Free Speech

Anupam Chander[*] *and Uyên P. Lê*[**]

ABSTRACT: When civic engagement is increasingly mediated online, the law regulating cyberspace becomes the law regulating speech. Yet, free speech texts and free speech theorists pay scant attention to the ways that cyberlaw configures the principal mechanism for exercising free speech rights today—communication online. Conversely, while many have long observed that the Internet enables speech, scholars have failed to recognize the role that the First Amendment played in configuring the law of cyberspace. A strong normative commitment to free speech helped clear the legal hurdles for the development of history's most powerful platforms for speech. Because of law, speech became free—free as in speech, and free as in beer. This is the First Amendment/Cyberlaw Dialectic: the First Amendment constituted cyberlaw, and cyberlaw, in turn, constituted free speech.

But this moment of free speech is fragile, threatened by mass electronic surveillance, mega-trade treaties with ever stricter intellectual property protections, and criminal copyright law. How we approach such issues will determine the extent of government censorship, private third-party censorship, and even self-censorship and sousveillance. The future of free speech hangs in the balance.

* Professor of Law, University of California, Davis; B.A., Harvard University; J.D., Yale Law School.

** Free Speech and Technology Fellow, University of California, Davis; B.A., Yale University; J.D., University of California, Davis.

We thank Vik Amar, Ashutosh Bhagwat, Ken Bamberger, Alan Brownstein, Michael Froomkin, Jerry Kang, Carlton Larson, Vincent Polley, Saikrishna Prakash, Derek Slater, Madhavi Sunder, and William Wang, as well as a Berkeley law faculty workshop and Zachary Sanderson and other editors of the *Iowa Law Review*, for very helpful comments. We are grateful as well to Alex Macgillivray, then-general counsel of Twitter, for his insights, and to Google for supporting this work with a Google Research Award. All views expressed herein are our own and should not be attributed to others.

I. INTRODUCTION

"Every freeman has an undoubted right to lay what sentiments he pleases before the public."

Then-Judge James Iredell, 1799[1]

"We are the free speech wing of the free speech party."

Alex Macgillivray, Then-General Counsel, Twitter, 2011[2]

Fifty years ago, the Supreme Court established for the first time that tort law was subject to the First Amendment.[3] The central insight of *New York Times Co. v.*

1. Case of Fries, 9 F. Cas. 826, 839 (C.C.D. Pa. 1799) (No. 5126) (quoting 4 WILLIAM BLACKSTONE, COMMENTARIES *151).

2. Emma Barnett, *Twitter Chief: We Will Protect Our Users from Government*, TELEGRAPH (Oct. 18, 2011, 10:23 AM), http://www.telegraph.co.uk/technology/twitter/8833526/Twitter-chief-We-will-protect-our-users-from-Government.html.

3. ROBERT M. O'NEIL, THE FIRST AMENDMENT AND CIVIL LIABILITY 13 (2001) (observing that *Sullivan* "for the first time . . . [brought] civil sanctions clearly within the scope of First Amendment protection"); Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1656 (2009) ("For most of American history, private lawsuits did not implicate the First Amendment, regardless of whether they sought remedies for tort violations or enforced contracts or property rules."); L. Lin Wood & Corey Fleming Hirokawa, *Shot by the Messenger: Rethinking Media Liability for Violence Induced by Extremely Violent Publications and Broadcasts*, 27 N. KY. L. REV. 47, 49 (2000) ("Prior to . . . *New York Times* [*Co.*] *v. Sullivan*, the First Amendment was

Sullivan was that private claims empowered by the state can undo free expression.[4] But the speech protected in the case that launched the modern First Amendment[5] cost $4800 in 1960.[6] Indeed, in his argument to the Court, Commissioner L.B. Sullivan ridiculed the *Times*' claim to be promoting the "equality of practical enjoyment of the benefits" of free speech and press.[7] Justice Brennan, writing for the Court, could only argue that "'editorial advertisements' of this type" at issue in the case allowed "persons who do not themselves have access to publishing facilities . . . to exercise their freedom of speech even though they are not members of the press."[8] Still, by turning the First Amendment's gaze from direct state regulation of speech to private law, *Sullivan* helped usher in an era when speech, powered by the Internet, would in fact become *free*—in both senses of the term. *Free* as in speech, and *free* as in beer.[9]

Since the rise of the World Wide Web, scholars have sought to understand its relationship to the First Amendment. Eugene Volokh observed that the Internet

thought not to prohibit or limit state tort laws that allowed private actions for damages related to injuries caused by negligent publications." (footnote omitted)).

4. *Sullivan* is often heralded for introducing the requirement of malice for any case of libel against a public official, but its more fundamental innovation was to render private law within the disciplinary domain of the First Amendment's free speech and free press clause. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 291–92 (1964). Such an approach was so new that the Alabama Supreme Court could have dispatched the *New York Times*' constitutional arguments earlier in the case in merely two sentences—the first stating that the First Amendment did not apply to state libel, and the second that there was no state action in a private tort claim. *See* N.Y. Times Co. v. Sullivan, 144 So. 2d 25, 40 (Ala. 1962).

5. *Sullivan* has been widely extolled (though largely on other grounds). *See* Harry Kalven, Jr., *The* New York Times *Case: A Note on "The Central Meaning of the First Amendment,"* 1964 SUP. CT. REV. 191, 208–10 (explaining that the case defined the "central meaning" of the First Amendment); *id.* at 221 n.125 (quoting Alexander Meiklejohn's statement in response to the *Sullivan* decision: "an occasion for dancing in the streets"); *see also* LEE C. BOLLINGER, UNINHIBITED, ROBUST, AND WIDE-OPEN: A FREE PRESS FOR A NEW CENTURY 14 (2010) (calling *Sullivan* "[o]ne of the most important First Amendment decisions in the twentieth century, and perhaps of all time"); Floyd Abrams, *In Memoriam: William J. Brennan, Jr.*, 111 HARV. L. REV. 18, 21 (1997) (noting *Sullivan* "is the quintessential First Amendment ruling in our history"); Richard A. Epstein, *Was* New York Times v. Sullivan *Wrong?*, 53 U. CHI. L. REV. 782, 782 (1986) (calling *Sullivan* an "epochal case").

6. *Sullivan*, 376 U.S. at 260 (noting that a full page advertisement cost $4800). A similar advertisement today runs between approximately $67,000 and $241,000. N.Y. TIMES, 2014 BUSINESS ADVERTISING RATES 4 (2014), *available at* http://nytmediakit.com/uploads/rates/14-0208_2014_Business_RateC_AW5.pdf; *see also* Jen Chung, *Full-Page NY Times Ad with A.O. Scott's Tweet Cost $70,000*, GOTHAMIST (Jan. 6, 2014, 5:30 PM), http://gothamist.com/2014/01/06/full-page_ny_times_ad_with_ao_scott.php.

7. Brief for Respondent at 31, *Sullivan*, 376 U.S. 254 (No. 39), 1963 WL 105892, at *31. "The *Times* charged the regular commercial advertising rate of almost five thousand dollars, scarcely as 'an important method of promoting some equality of practical enjoyment of the benefits the First Amendment was intended to secure.'" *Id.*

8. *Sullivan*, 376 U.S. at 266.

9. This turns on its head Richard Stallman's famous aphorism about open source software—free as in speech, not free as in beer. Jonathan Zittrain, *Normative Principles for Evaluating Free and Proprietary Software*, 71 U. CHI. L. REV. 265, 271 (2004) (discussing Stallman's description of "free software").

diversifies the range of speakers and increases access to speech, reducing the historical bias in favor of the speech of the rich.[10] Lawrence Lessig argued that the architecture of the Internet allowed "a First Amendment *in code* more extreme than our own First Amendment *in law*."[11] James Boyle and Yochai Benkler warned that intellectual property protections were fencing off speech behind proprietary lines.[12] Cass Sunstein worried that users would use the new medium to cocoon themselves from contrary perspectives.[13] Michael Froomkin showed that the standards-setting process used for Internet architecture approximates Jürgen Habermas' discourse ideal.[14] Seth Kreimer argued that intermediary liability would lead intermediaries to censor speech broadly.[15] Rebecca Tushnet suggested that online intermediaries will favor speech congenial to their corporate interests.[16] Christopher Yoo observed that consumers often rely on intermediaries to filter speech for us.[17] Edward Lee argued that the *Sony* safe harbor for new technologies has First Amendment underpinnings.[18] In the latest interventions, Jane Bambauer affirms that data is speech,[19] while Jack Balkin warns of the rise of "collateral censorship" through a public–private alliance.[20]

Yet despite this extensive commentary, scholars have largely ignored a key insight: the First Amendment played an essential role in configuring the legal environment that enabled the rise of the Internet as we know it today, and in the process, helped bring the promise of 1789 closer to fruition.[21] Cyberlaw is today's

10. Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1826–1828 (1995). This contention would be used to argue against applying the fairness doctrine to this new domain.

11. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 167 (1999); *see also* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 395–96 (1999).

12. JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 183 (1996); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 446 (1999).

13. CASS SUNSTEIN, REPUBLIC.COM 192–94 (2001). *But see* Anupam Chander, *Whose Republic?*, 69 U. CHI. L. REV. 1479, 1481 (2002) (reviewing SUNSTEIN, *supra*) (countering that cyberspace also enhances the voices of marginalized people to the world and allows individuals to interact based on interests rather than national identity).

14. A. Michael Froomkin, *Habermas@Discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 841, 844 (2003).

15. Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 30–31 (2006).

16. Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1015–16 (2008).

17. CHRISTOPHER S. YOO, THE DYNAMIC INTERNET: HOW TECHNOLOGY, USERS, AND BUSINESSES ARE TRANSFORMING THE NETWORK 120–21 (2012).

18. Edward Lee, *Freedom of the Press 2.0*, 42 GA. L. REV. 309, 316–17 (2008).

19. Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV 57, 60–61 (2014).

20. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2309 (2014).

