 387, 413 (3d Cir. 2011) (upholding the suspicionless collection of DNA samples from arrestees and pretrial detainees, and noting that "DNA profiling is simply a more precise method of ascertaining identity and is thus akin to fingerprinting").

[224] *See* Branzburg v. Hayes, 408 U.S. 665 (1972) (rejecting a testimonial privilege for reporters to protect the anonymity of confidential sources, because there is a stronger constitutional interest in allowing grand juries to perform their function of investigating potential criminal conduct); Reporters Committee for Freedom of Press v. AT&T Co., 593 F.2d 1030, 1049 (D.C. Cir. 1978) (a court's "[g]ood faith investigation interests always override a journalist's interest in protecting his source").

[225] *See Branzburg*, 408 U.S. at 699-700, 707-08; *id.* at 709-10 (Powell, J., concurring) ("If a newsman believes that the grand jury investigation is not being conducted in good faith he is not without remedy. Indeed, if the newsman is called upon to give information bearing only a remote and tenuous relationship to the subject of the investigation, or if he has some other reason to believe that his testimony implicates confidential source relationship without a legitimate need of law enforcement, he will have access to the court on a motion to quash and an appropriate protective order may be entered."); *Reporters Committee*, 593 F.2d at 1061 & n.107. Justice Powell, who cast the fifth vote but joined the majority, has often been credited instead as having authored a controlling plurality opinion.

[226] *See* McKevitt v. Pallasch, 339 F.3d 530, 532-33 (7th Cir. 2003) (listing cases, and concluding that "courts should simply make sure that a subpoena duces tecum directed to the media, like any other subpoena duces tecum, is reasonable in the circumstances, which is the general criterion for judicial review of subpoenas").

[227] *See* McCray v. Illinois, 386 U.S. 300 (1967); Roviaro v. United States, 353 U.S. 53, 59 (describing the purpose of the informer's privilege as "recogniz[ing] the obligation of citizens to communicate their knowledge of the commission of crimes to law-enforcement officials and, by preserving their anonymity, encourag[ing] them to perform that obligation").

the privilege must yield to the Confrontation Clause if the informer's identity is "relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause,"[228] the courts have tended to construe that dictate as narrowly as possible.[229] The relevant distinction is that the informant's identity is being protected by the government, not from the government.[230] Thus, the informant's anonymity is limited in purpose and scope, because his identity is on file with the government.[231]

The second exception is civil suits, which lack the law enforcement heft of criminal proceedings. Courts have been slower to disfavor anonymity when it is one private entity against another. To allay the concern of harassment and frivolous litigation, for instance, most courts have demanded at least proof of a prima facie case in order to consider such a request. Some courts have added further conditions such as providing the John Doe with notice and an opportunity to be heard, or conducting an explicit "balancing of the interests."[232] Those requirements elevate the threshold that must be met in order to satisfy the court that an individual should be unmasked. But the conditions are not intended to be difficult, and more importantly they reserve to the courts the prerogative of making the determination.

V. CONCLUSION

For years, we have accepted as gospel 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 blocking controls in one place only causes them to bubble up elsewhere. Rather than reflexively resisting all authoritative control, we should think more carefully about prioritizing the disorderly aspects of the internet that matter most. Zittrain has argued persuasively that generativity should top that list. But being at the head is not meaningful if it is a list of one. If we want a governable internet that is also generative, we must find something to curb other than generativity. The regulation of online anonymity provides that needed flexibility.

Many of us have become accustomed to the idea of being anonymous when we surf online. Yet, anonymity has never been inviolate, and the

---

[228] *Roviaro*, 353 U.S. at 60-61.

[229] *See* United States v. Gaston, 357 F.3d 77, 84 (D.C. Cir. 2004) ("One must be careful not to read too much into this last statement from Roviaro. In speaking of evidence 'relevant or helpful to the defense' the Court could hardly have meant that the privilege covers only irrelevant and unhelpful evidence.").

[230] The same purpose also justifies the protection of anonymity under the Intelligence Identities Protection Act of 1982, 50 U.S.C. §§ 421-26, which protects the identities of covert agents.