21. Two important recent papers ply similar terrain but are radically different in both their claims and their approach. Andrew Tutt argues that "intermediaries stand to control—often unnoticeably but nevertheless profoundly—what information individuals receive, how they receive it, and with whom

speech law. Yet, free speech casebooks and texts pay little attention[22] to the ways that cyberlaw configures the principal mechanism for exercising free speech rights today—communication online.[23] The First Amendment protected Internet intermediaries from obligations to censor, while at the same time rebuffing efforts to impose stricter privacy obligations on Internet enterprises.[24] The First Amendment thus created the business model of new media, permitting it to publish vast amounts of speech but not be held liable for that speech, while at the same time earning income through advertising based on personal profiling. For the first time, individuals could now speak to the nation—through YouTube, Twitter, blogs, comments, Facebook, and Google—without needing either princely sums for national advertising or the permission of editors. This is the First Amendment/ Cyberlaw Dialectic: the First Amendment constituted cyberlaw, and cyberlaw in turn constituted free speech.

While the First Amendment failed to constrain ever-lengthening copyright terms,[25] we show that concerns for speech stymied excessive copyright protections in other crucial ways, from the Digital Millennium Copyright Act ("DMCA") to the anti-SOPA campaign. Our analysis also helps solve a puzzle: In these debates, why might Congress have favored Silicon Valley upstarts over the well-heeled and powerful media companies of Hollywood and New York? Did not the movie, television, and newspaper companies epitomize the concerns of the First Amendment? Did not old media have far more power in the halls of Congress than Silicon Valley? The answer lies in the way that new media differs from old media. New media made speech free in ways old media never could. No longer did one need the permission of a narrow set of editors who controlled television channels

they can share it." Andrew Tutt, *The New Speech*, 41 HASTINGS CONST. L.Q. 235, 237 (2014). While we appreciate Tutt's argument, we focus on the ways that intermediaries *free* speech in ways never before possible. While Jacqueline Lipton argues for the importance of Internet intermediaries, her focus is not on their connection to speech or the First Amendment. *See generally* Jacqueline D. Lipton, *Law of the Intermediated Information Exchange*, 64 FLA. L. REV. 1337 (2012).

22. *See generally* VINCENT BLASI, IDEAS OF THE FIRST AMENDMENT 625–32 (2d ed. 2012) (providing excerpts of two law review articles on Internet intermediaries); STEVEN H. SHIFFRIN & JESSE H. CHOPER, THE FIRST AMENDMENT: CASES—COMMENTS—QUESTIONS 457–59 (5th ed. 2011) (providing three paragraphs on indecency and the Internet); GEOFFREY R. STONE ET AL., THE FIRST AMENDMENT 184–85, 238–39, 274–79, 400, 418–22, 641–44 (4th ed. 2012) (providing excerpts of cases, books, and articles on privacy and indecency on the internet); KATHLEEN M. SULLIVAN & NOAH FELDMAN, FIRST AMENDMENT LAW 181–90 (5th ed. 2013) (excerpts of three cases); WILLIAM W. VAN ALSTYNE & KURT T. LASH, THE AMERICAN FIRST AMENDMENT IN THE TWENTY-FIRST CENTURY: CASES AND MATERIALS 1010–19 (5th ed. 2014) (providing an excerpt of case and brief discussion of immunity for Internet service providers); EUGENE VOLOKH, THE FIRST AMENDMENT AND RELATED STATUTES: PROBLEMS, CASES AND POLICY ARGUMENTS 121–23, 126–27 (5th ed. 2014) (discussing immunity for Internet service providers).

23. A major study concludes that the Internet is an increasingly important tool for civic engagement today. *See* AARON SMITH, PEW RESEARCH INTERNET PROJECT, CIVIC ENGAGEMENT IN THE DIGITAL AGE (2013), *available at* http://www.pewinternet.org/2013/04/25/civic-engagement-in-the-digital-age/.

24. *See infra* Part II.C.

25. Golan v. Holder, 132 S. Ct. 873, 889–91 (2012); Eldred v. Ashcroft, 537 U.S. 186, 218–21 (2003).

or newspaper pages. Old media helped a few people speak; new media gave voice to the rest of us.[26] Mass media transformed from simplex to duplex communication, and from top-down to bottom-up.

Some will be skeptical: Did not the Internet itself allow individuals to post a webpage that the world could see without the need for intermediaries?[27] But experience with the first two decades of the web taught us this: If someone cries on a lonely blog, no one may hear. Internet intermediaries turn out to be crucial to helping individuals share information with friends, family, and strangers, through search engines, social networks, and even personal magazines.[28] Call this the "Lonely Blog" versus the "Networked User" phenomenon. Google, Facebook, and Twitter, not to mention Instagram, Pinterest, and other services not yet invented, help individuals speak with each other, even in the form of 140 characters or six-second videos.

This moment of free speech, radical by historical standards and unimaginable even in 1964, hangs at a precipice. Rather than a medium for free expression, the Internet might become widely censored or even more widely surveilled, with every utterance subject to third-party censorship or, even more pernicious, self-censorship. The new measures threaten to turn us from citizens to subjects. Today's threats to speech increasingly arise online. Millions of people protesting the Stop Online Piracy Act ("SOPA") argue the bill would "censor the Internet."[29] The enforcement of criminal copyright law through seizures of domain names and computer servers implicate First Amendment protections against prior restraints. The United States deplores efforts to relocate Internet governance to international fora, fearing the censors of China, Iran, and Russia.[30] At the same time, the "21st-century" trade agreements[31] promising a free trade area across the Pacific and the Atlantic include hidden implications for speech. Mass electronic surveillance of

26. We recognize, of course, that not everyone has Internet access. *See infra* text accompanying note 124.

27. *See generally* Derek E. Bambauer, Response, *Middlemen*, 64 FLA. L. REV. F. 64 (2012); Debora Halbert, *Two Faces of Disintermediation: Corporate Control or Accidental Anarchy*, 2006 MICH. ST. L. REV. 83; Lipton, *supra* note 21; Guy Pessach, *Deconstructing Disintermediation: A Skeptical Copyright Perspective*, 31 CARDOZO ARTS & ENT. L.J. 833 (2013).

28. Services such as Flipboard, Issuu, and MagCloud allow anyone to publish her own magazine. *See* FLIPBOARD, http://flipboard.com (last visited Oct. 25, 2014); ISSUU, http://issuu.com (last visited Oct. 25, 2014); MAGCLOUD, http://www.magcloud.com (last visited Oct. 25, 2014).

29. Dara Kerr, *Millions Sign Google's Anti-SOPA Petition*, CNET (Jan. 18, 2012, 7:17 PM), http://www.cnet.com/news/millions-sign-googles-anti-sopa-petition/ (quoting Google's "End Piracy, Not Liberty" petition).

30. H.R. 1580, 113th Cong. § 1(1) (as introduced, Apr. 16, 2013) ("Given the importance of the Internet to the global economy, it is essential that the Internet remain stable . . . ."); WORLD CONFERENCE ON INT'L TELECOMMS., DOCUMENT #-E, UNITED STATES OF AMERICA: PROPOSALS FOR THE WORK OF THE CONFERENCE (2012), *available at* http://www.state.gov/documents/organization/196244.pdf.

31. IAN F. FERGUSSON ET AL., CONG. RESEARCH SERV., R42694, THE TRANS-PACIFIC PARTNERSHIP (TPP): NEGOTIATIONS AND ISSUES FOR CONGRESS 2 (2013).

ordinary persons will chill even speech among friends. We observe a kind of antinomy: The digitization of speech lends itself to widespread surveillance, wrecking the very freedoms the digitization made possible.

Our account sheds light on the First Amendment itself. The marketplace of ideas, it turns out, depends on an actual market. When First Amendment scholars write about commerce, they focus largely on commercial speech. When they speak of the Internet, they focus on censorship of pornographic speech. In our account, the First Amendment reveals itself as an industrial policy. In an information age, free speech greases the economic engine. By revealing the free speech foundations of American cyberlaw, we hope to encourage other countries around the world eager to incubate the next Silicon Valley to embrace free speech. Governments from Brazil to India to Russia, seeking to incubate their own Silicon Valleys, must recognize the vital role that free speech plays in enabling Internet enterprise. This Article reconceptualizes threats to web industries as threats to free speech itself. The elusive distinction between free speech and free press resolves itself through a recognition of the press as the technology of speech.[32] When Google, Twitter, and Facebook allow us to speak to each other, a threat to any of them becomes a threat to all of us.

Some First Amendment scholars may worry that our argument edges towards the precipice of a new Lochnerism, with the First Amendment deployed to strike down a host of consumer regulations.[33] As Robert Post observes, "If every state regulation touching on what we call, in ordinary language, 'communication' were to be subject to constitutional review under the standards of the First Amendment, large swaths of perfectly common forms of regulation would be constitutionalized."[34] In 2011, the Supreme Court itself invoked *Lochner* when striking down a Vermont privacy regulation on First Amendment grounds.[35] While our argument might seem to embrace unlimited expansion of the First Amendment, we believe that recognizing the core expressive interests at stake in cyberlaw

32. For important accounts of the contemporary meaning of the freedom of the press, see generally Lee, *supra* note 18 (detailing the historical copyright law and freedom of the press); Christina Mulligan, *Technological Intermediaries and Freedom of the Press*, 66 SMU L. REV. 157 (2013) (arguing that the Internet and online service providers should be allowed more protections); Eugene Volokh, *Freedom for the Press as an Industry, or for the Press as a Technology? From the Framing to Today*, 160 U. PA. L. REV. 459 (2012) (analyzing how the Supreme Court and lower courts analyze freedom of the press); Sonja R. West, *Awakening the Press Clause*, 58 UCLA L. REV. 1025 (2011) (arguing for a narrow definition of "the press").

33. *See, e.g.*, Vikram David Amar & Alan Brownstein, *The Voracious First Amendment:* Alvarez *and* Knox *in the Context of 2012 and Beyond*, 46 LOY. L.A. L. REV. 491, 535–40 (2013) (highlighting the Court's inconsistencies behind the Free Speech Clauses); Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 477, 488 (2011) (describing the risk of Lochnerism arising from an autonomy-based theory of the First Amendment).

34. Post, *supra* note 33, at 477.

35. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2665 (2011) ("Vermont's law does not simply have an effect on speech, but is directed at certain content and is aimed at particular speakers. The Constitution 'does not enact Mr. Herbert Spencer's Social Statics.' It does enact the First Amendment." (quoting Lochner v. New York, 198 U.S. 45, 75 (1905) (Holmes, J., dissenting))).

actually provides an important rationale that should restrain undue expansion. Free speech must not be a get-out-of-jail-free card, a talisman to ward off regulation. Even if the First Amendment is the first among the amendments,[36] that does not render other constitutional values effete. Free speech is hardly the only value in a democratic state.[37] Martha Nussbaum enumerates a broad array of capabilities that are necessary to human flourishing, of which speech is but one.[38]

Our Article proceeds as follows. In Part II, we show how the First Amendment helped make American cyberlaw an engine for free speech, from rebuffing early efforts to censor the Internet to reducing liabilities for the speech of users or the data gathering of marketeers. Rather than seeing free speech as a bit player on the Internet, only disciplining occasional attempts to impose censorship regimes, our account brings free speech to the center stage of the legal framework for the web. In Part III, we turn to contemporary threats to history's most powerful platform for speech. We show that the central defect of SOPA was its threat to free speech, and then show that this threat to speech is migrating into other less-visible regimes—from criminal law enforcement, to the Trans-Pacific Partnership and efforts to bring the Internet under control of the United Nations. We apply the analysis to the European Union's proposed right to forget, observing its tension with a central free speech tenet—the right to remember. The most serious threat to free speech arises from the self-censorship that will follow from widespread electronic surveillance (which may be facilitated by the new technologies of Web 3.0 and the Internet of Things).

II. MAKING SPEECH *FREE*

Picture Senator James Exon's desk on the Senate floor in the summer of 1995. Senators huddle over the desk, perusing a blue folder containing pornography downloaded from the Internet.[39] Senator Exon sought to demonstrate the indecent material available on the Internet.[40] What came to be known as the "Blue Book"[41]

36. *See generally* Akhil Reed Amar, *The First Amendment's Firstness*, 47 U.C. DAVIS L. REV. 1015 (2014).

37. *See* Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 796 (2003) (arguing that cyberlaw scholars have ignored values of equality and distributive justice).

38. Martha C. Nussbaum, *Capabilities as Fundamental Entitlements: Sen and Social Justice*, 9 FEMINIST ECON. 33, 42 (2003) (describing speech as one aspect of a broader capability, "Control Over One's Environment"). On the capabilities approach to constitutional interpretation, see generally Martha C. Nussbaum, *Foreword: Constitutions and Capabilities: "Perception" Against Lofty Formalism*, 121 HARV. L. REV. 4 (2007).

39. 141 CONG. REC. S8330 (daily ed. June 14, 1995) (statement of Sen. James Exon); *id.* ("I looked over the shoulders of a huddle of Senators going through the blue book of the Senator from Nebraska. I saw one page of it, but I do not care to see that kind of filth." (statement of Sen. Patrick Leahy)).

40. *See, e.g.*, *id.* at S8339–40; *id.* at S8332 (statement of Sen. Daniel Coats); 141 CONG. REC. S8089 (daily ed. June 9, 1995) (statement of Sen. James Exon). An Internet awash in pornography was a claim supported by a study that formed the basis for a *Time* magazine front cover story. Marty Rimm, *Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2000*

would eventually lead to the first Supreme Court case involving the Internet and the First Amendment, and also, unexpectedly, the most important piece of legislation supporting the rise of cyberspace as we know it today. The controversy attending the Communications Decency Act ("CDA") marked the first great speech conflict of the Internet, even resulting in the first Internet protest blackout, presaging the wider SOPA protest nearly two decades later.[42] Struggles over the Internet over decades to come would often revolve around speech.

Whatever one's theory of speech, the Internet helped realize speech in ways never before possible.[43] Consider three classic free speech theories: democratic self-governance, marketplace of ideas, and human dignity and self-fulfillment. The theory of "democratic self-governance" stresses the role of free speech in actualizing society's participation in governance.[44] The Internet not only reduces barriers to participation, it increases the pace of activism and discourse—petitions and protests can be offered with a few keystrokes. Instead of political participation, the "marketplace of ideas" theory focuses on free speech as a critical vehicle for truth-seeking by ensuring an open forum where ideas compete against each other, furthering human enlightenment.[45] On the Internet, truth and lies jostle for

Cities in Forty Countries, Provinces, and Territories, 83 GEO. L.J. 1849, 1867 (1995) (concluding that 83.5% of images on Usenet are pornographic); *see generally* Philip Elmer-Dewitt, *On a Screen Near You: Cyberporn*, TIME, July 3, 1995, at 38, *available at* http://content.time.com/time/magazine/article/0,9171,134361,00.html. The study's methodology was widely critiqued. Donna L. Hoffman & Thomas P. Novak, *A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article: "Marketing Pornography on the Information Superhighway,"* MASS. INST. TECH. (July 2, 1995), http://mit.edu/activities/safe/writings/pornography/cmu-study/critique-by-hoffman; David G. Post, *A Preliminary Discussion of Methodological Peculiarities in the Rimm Study of Pornography on the "Information Superhighway,"* MASS. INST. TECH. (June 28, 1995), http://www.mit.edu/activities/safe/writings/pornography/cmu-study/critique-by-post; Brian Reid, *Critique of the Rimm Study*, MASS. INST. TECH. (July 5, 1995, 8:30 PM), http://xenia.media.mit.edu/~rhodes/Cyberporn/reid.on.rimm.html.

41. Elmer-DeWitt, *supra* note 40.

42. On December 12, 1995, over 20,000 "netizens" reached out to members of Congress with phone calls, faxes, and email messages urging them to oppose the CDA. This was the largest Internet protest to that date. *The National Day of Protest Against Internet Censorship Legislation Is Huge Success!*, CTR. FOR DEMOCRACY & TECH., http://web.archive.org/web/19970613212231/http://www.cdt.org/net_protest.html (last visited Oct. 26, 2014). For a detailed account of the controversies, see generally MIKE GODWIN, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE (1998) (discussing the legislative struggle to regulate the Internet in the late 1990s).

43. In the first federal judicial decision considering a First Amendment challenge to Internet regulation, Judge Stewart Dalzell characterized the Internet as "a far more speech-enhancing medium than print, the village green, or the mails," concluding that "the Internet may fairly be regarded as a never-ending worldwide conversation." ACLU v. Reno, 929 F. Supp. 824, 882–83 (E.D. Pa. 1996).

44. ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 75 (1960) (declaring the purpose of the First Amendment "is to give to every voting member of the body politic the fullest possible participation in the understanding of those problems with which the citizens of a self-governing society must deal").

45. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . ."); JOHN STUART MILL, ON LIBERTY

primacy, much in the way that marketplace theorists imagine, but with an intensity and participation rate previously unimaginable. As exemplified by Wikipedia, the Internet allows a decentralized network of vigilant individuals to collaborate and debate on "truth." The "human dignity and self-fulfillment" theory of free speech avers that the freedom of speech is necessary to dignity and autonomy.[46] The Internet makes self-expression possible with a reach previously unknown to ordinary persons.

A. LIABILITY AND SPEECH

With memories of the Blue Book likely in mind, Congress in 1996 overwhelmingly passed the CDA.[47] Its central provision, what would be § 223 of the U.S. Code, placed liability on intermediaries for the sending or transmission of "indecent" communication to minors.[48] Congressman Jerrold Nadler, a critic of the bill, called it "the cyberspace equivalent of book burning."[49] In a moment largely lost to history, Yahoo! and other Internet services darkened their websites, using white text on a black background, to denounce the threat to "the very existence of the Internet as a viable means of free expression, education, and political discourse."[50] By requiring Internet services to ensure that children could not access

40 (Boston: Ticknor & Fields 2d ed. 1863) (1859) ("Complete liberty of contradicting and disproving our opinion, is the very condition which justifies us in assuming its truth for purposes of action; and on no other terms can a being with human faculties have any rational assurance of being right."); JOHN MILTON, AREOPAGITICA 58 (Cambridge Univ. Press 1918) (1644) ("[T]hough all the winds of doctrine were let loose to play upon the earth, so Truth be in the field, we do injuriously by licensing and prohibiting to misdoubt her strength. Let her and Falsehood grapple; who ever knew Truth put to the worse, in a free and open encounter?").

46. David A.J. Richards, *Free Speech and Obscenity Law: Toward a Moral Theory of the First Amendment*, 123 U. PA. L. REV. 45, 62 (1974) ("[T]he significance of free expression rests on the central human capacity to create and express symbolic systems, such as speech, writing, pictures . . . . The value of free expression . . . rests on its deep relation to self-respect arising from autonomous self-determination without which the life of the spirit is meager and slavish."); *see also* Thomas Scanlon, *A Theory of Freedom of Expression*, 1 PHIL. & PUB. AFF. 204, 213–218 (1972) (discussing the relationship between the state and individuals' autonomy).

47. Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, § 502, 110 Stat. 133 (codified as amended at 47 U.S.C. §§ 223, 230 (2012)).