[231] But the informer's privilege is vulnerable to abuse by corrupt federal officials. *See, e.g.*, Adam Nagourney & Abby Goodnough, *Long Elusive, Irish Mob Legend Ended Up a California Recluse*, N.Y. TIMES, June 24, 2011, at A1, http://www.nytimes.com/2011/06/24/us/24bulger.html (describing the mishandling of Whitey Bulger by FBI agents).

[232] *See* Calvert et al., *supra* note 109, at 40-45 (distilling and comparing six possible factors used by courts in unmasking tests).

incongruity of handling it with kid gloves now can be seen as we generalize beyond the internet. The cumulative effect of the case law shows that the courts have regularly exercised substantial control over the use of anonymity. Only when an identification request is arbitrary or in bad faith, or an actual risk of harm exists, have the courts intervened to shelter anonymity. Nor have our offline sensibilities been shaped by the changing technologies of anonymity. If we were to find it prudent to switch course and begin regulating online anonymity, there would be ample room to do so within our jurisprudential guidelines.

The first place to start would be to embed reliable network identification through the use of IPv6. The current internet addressing system, IPv4, is due to be replaced by IPv6 because we have already allocated all available addresses. By providing a greatly expanded 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. 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. Shared addressing employs a different scheme that allows a single, assigned address to be used simultaneously by multiple users and devices. Both workarounds rely on maintaining imprecise relationships between user devices and IP addresses. Using IPv6 to assign a unique and static IP address to each device would go a long way toward providing courts with the ability to track down suspicious devices.

At least three vulnerabilities would remain: (1) the potential inaccuracy of network activity logs, (2) the use of intermediary devices to mask the originating IP address, and (3) the spoofing of IP addresses.[233] In layman's terms, an identity can be forgotten or misremembered; an identity can be covered up; or an identity can be falsified. Those vulnerabilities can be mitigated but probably 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 tampering. Enacting statutory duties would help, but errors and security breaches would likely crop up. The second presents the most difficult technological challenge, because it entails tracing and uprooting the entire structure of an underground proxy network. Above-the-board operations like Tor might be easily dissuaded, but a determined criminal operation would use every means possible to protect itself. The third is the simplest, as it can be foiled mainly by performing server-side validation, but nevertheless deserves mention because it can still be exploited for distributed denial of service ("DDOS") attacks.

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: by withholding or failing to keep appropriate records, allowing network traffic to be scrubbed of identifying details, and improperly validating spoofed credentials. The foreign government could also

[233] *See* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 399 n.172 (2011).

obfuscate its own military activities, or refuse to extradite criminals residing within its territory. The challenge of international cooperation is a longstanding one, and one that will not be resolved anytime soon, but one option would be to create a "trusted" network of internet allies, and flag as suspicious all traffic entering from any untrusted country.

Where those problems are too intractable, it may be necessary to return to generativity-based solutions. At one extreme, some activities may be so hazardous (a la nuclear technology) that we do not want to allow any form of public access, anonymous or otherwise. Conversely, some anonymous abuses may be so petty that strict enforcement is unwarranted. More likely, most activities will fall somewhere in between, and we will want to seek out ways of organizing the system to minimize the harmful impact of anonymous users. In the late 1990s, eBay held fraud to less than 0.01 percent by creating a feedback system, and providing other community-building devices such as "neighborhood watch" groups and the Giving Board.[234] Similarly, Craigslist initially fended off abuse in its first few years by manually screening nearly every one of the tens of thousands of messages that were posted on the site; since then, users of the site have assisted in flagging inappropriate postings.[235] Nevertheless, it is telling that both sites have taken steps in more recent years to encourage their users to use their real identities. The point is not to vilify anti-generative measures, or to exalt identification requirements. Regardless of the balance we ultimately accept, we should be cognizant that there is a choice to be made, and that the choice will affect how exceptional the internet remains.

[234] JOHN HENRY CLIPPINGER, A CROWD OF ONE 118-19 (2007).
[235] Wolf, *supra* note 21.