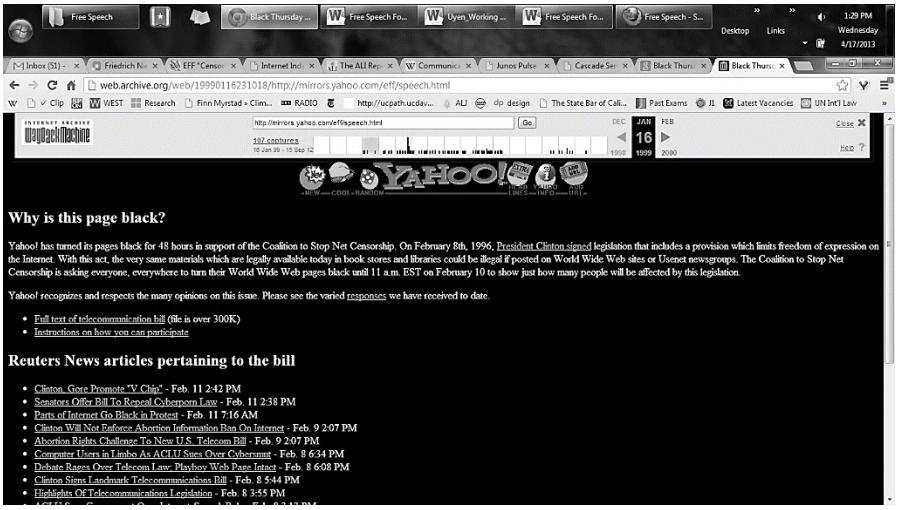
48. 47 U.S.C. § 223(a)(1)(B), (d) (1996), *invalidated by* Reno v. ACLU, 521 U.S. 844 (1997).

49. Peter H. Lewis, *Protest, Cyberspace-Style, for New Law*, N.Y. TIMES (Feb. 8, 1996), http://www.nytimes.com/1996/02/08/us/protest-cyberspace-style-for-new-law.html.

50. *Join Hundreds of Thousands of Other Internet Users in * 48 Hours of Protest * After President Clinton Signs the Bill That Will Censor the Internet*, CTR. FOR DEMOCRACY & TECH., http://web.archive.org/web/20080117200241/http://www.cdt.org/speech/cda/960203_48hrs_alert.html (last visited Oct. 26, 2014); Meeks Mixed Media, *The Day the Internet Went Dark—The Fight Against the Communications Decency Act*, YOUTUBE (Nov. 17, 2011), http://www.youtube.com/watch?v=iArH2pS2-bM. Netscape and Senator Patrick Leahy also blackened their home pages, as did some 1500 other sites. Dan Mitchell, *Remembering the Great Web Blackout*, WIRED (Feb. 8, 1997), http://archive.wired.com/politics/law/news/1997/02/1947. The blackout campaign, which had various names such as "A Thousand Points of Darkness," "Black Thursday," and "The Great Web Blackout," was led by the Voters Telecommunications Watch and the Electronic Frontier Foundation. Lewis, *supra* note 49; Mitchell, *supra*.

"indecent" material, the CDA would have: (1) forced them to carry out an impossible task, namely to identify and eliminate all the "indecent" speech on their sites teeming with user content; or otherwise (2) to require age verification. Imagine if Pinterest or Google had to police their services for indecency, the failure of which would subject them to fines and/or a maximum of two years imprisonment.[51]

Figure 1. Yahoo's webpage in the Internet protest blackout, February 1996.



But another provision of the CDA, amending § 230 of the U.S. Code, would prove a godsend to Internet companies.[52] That provision originated in the House of Representatives, where it passed overwhelmingly, 420–4.[53] It was joined somewhat unnaturally to § 223 in the Conference Committee. Section 230 explicitly recognized the Internet as "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[54] It immunized Internet intermediaries for the actions of their users. On the House floor, Representative Zoe Lofgren embraced the speech

51. 47 U.S.C. § 223(a)(2), (d)(2).

52. Jerry Berman of the Center for Democracy and Technology recognized that the Internet may have lost the battle in the Senate with the anti-decency provisions, but that with the introduction of the Cox–Wyden Amendment discussed below, the Internet "may win the war." John Schwartz, *House Vote Bars Internet Censorship: Amendment to Communications Bill Seems in Conflict with Senate*, WASH. POST, Aug. 5, 1995, at A11.

53. The anti-indecency provision of the CDA was proposed by Senator James Exon and Senator Daniel Coats, while the House version of the telecommunication reform bill lacked any censorship requirement. The House provision that led to § 230 was proposed by Representatives Christopher Cox and Ronald Wyden. Schwartz, *supra* note 52; *see also* Internet Freedom and Family Empowerment Act, H.R. 1978, 104th Cong. § 2 (1995) (enacted); THE COMMUNICATIONS ACT: A LEGISLATIVE HISTORY OF THE MAJOR AMENDMENTS, 1934–1996, at 141–46 (Max D. Paglin ed., 1999).

54. H.R. 1978 § 2.

freedoms enshrined in § 230, which she believed would "preserve the [F]irst [A]mendment and open systems on the Net."[55]

Having passed this bill at war within itself, fettering speech while liberating it, Congress now passed the baton to the courts. And the courts responded dramatically, repudiating the speech fetters of § 223, while strengthening the speech freedoms of § 230.

When the Supreme Court struck down the age verification provisions of the CDA in its first decision involving the Internet, it did so explicitly to protect freedom of speech in this new communications medium. In *Reno v. ACLU*, the Court ruled unconstitutional core provisions of the CDA that sought to keep children from accessing material judged indecent by a community.[56] If the CDA's anti-indecency provisions had survived, many websites might have been reluctant to allow individuals to post freely, fearing liability arising out of postings that some community might find "indecent." Age verification through credit cards might lead websites to require a fee because credit card companies charge for verification.[57] The CDA spelled the end of a free Internet. Moreover, only those adults with credit cards would now be able to access these sites. Furthermore, the CDA would have meant that social media websites unable to monitor their sites for "indecency" would have had to deny access to youth.

The Supreme Court embraced the speech potential of cyberspace. Justice Stevens began his opinion for the Court by declaring the Internet "a unique and wholly new medium of worldwide human communication."[58] The opinion announced that the Court would treat this new medium differently than the broadcast medium of radio and television: "Neither before nor after the enactment of the CDA have the vast democratic forums of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry."[59] The Court emphasized the value of the Internet to democratic exchange, observing that the Internet offered a medium "to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls."[60]

Not only did the Supreme Court strike out anti-speech aspects of the CDA, the lower courts, informed by the First Amendment, interpreted § 230 broadly. Most importantly, the courts eliminated both publisher and distributor liabilities for web intermediaries. In *Zeran v. American Online, Inc.*, the Fourth Circuit held that

55. 141 CONG. REC. H8471 (daily ed. Aug. 4, 1995) (statement of Rep. Zoe Lofgren).

56. Reno v. ACLU, 521 U.S. 844, 875–79 (1997).

57. *Id.* at 856.

58. *Id.* at 850 (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997)) (internal quotation marks omitted).

59. *Id.* at 868–69.

60. *Id.* at 851. Senator Patrick Leahy welcomed the decision: "The Supreme Court has made clear that we do not forfeit our First Amendment rights when we go on-line. This decision is a landmark in the history of the Internet and a firm foundation for its future growth. Altering the protections of the First Amendment for on-line communications would have crippled this new mode of communication." 143 CONG. REC. S6491 (daily ed. June 26, 1997) (statement of Sen. Patrick Leahy).

§ 230's explicit elimination of publisher liability implied the elimination of distributor liability as well.[61] The court reasoned that distributor liability would chill speech because service providers would take down information that some user found offensive for fear of liability for letting it remain: "Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not."[62] Distilling the larger purpose of § 230, the Fourth Circuit declared that Congress' intent was "to promote unfettered speech on the Internet."[63] Writing for the court, Chief Judge J. Harvie Wilkinson III explained:

> Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.[64]

Over the next decade and more, § 230 would prove a lifeline to Internet enterprises, their first line and often last line of defense against suits.[65]

Section 230 was not a blanket immunity for *all* speech—rather it protected intermediaries *qua* intermediaries. Intermediaries could still be held liable for their own speech. The CDA immunized a service only when the service could not itself be said to be the speaker—in the CDA's terms, when the service did not "develop" the offensive material but remained a true intermediary for the speech of others.[66] Internet defendants have found the CDA defense unavailing precisely when they

61. Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

62. *Id.* at 333.

63. *Id.* at 334.

64. *Id.* at 330. Such a broad embrace of § 230 would continue into state courts as well. The California Supreme Court described § 230 as "protect[ing] online freedom of expression," stressing that it protected against the chilling of speech because "[n]otice-based liability for service providers would allow complaining parties to impose substantial burdens on the freedom of Internet speech by lodging complaints whenever they were displeased by an online posting." Barrett v. Rosenthal, 146 P.3d 510, 525, 529 (Cal. 2006).

65. *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 653 n.58 (2014) (collecting dozens of cases where Internet companies successfully relied on § 230 to defend against federal and state claims).

66. 47 U.S.C. § 230(c)(1) (2012) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); *id.* § 230(f)(3) ("'[I]nformation content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.").

become the speaker.[67] In this way, § 230 recognized the special role of intermediaries, who serve as a vehicle for the speech of others.

B. COPYRIGHT AND CENSORSHIP

Copyright has sometimes been seen as a realm outside the First Amendment, immune from its constraints. Indeed, efforts by public domain advocates to discipline copyright through the First Amendment have been rebuffed by courts.[68] Yet, as we show below, First Amendment concerns helped animate the statutory protections Congress offered to Internet intermediaries in the DMCA.

When the DMCA was first proposed, however, free speech advocates rang the alarm. Just like they had focused on the anti-indecency provisions of the CDA, they focused now on the anti-circumvention measures in the DMCA's title I. They worried that criminalizing devices that broke through access and copy protections would stifle comment on others' works, making impossible the copy-and-paste that facilitates critique.[69] The public dialogue around the statute focused on the statute's protections for the copyright industry, not on the immunities for those who might upset that industry.

Yet, even at the time, the proponents of the statute understood that title II helped create the conditions for free speech. Most importantly, Congress recognized in title II the new industry of speech—the Internet service providers that enabled individuals to express themselves. The House report explained that title II "essentially codifies the result in the leading and most thoughtful judicial decision to date: *Religious Technology Center v. Netcom On-line Communications Services, Inc.*"[70] In that case, Judge Ronald Whyte of the Northern District of California had explicitly used First Amendment concerns to protect web services that had been used for copyright infringement. The case exemplified the risk that excessive copyright liability posed for speech. The copyright holders for the works of Church of Scientology founder L. Ron Hubbard sued those operating a Usenet

67. *See, e.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164–65 (9th Cir. 2008) (en banc).

68. *See* Golan v. Holder, 132 S. Ct. 873, 878 (2012) (holding that the First Amendment does not "make[] the public domain . . . a territory that works may never exit"); Eldred v. Ashcroft, 537 U.S. 186, 194 (2003) (holding that a copyright extension did "not alter[] the traditional contours of copyright protection [and thus] First Amendment scrutiny [was] unnecessary"); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985) (holding that First Amendment protections are accounted for in the "distinction between copyrightable expression and uncopyrightable facts and ideas").

69. *See* JESSICA LITMAN, DIGITAL COPYRIGHT 169–70 (2001); Benkler, *supra* note 12, at 415–16; Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 833–35 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 535–37 (1999); Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635, 646–48 (2004). We do not mean to point fingers or to suggest that the concern was without merit; for one of the authors' own contributions to this literature, see Anupam Chander, *Exporting DMCA Lockouts*, 54 CLEV. ST. L. REV. 205, 208–10 (2006).

70. H.R. REP. NO. 105-551, pt. 1, at 11 (1998).

bulletin board where a "former minister of Scientology turned vocal critic" had posted portions of Hubbard's works.[71] Judge Whyte wrote, "If Usenet servers were responsible for screening all messages coming through their systems, this could have a serious chilling effect on what some say may turn out to be the best public forum for free speech yet devised."[72] Judge Whyte explained that the Internet services sued in the case "play a vital role in the speech of their users."[73] He characterized copyright liability as a possible "'prior restraint' on free speech."[74]

Introducing what would become title II,[75] Senator John Ashcroft declared that immunities against copyright liability would serve free speech. He observed that online service providers could provide to "those who use the Internet or information in a digital format for education, entertainment, research" and that their—both the online service providers' and users'—"opportunity to speak and to learn needs to be protected."[76] In enacting title II, Congress defied the copyright industry, which believed that the common law liability rule sufficed.

When the House acted to adopt the conference report on October 12, 1998, Representative Barney Frank spoke of the impact of Congressional action on free speech online: "We have in this country the freest speech in the world, . . . but we are developing a second line of law which says electronically-transmitted speech is

71. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1365–66 (N.D. Cal. 1995).

72. *Id.* at 1377–78.

73. *Id.* at 1383.

74. *Id.*

75. The original versions of the DMCA introduced in the House, H.R. 2281, and the Senate, S. 1121, on July 29, 1997, lacked any copyright liability limitation. *See* WIPO Copyright and Performances and Phonograms Treaty Implementation Act of 1997, S. 1121, 105th Cong. (1997); WIPO Copyright Treaties Implementation Act, H.R. 2281, 105th Cong. (as introduced by Rep. Howard Coble, July 29, 1997). Senator John Ashcroft introduced an alternative bill, S. 1146, on September 3, 1997, to amend the provisions of 17 U.S.C. by adding a new § 512 to provide limitations on copyright liability for online service providers. *See* Digital Copyright Clarification and Technology Education Act of 1997, S. 1146, 105th Cong. § 102(a) (1997). Representative Howard Coble introduced the House version, H.R. 2180, on July 17, 1997. *See* On-Line Copyright Liability Limitation Act, H.R. 2180, 105th Cong. (1997). To reconcile the differences between the Senate and House bills, Representative Coble introduced H.R. 3209, which was incorporated into H.R. 2281 (also introduced by Representative Coble), and became part of title II. *See* On-Line Copyright Infringement Liability Limitation Act, H.R. 3209, 105th Cong. (1998); *see also* Michelle A. Ravn, *Navigating Terra Incognita: Why the Digital Millennium Copyright Act was Needed to Chart the Course of Online Service Provider Liability for Copyright Infringement*, 60 OHIO ST. L.J. 755, 778–83 (1999). For a full legislative history, see S. REP. NO. 105-190, at 2–8 (1998).

76. *The Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Comm. on the Judiciary*, 105th Cong. 42 (1997) (statement of Sen. John Ashcroft).

> Any effort to address the copyright protection of material on the Internet must protect everyone who stands to benefit from the expansion of electronic commerce.
>
> The content community has to be highly regarded—and I understand completely the need for the protection—but so do the online service providers, and those who use the Internet or information in a digital format for education, entertainment, research, and others. Their opportunity to speak and to learn needs to be protected.

Id.

not as constitutionally protected. We must reverse that trend or we will erode our own freedoms."[77] Representative Frank believed that title II ensured that Internet intermediaries would not act as censors: "In the Committee on the Judiciary, we worked very hard in particular in trying to work out a formula that would protect intellectual property rights and not give the online service providers an excessive incentive to censor."[78]

The importance of DMCA title II to free speech is hard to overstate. Before title II, the sword of copyright liability hung over the Internet. In *Playboy Enterprises Inc. v. Frena*[79] and *MAI Systems Corp. v. Peak Computer, Inc.*,[80] federal courts had held Internet service providers liable for copyright infringement occurring through their services, even for the temporary reproductions that arise in the ordinary course of Internet activity. If providers of web services were liable for this, the Internet would have shut down. The direct relationship between copyright and censorship would become even clearer with SOPA.[81] The liberating effect of the DMCA on speech can be discerned through a counterfactual: Can we imagine the rise of Google or Facebook if providers were liable for user copyright infringements?

C. PRIVACY AND DISCLOSURE

In 1995, the European Union ("EU") adopted the Data Protection Directive, a vast new regime of privacy protection.[82] In 1998, Japan launched a comprehensive data bureaucracy, the Supervisory Authority for the Protection of Personal Data, to oversee businesses handling personal data under government guidelines; broad statutes governing personal information would follow in 2001 and 2003.[83] In 2001, South Korea implemented laws protecting consumer privacy.[84] The United States Congress, however, remained remarkably restrained, limiting itself to a law

77. 144 CONG. REC. H10,618 (daily ed. Oct. 12, 1998) (statement of Rep. Barney Frank).

78. *Id.*

79. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).

80. MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518–19 (9th Cir. 1993).

81. *See infra* Part III.A.

82. Council Directive 95/46, 1995 O.J. (L 281) (EC).

83. Kojinjōhōnohogonikansuruhōritsu (zantei-ban) [Act on the Protection of Personal Information], Act. No. 57 of 2003 (Hōrei hon'yaku dētashū [Hon'yaku DB]) (Japan), http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf; Tokutei denki tsūshin ekimu teikyō-sha no songai baishō sekinin no seigen oyobi hasshinsha jōhō no kaiji ni kansuru hōritsu [Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders], Act No. 137 of 2001, art. 4 (Hōrei hon'yaku dētashū [Hon'yaku DB]) 02 (Japan), http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=04&re=.

84. Act on Promotion of Information and Communications Network Utilization and Data Protection, Act No. 7812, July 1, 2001 (S. Kor.), *translated in* http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

protecting the privacy of children under 13.[85] While numerous omnibus privacy bills were introduced, none passed.[86] Why?

Certainly, a pro-business attitude played a crucial role in the American preference for Internet self-regulation expressed throughout the 1990s. Unlike intellectual property, privacy did not have an obvious industry antagonistic to Silicon Valley's interests in the area, and so, industry was largely united against broad privacy laws. But a preference for business was not the only concern. The penchant for self-regulation had a constitutional underpinning: By allowing private parties to regulate themselves, there would be no government regulatory scheme or mandate that could conceivably impinge on their First Amendment rights. Indeed, as we will show here, the First Amendment posed a substantial hurdle to broad privacy regulations like those passed in other advanced economies.[87] We do not mean to suggest that privacy statutes are unconstitutional per se—but that Congress is reluctant to regulate privacy because such statutes might impinge on free speech.

Even before the Internet, the First Amendment had constrained the common law privacy torts.[88] William Prosser's privacy torts had seen their growth stunted

85. 15 U.S.C. §§ 6501–6506 (2012).

86. The 105th Congress (1997–1999) saw nine bills on online privacy introduced, including the Data Privacy Act of 1997, the Communications Privacy and Consumer Empowerment Act, the Federal Internet Privacy Protection Act of 1997, and the Consumer Internet Privacy Protection Act of 1997. H.R. 2368, 105th Cong. (1997); H.R. 1964, 105th Cong. (1997); H.R. 1367, 105th Cong. (1997); H.R. 98, 105th Cong. (1997). Similar efforts continued in the 106th Congress (1999–2001), with 16 bills introduced, eight in each chamber. These included the Internet Integrity and Critical Infrastructure Protection Act of 2000, the Privacy Commission Act, the Online Privacy Protection Act of 1999, the Electronic Privacy Bill of Rights Act of 1999, and the Internet Growth and Development Act of 1999. S. 2448, 106th Cong. (2000); H.R. 4049, 106th Cong (2000); S. 809, 106th Cong. (1999); H.R. 3321, 106th Cong. (1999); H.R. 1685, 106th Cong. (1999). Privacy advocates remained hopeful in the 107th Congress (2001–2003). Within the first few weeks, several bills focusing on online privacy were introduced, including the Consumer Online Privacy and Disclosure Act, the Consumer Internet Privacy Enhancement Act, the Social Security On-line Privacy Protection Act, and the Online Privacy Protection Act of 2001. H.R. 347, 107th Cong. (2001); H.R. 237, 107th Cong. (2001); H.R. 91, 107th Cong. (2001); H.R. 89, 107th Cong. (2001).

87. Eugene Volokh suggests First Amendment constraints on privacy law that go far beyond what we find: "[R]estrictions on speech that reveal[] personal information are constitutional under current doctrine only if they are imposed by contract . . . ." Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1122 (2000). For alternative views, see generally Robert C. Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 601 (1990); Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967 (2003).

88. *See, e.g.*, 1 RODNEY A. SMOLLA, LAW OF DEFAMATION § 4:65 n.3 (2d ed. 2012) ("The tort of publication of private facts raises such serious first amendment difficulties . . . that its continuing existence is in genuine doubt."); Thomas I. Emerson, *The Right of Privacy and Freedom of the Press*, 14 HARV. C.R.-C.L. L. REV. 329, 333 (1979) (observing that two of Prosser's torts, the public disclosure of embarrassing private facts and false light torts, "raise serious first amendment problems"); Paul Gewirtz, *Privacy and Speech*, 2001 SUP. CT. REV. 139, 176 (noting that "in virtually every case

by courts concerned about free speech.[89] Even Louis Brandeis, whose writing had helped fashion the privacy torts, had retreated from his earlier strong privacy views, endorsing Justice Oliver Wendell Holmes' view that "a free trade in ideas" might override concerns of "opinions that we loathe and believe to be fraught with death."[90] While Congress responded to the development of computer databases by requiring the federal government to keep information private,[91] it was reluctant to offer similar regulations of databases assembled by private parties, such as outside credit information and health records.

Efforts to impose privacy regulations on private entities were met with First Amendment concerns.[92] That is not to say that free speech by itself foiled privacy

that the Supreme Court decides involving a press/privacy conflict, the privacy claim loses," but arguing that "[t]he Supreme Court has allowed the speech/privacy balance to shift too far against privacy interests"); Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMM. & HIGH TECH. L. 357, 361 (2011) ("[T]he First Amendment should trump disclosure privacy in all but a narrow category of cases."); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 293 (1983) (noting "the inherent difficulty under the first amendment of treating truthful speech as tortious"); *see also* Fla. Star v. B.J.F., 491 U.S. 524, 530 (1989) (observing "tension between the right which the First Amendment accords to a free press, on the one hand, and the protections which various statutes and common-law doctrines accord to personal privacy against the publication of truthful information"); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496 (1975) ("[P]olitical institutions must weigh the interests in privacy with the interests of the public to know and of the press to publish."). *But cf.* Melville B. Nimmer, *The Right to Speak from* Times *to* Time*: First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 CALIF. L. REV. 935, 957 (1968) ("Intrusion does not raise First Amendment difficulties since its perpetration does not involve speech or other expression.").

89. *See, e.g.*, Hall v. Post, 372 S.E.2d 711, 714 (N.C. 1988) (holding "that claims for invasions of privacy by publication of *true* but 'private' facts are not cognizable at law"); Renwick v. News & Observer Publ'g Co., 312 S.E.2d 405, 412 (N.C. 1984), *cert. denied*, 469 U.S. 858 (1984) (refusing to recognize the false light invasion of privacy tort because it "would . . . add to the tension . . . between the First Amendment and [privacy] torts"). The concern would continue into more recent cases as well. Taus v. Loftus, 151 P.3d 1185, 1204 (Cal. 2007) (declining to recognize an action of public disclosure of private facts because the investigation and publication were "clearly activit[ies] in furtherance of [defendants'] exercise of . . . free speech" (alteration in original) (internal quotation marks omitted)); Denver Publ'g. Co. v. Bueno, 54 P.3d 893, 894 (Colo. 2002) (declining to recognize the tort of false light invasion of privacy because it "raises the spectre of a chilling effect on First Amendment freedoms"); Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1100 (Fla. 2008) (refusing to recognize the tort of false light invasion of privacy because it lacked "the attendant protections of the First Amendment"); Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) (declining to adopt a false light tort because "claims under false light are similar to claims of defamation, and to the extent that false light is more expansive than defamation, tension between this tort and the First Amendment is increased"); Cain v. Hearst Corp., 878 S.W.2d 577, 579 (Tex. 1994) (declining to recognize the tort of false light invasion of privacy).

90. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

91. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2012)).

92. Bruce E.H. Johnson & Anuj C. Desai, *Consumer Privacy and the First Amendment*, *in* COMMUNICATIONS LAW 513, 522 (Practising Law Inst. ed., 2000) ("Because [the proposed federal privacy] laws purport to give individuals a nearly unfettered right to control personally-identifiable information about themselves (that is, a right to control what others say about them), these laws will likely raise First Amendment issues . . . .").

law. Instead, concerns over free speech intermingled with concerns over regulating enterprise, forestalling congressional activity in the area. As James Whitman writes, "Freedom of expression has been the most deadly enemy of continental-style privacy in America."[93] Writing to the House Subcommittee on Commerce, Trade, and Consumer Protection in 2001, Fred Cate cautioned against adopting the European approach to privacy, noting that, "of course, Europe does not have a 'First Amendment' or a tradition of constitutional protection for information flows."[94]

This hesitance about broad privacy mandates on Internet service providers would only be confirmed in 1999 when the Court of Appeals of the Tenth Circuit declared consumer privacy rules for telecommunications providers unconstitutional. In *U.S. West, Inc. v. FCC*, the appeals court ruled that requiring telephone companies to obtain customer consent before using personal information outside certain specified domains violated the companies' First Amendment rights.[95] Acting under the authority of a section of the Telecommunications Act of 1996 entitled "Privacy of customer information," the Federal Communications Commission ("FCC") had sought to require opt-in consent before a telecommunications provider could use consumer information outside specified purposes.[96] In striking down the regulation, the Tenth Circuit held that the government had to narrowly tailor the privacy regulation to pass constitutional muster.[97] The court reasoned that the FCC could have considered an opt-out consent to accomplish the statute's purpose. And it demonstrated a clear hostility to opt-in requirements of the type promoted in Europe.

The implications for the regulation of Internet enterprises of *U.S. West* were relatively direct. At the most fundamental, the courts made clear that privacy rules regulating the use of consumer information—even by commercial entities—were subject to First Amendment scrutiny. In *U.S. West*, the court held that privacy regulation "implicate[s] the First Amendment by restricting protected commercial speech."[98] In the Supreme Court's 2001 decision in *Bartnicki v. Vopper*, the Court again affirmed that "the naked prohibition against disclosures is fairly

93. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1209 (2004). Whitman observed the American attitude: "Most of all, when they do propose regulation, they tend, in a characteristically American way, to favor 'market-based solutions to personal data protection,' as Pamela Samuelson writes, 'over the strict comprehensive regulatory regime adopted . . . in Europe.'" *Id.* at 1193 (citing Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1127–28 (2000)).

94. *Privacy in the Commercial World: Hearing Before the Subcomm. on Commerce, Trade & Consumer Prot. of the H. Comm. on Energy & Commerce*, 107th Cong. 105 (2001) (statement of Fred H. Cate, Professor of Law, Indiana University Maurer School of Law).

95. U.S. W., Inc. v. FCC, 182 F.3d 1224, 1228 (10th Cir. 1999).

96. *Id.* at 1228–30.

97. *Id.* at 1238–39 ("FCC's failure to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy, indicates that it did not narrowly tailor the [consumer privacy] regulations regarding customer approval.").

98. *Id.* at 1233.

characterized as a regulation of pure speech."[99] The Court repeated: "[T]he acts of disclosing and publishing information . . . constitute speech."[100]

Efforts to regulate consumer information would clearly raise First Amendment scrutiny. As the Tenth Circuit described in *U.S. West*, "the essence of the statutory scheme [at issue in the case] requires a telecommunications carrier to obtain customer approval when it wishes to use, disclose, or permit access to [customer information] in a manner not specifically allowed [by the statute]."[101] The statute targeted specific information about the customer's use of the service: "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[102] As the court described, this included information "such as when, where, and to whom a customer places calls."[103] Translated to the web, such details might include what websites one visited, whom one contacted, and where one was—the precise kind of data that is very attractive for online marketing.

First Amendment concerns also kept strong state privacy laws at bay.[104] For example, in 2011, California considered a law that would adjust the default privacy setting on social networks to not share information and would allow a user to delete personal information about himself or herself from a social network. The bill would have required social networks to remove "personal identifying information" upon the individual's request or, if the individual was a minor, his parents' requests.[105] Silicon Valley advocates argued that California's proposed bill undermined speech, noting that, as written, the "Social Networking Privacy Act" would allow anyone who worked at the California Senate to remove all

99. Bartnicki v. Vopper, 532 U.S. 514, 526 (2001).

100. *Id.* at 527 (internal quotation marks omitted).

101. *U.S. W., Inc.*, 182 F.3d at 1229.

102. *Id.* at 1228 n.1.

103. *Id.*

104. S.B. 501, 2013–2014 Leg., Reg. Sess. (Cal. 2013) (as introduced, Feb. 21, 2013) (requiring social networking sites to remove personal information that is accessible online of any registered users upon their requests or their parents' request if users are minors); S.B. 242, 2011–2012 Leg., Reg. Sess. (Cal. 2011), (prohibiting social networking sites from displaying the home address or phone number of registered users who identified as minors); S.B. 1361, 2009–2010 Leg., Reg. Sess. (Cal. 2010) (prohibiting social networking sites from disclosing the home address or telephone number of minor-registered users to the public or other registered users); Assemb. B. 632, 2009–2010 Leg., Reg. Sess. (Cal. 2009) (requiring social networking sites to provide a disclosure to users that images can be copied without consent or in violation of sites' privacy policies by third parties); Assemb. Con. Res. 106, 2007–2008 Leg., Reg. Sess. (Cal. 2008) (urging Internet intermediaries to work with the Internet Safety Technical Task Force and law enforcement to reduce criminal behaviors taking place online).

105. What would have been section 60(c)(1) of the California Civil Code states: "A social networking Internet Web site shall remove the personal identifying information of a registered user in a timely manner upon his or her request." S.B. 242 § 1.

references to that body from a social network.[106] But even industry criticisms did not fully appreciate the extent of the free speech threat posed by the statute. Essentially, the bill would have codified a kind of mini-"right to be forgotten."[107] It gave users the ability to erase their names from social media sites.[108] Users could stop other people from saying bad things about them, simply by having their names deleted. Negative speech could be removed with a few keystrokes, even if it were truthful. A penalty of $10,000 for each violation, in combination with the onerous obligation of verifying parental-registered user relationships, would ensure that companies would remove information liberally, particularly where minors were concerned.

"[I]nformation is power," Justice Kennedy declared, in his opinion for the Court in 2011.[109] In *Sorrell v. IMS Health*, the Supreme Court dramatically demonstrated the seriousness of First Amendment constraints on privacy regulations on information intermediaries.[110] The Court struck down a Vermont privacy law that prevented pharmacies from sharing physician prescription data for marketing purposes without physician consent.[111] Reasoning that marketing was a protected expressive purpose, the Court held that the statute was a content-based restriction on protected expression.[112] The Court extolled the virtues of free information.[113] Justice Kennedy wrote, "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[114] This included anodyne details of prescription practices. Because consumer privacy laws suppress the gathering, retention, or use of typically mundane facts about individuals, the Court's embrace of facts suggests that consumer privacy law would meet stiff First Amendment challenge.

Does *Sorrell* mean "the death of privacy"?[115] No, but it suggests serious limits to privacy law. Would, for example, a privacy statute targeting only social networks be seen as disfavoring a particular category of speaker? Would a statute

106. Letter from Silicon Valley Leadership Grp. et al., to Sen. Ellen Corbett (May 16, 2011), *available at* http://www.scribd.com/doc/55576694/SB242CoalitionFloorOpppose. A later draft of the bill accordingly removed "place of employment" as a type of personal information subject to takedown requests. *Compare* S.B. 242 § 1 (as amended by Senate, May 25, 2011), *with* S.B. 242 § 1 (as amended by Senate, May 2, 2011).

107. For a discussion of the fuller "right to be forgotten," see *infra* Part III.D.

108. Later drafts would remove one's right to remove one's name from social media sites by amending the definition of "personal identifying information" to exclude one's name. *Compare* S.B. 242 § 1 (as amended by Senate, May 2, 2011), *with* S.B. 242 § 1 (as introduced, Feb. 9, 2011).

109. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2671 (2011) (quoting a Vermont physician).

110. *See id.* at 2659.

111. *Id.*

112. *Id.* at 2672.

113. *Id.* at 2671–72.

114. *Id.* at 2667.

115. *See* Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 856 (2012) (noting that "the majority's opinion contains broad hints" which would "have dramatic . . . implications" for future regulations "that seek to control the disclosure of personal information").

requiring explicit consent before the use or sharing of a user's personal information be seen as insufficiently narrowly tailored when an opt-out mechanism might have been used? As Justice Kennedy writes, "The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[116]

D. THE FREE SPEECH STRUCTURE OF CYBERLAW

In fits and starts, Congress and the courts recognized that broad liabilities on Internet intermediaries would impinge on the speech of ordinary persons. In so doing, they were translating the logic of *New York Times Co. v. Sullivan* to the information age. *Sullivan* marked its 50th anniversary in 2014.

Sullivan understood that free speech depends on a free press. In that case, a "rule of liability" was held to "abridge[] the freedom of speech and of the press."[117] Where earlier the First Amendment had focused on direct governmental regulation, *Sullivan* recognized that speech could be burdened indirectly, by delegating the right to sanction speech to private parties. Laws aimed at speech intermediaries implicated the speech of ordinary persons. This would be true even if it were simply private parties suing other private parties. The Court recognized that a private claim would cause the newspaper to avoid such controversial topics in the future.[118] In *Sullivan*, when private citizens criticized Alabama officials through an advertisement in the *New York Times*, the officials sued the deep-pocketed newspaper that published their advertisement. A liberal liability rule against the newspaper would, the Supreme Court understood, undermine the speech of those persons who had posted the advertisement. The Court recognized that advertising itself was a direct form of speech by persons other than the press, and that liberally allowing liability arising out of these advertisements would lead the newspaper to sharply curtail what was said in its advertisements:

> Any other conclusion would discourage newspapers from carrying "editorial advertisements" of this type, and so might shut off an important outlet for the promulgation of information and ideas by persons who do not themselves have access to publishing facilities—who wish to exercise their freedom of speech even though they are not members of the press.[119]

Even though the Court described the danger as "self-censorship," in fact the problem was that the *New York Times* would not only censor itself, it would censor third parties in the future by refusing to accept advertisements on controversial topics. A contrary ruling would have essentially privatized censorship.

116. *Sorrell*, 131 S. Ct. at 2672.

117. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 268, 292 (1964).

118. *Id.* at 279 ("A rule compelling the critic of official conduct to guarantee the truth of all his factual assertions—and to do so on pain of libel judgments virtually unlimited in amount—leads to a comparable 'self-censorship.'").

119. *Id.* at 266.

Private liability regimes are one-directional: Liability arises only if the speech intermediary publishes the speech, not if it censors it. Thus, the slightest uncertainty resolves in favor of censorship. Private law can thus function as a one-way ratchet towards censorship. This incentivizes broad suppression of speech, and so, must be scrutinized with care.[120] The constitutional interest in such cases is significant because the regulation does not target only "low-value" speech (instead sweeping in both high-value and low-value speech) and because the very ability of speech intermediaries to carry on may be at stake. Even if the regulation itself appears content neutral, the effect of the liability regime will be to deter controversial speech, the speech at the edges of what might invoke liability.[121] Censor or shutter.

Sullivan held that even speech paid for by private parties and posted as an advertisement was constitutionally protected—that the commercial context of the speech did not take it outside the First Amendment. Furthermore, the case involved statements that were actual untruths (which the *New York Times* itself admitted). Even still, the *Times* was excused. To hold otherwise would substantially chill speech.

The Internet would take us much farther towards the promise of free speech than even a *New York Times* freed of stiff defamation judgments. Recall that the advertisement taken out in the *Times* cost $4800 in 1960, beyond the means of most ordinary persons (the average yearly income per family at the time was $5600).[122] The Internet allows members of the public to speak directly to the country, even without the hundreds of thousand dollars required to take out a similar advertisement today.[123] All one needs to join Facebook or Twitter is access to a computer and an email address (the latter available for free).[124] In theory, one does not need a Silicon Valley intermediary to do this, as the World Wide Web is designed to enable ordinary persons to share a webpage viewable on all connected computers. But experience taught us that social networks were crucial to enabling

120. *See* Ashutosh Bhagwat, *The Test That Ate Everything: Intermediate Scrutiny in First Amendment Jurisprudence*, 2007 U. ILL. L. REV. 783, 801 (describing intermediate scrutiny as requiring that the law "serve some sort of a significant/substantial/important governmental interest and [be] reasonably well tailored to that purpose" (emphasis omitted)).

121. Marjorie Heins, *Viewpoint Discrimination*, 24 HASTINGS CONST. L.Q. 99, 122 (1996) ("Speech that is controversial, that 'induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger,' is precisely the speech most in need of constitutional protection." (quoting Texas v. Johnson, 491 U.S. 397, 408–09 (1989))).

122. BUREAU OF THE CENSUS, U.S. DEP'T OF COMMERCE, SERIES P-60, NO. 36, CURRENT POPULATION REPORTS: CONSUMER INCOME 1 (1961), *available at* http://www2.census.gov/prod2/popscan/p60-036.pdf.

123. The *New York Times* now charges up to approximately $241,000 for full-page advertisements. *See supra* note 6.

124. Though hardly universal, Internet access is increasing in the United States, fairly widespread across economic strata and demographic groups. Among American families, 74.8% have Internet access from home. U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, MEASURING AMERICA: COMPUTER & INTERNET TRENDS IN AMERICA 1 (2014), *available at* http://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf.

information to reach a broader audience. Facebook, Twitter, and Google enabled users to "follow" others, collecting all their "friends'" posts in one easy-to-read page and allowing for a kind of 24-hour-a-day virtual salon to occur. Being held liable for the speech of their users would lead these services to censor material liberally, or to shut down if such censorship proved practically impossible. After all, the small additional revenues attributable to controversial speech might well not justify the expected costs of a lawsuit or a judgment.

The American commitment to free speech also rebuffs efforts to enact broad privacy protections. *U.S. West* and *Sorrell* demonstrated that the First Amendment serves as a significant check on the kinds of privacy protections that might be imposed on Internet intermediaries. The Supreme Court's 2001 decision in *Bartnicki* held that a privacy-related wiretapping claim brought by one private party against another implicated speech, and thus, had to pass First Amendment muster. The case again relied on the logic of *Sullivan*.

When it comes to speech, Internet intermediaries are likely to be ensnared, caught in the middle of the worldwide war fueled by copyright interests, users' privacy, and governments' desire to control what is said and to listen in on what people are saying. Internet intermediaries are often the most vulnerable and effective points of control for any government keen on controlling speech. We thus turn to some of the most important contemporary cyberlaw conflicts, demonstrating that the contest over the contours of free speech underlies them all.

III. KEEPING SPEECH *FREE*

Today's speech law is being made in the major cyberlaw disputes of the day. Recognizing the free speech structure of cyberlaw helps us understand that today's major cyberlaw disputes will configure the possibility of free speech in the days to come.

We review here the following Internet controversies: SOPA, a bill that would have enhanced public and private copyright enforcement powers; the intellectual property chapter of the proposed Trans-Pacific Partnership free trade agreement; the United States government's seizure of domain names in connection with copyright infringement claims; efforts to increase the United Nations' control over the Internet through the International Telecommunication Union ("ITU"); the EU's proposed "right to be forgotten"; the new technologies of Web 3.0 and the Internet of Things; and finally, the ubiquitous surveillance of electronic records by the United States government.

A. SOPA STRIKES BACK

January 18, 2014, marked the second anniversary of the "SOPA Blackout," which—like the "A Thousand Points of Darkness" protest in 1995—now seems like a forgotten floppy disk of the digital age. But the threats raised by SOPA remain. They have migrated away from the public halls of Congress to the more secretive world of international diplomacy. Two mega-trade treaties, the Trans-Pacific Partnership Agreement ("TPP") and the Transatlantic Trade and

Investment Partnership ("TTIP"), seek to establish free trade from Asia across the Pacific and then across the Atlantic, with the United States as its epicenter. To understand what is at stake in TPP and TTIP, we must first briefly revisit SOPA.

SOPA sought to make U.S. copyright and trademark holders global censors.[125] Introduced on October 26, 2011, in the House of Representatives, SOPA sought to enhance public and private power to shutter Internet sites on behalf of copyright interests.[126] In November, opponents declared an "American Censorship Day."[127] Then on January 18, 2012, Google and other sites slapped a black band across their logo, visually recalling the censorship of an analog age, while other sites, like Wikipedia, blacked out their site entirely.[128] The perceived threat to speech was made plain in the most dramatic terms.

Proponents cast the bill as necessary to combat foreign websites that facilitate infringement of U.S. copyrights. SOPA would have permitted copyright holders and the U.S. Department of Justice to seek court orders against foreign websites accused of facilitating copyright infringement.[129] But it would go much further than restraining alleged foreign rogues through the courts. The bill defined "U.S.-directed sites" to include sites *inside* the United States, even ones without any foreign component.[130] Such a site would be declared "dedicated to theft of U.S. property" if its owner had "taken . . . deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out" infringement.[131] Given that almost any site with user-generated content will include copyright-infringing work, even ordinary sites might then be declared rogue. The bill imposed a secondary boycott,[132] under which any intellectual property holder could require companies to either remove a "rogue" site from search results or to cease payment

125. *See* Stop Online Piracy Act, H.R. 3261, 112th Cong. §§ 102(c)(2), 103(b), (d)(2) (2011). A companion bill was introduced in the Senate as the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PIPA"). S. 968, 112th Cong. (2011).

126. The Senate version of the bill, PIPA, would have had similar adverse impacts on speech. *See* Letter from John R. Allison et al., Professor, McCombs Sch. of Bus., Univ. of Tex. at Austin, to U.S. Cong. (July 5, 2011), *available at* http://www.wyden.senate.gov/download/?id=8255 7539-159c-4237-b6a0-27d0d43b7797&download=1. (One of us, Anupam Chander, was a signatory to this letter.)

127. *See, e.g.*, Parker Higgins, *American Censorship Day Is This Wednesday—And You Can Join In!*, ELEC. FRONTIER FOUND. (Nov. 10, 2011), http://www.eff.org/deeplinks/2011/11/american-censorship-day-wednesday-and-you-can-join.

128. David Drummond, *Don't Censor the Web*, GOOGLE OFFICIAL BLOG (Jan. 17, 2012), http://googleblog.blogspot.com/2012/01/dont-censor-web.html.

129. H.R. 3261 § 102(b), (c)(2).

130. *Id.* § 101(23) ("The term 'U.S.-directed site' means an Internet site or portion thereof that is used to conduct business directed to residents of the United States . . . .").

131. *Id.* § 103(a)(1), (a)(1)(B)(ii)(I).

132. Secondary boycotts themselves raise First Amendment issues, Barbara J. Anderson, Comment, *Secondary Boycotts and the First Amendment*, 51 U. CHI. L. REV. 811, 817, 819–22 (1984), though the Supreme Court has rejected a First Amendment challenge to material support for terrorism. Holder v. Humanitarian Law Project, 561 U.S. 1, 8 (2010); David Cole, *The First Amendment's Borders: The Place of* Holder v. Humanitarian Law Project *in First Amendment Doctrine*, 6 HARV. L. & POL'Y REV. 147, 152 (2012).

or advertisement services.[133] More subtly, SOPA also induced, through a promise of immunity, websites and Internet service providers to proactively avoid, again without a court order, sites that might be found to be "dedicated to theft of U.S. property."[134]

The speech implications of the bill were astonishing. Any Internet website that hosted content supplied by users could be said to facilitate copyright infringement because users routinely post infringing material as a form of online sharing. The social web was at risk. The bill gave intellectual property holders the right to block financial and advertising support for websites "dedicated" to theft. Such a power would impinge on the speech of both the intermediaries—denied the right to advertise even without adversary proceedings establishing a primary violation—and the target website—denied the lifeblood of a business, funding and advertising. More importantly, the speech of multitudes of users was at stake because the platforms for their speech might disappear in the face of such risks. Moreover, the rights of intellectual property holders would trump the speech of both Internet intermediaries, target websites, and individual users, even without judicial determinations of infringement. Laurence Tribe denounced the statute for creating prior restraints.[135] More pernicious, however, the statute would constrain speech, even without intellectual property holders lifting a finger. The incentive of immunity for proactively refusing to deal with sites "dedicated" to theft would lead many services to blacklist sites that intellectual property holders might disfavor. By making private companies responsible for their users, SOPA would, as Rebecca MacKinnon observed, "emulate China's system of corporate 'self-discipline.'"[136]

If SOPA had been implemented, parts of the Internet would have effectively gone dark—denied domain names or advertising revenues—and been banned from search engines. The targets would not simply be "rogue" sites, whose *raison d'être* was an intellectual property violation, but also possibly sites like Etsy, selling some million handmade goods, some of which might infringe (handmade Mickey Mouse Club party hats, for example[137]). In this way, SOPA would jeopardize all sites containing user-generated content, including even such foundational services

133. H.R. 3261 § 103(b)(1)–(4) (requiring payment or advertising services to stop serving websites that an intellectual property owner claims violate its intellectual property).

134. *Id.* § 104, 104(1) ("[N]o liability for damages to any person shall be granted against, a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar for . . . voluntarily blocking access to or ending financial affiliation with an Internet site, in the reasonable belief that . . . the Internet site is a foreign infringing site or is an Internet site dedicated to theft of U.S. property . . . .").

135. Laurence H. Tribe, The "Stop Online Piracy Act" (SOPA) Violates the First Amendment 7–11 (Dec. 6, 2011) (unpublished manuscript), *available at* http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1.

136. Rebecca MacKinnon, Op-Ed., *Stop the Great Firewall of America*, N.Y. TIMES (Nov. 15, 2011), http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html.

137. *See* Search Results for "Mickey Mouse Club Party Hats," ETSY, http://www.etsy.com/search/handmade?q=mickey+mouse+club+party+hats. We are not suggesting that such items, in fact, infringe either copyright or trademark, but that they could conceivably be found to be infringing.

as Google or Facebook. This is not a fanciful hypothetical. In January 2012, Fox's Rupert Murdoch took to Twitter to accuse Google of being a "[p]iracy leader."[138] A prominent advertising firm listed the Internet Archive, Vimeo, and SoundCloud among a list of pirate sites.[139] Twitter's then-general counsel, Alex Macgillivray, illustrated the impact on speech of ordinary individuals through the hypothetical teacher Abe:

> Abe may wake up one morning and not be able to access any of his photos of his children. Neither he, nor his students, would be able to access any of his lectures. His trove of smart online discussions would likewise evaporate and he wouldn't even be able to complain about it on his blog.[140]

Some seven million people signed a petition that helped convince Congress to set SOPA aside.[141] This act of speech, which was only made possible by the awareness facilitated by speech intermediaries,[142] had protected speech itself.

At least temporarily. If we can't have intermediary policing imposed through domestic law, perhaps an international agreement might do the trick.[143] Led by the United States, a group of countries on both sides of the Pacific is negotiating what is heralded as a "landmark, 21st-century trade agreement."[144] In the latest leaked

138. Murdoch tweeted, "Piracy leader is Google who streams movies free, sells [advertisements] around them." David Carr, *A Glimpse of Murdoch Unbound*, N.Y. TIMES (Jan. 29, 2012), http://www.nytimes.com/2012/01/30/business/media/twitter-gives-glimpse-into-rupert-murdochs-mind.html.

139. Mike Masnick, *Universal Music Goes to War Against Popular Hip Hop Sites & Blogs*, TECHDIRT (June 20, 2011, 11:22 AM), http://www.techdirt.com/articles/20110620/01370314750/universal-music-goes-to-war-against-popular-hip-hop-sites-blogs.shtml.

140. Alex Macgillivray, *Overbroad Censorship & Users*, BRICOLEUR (Dec. 11, 2011), http://www.bricoleur.org/2011/12/overbroad-censorship-users.html.

141. David A. Fahrenthold, *SOPA Protests Shut Down Web Sites*, WASH. POST (Jan. 18, 2012), http://www.washingtonpost.com/politics/2012/01/17/gIQA4WYl6P_story.html; *SOPA Petition Gets Millions of Signatures as Internet Piracy Legislation Protests Continue*, WASH. POST (Jan. 20, 2012), http://articles.washingtonpost.com/2012-01-19/business/35440878_1_protest-against-anti-piracy-sopa-and-pipa-internet-piracy.

142. *Petition to Google: Please Put Information About SOPA on Your Main Page, the Homepage of Millions upon Millions of Americans, to Inform the Average Web User About What May Happen to Their Internet on December 21*, OCCUPY WALL ST. (Dec. 17, 2011), http://www.occupythegame.com/2011/12/17/petition-to-google-please-put-information-about-sopa-on-your-main-page-the-homepage-of-millions-up on-millions-of-americans-to-inform-the-average-web-user-about-what-may-happen-to-their-internet-on. During Wikipedia's 24-hour blackout period, its SOPA and PIPA page (which remained accessible) was viewed more than 162 million times, with more than eight million looking up legislators' contact information. *Wikipedia: SOPA Initiative/Learn More*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wikipedia:SOPA_initiative/Learn_more (last visited Oct. 26, 2014).

143. This represents what some have called "regime shifting." *See* Laurence R. Helfer, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking*, 29 YALE J. INT'L L. 1, 6–7 (2004).

144. *Enhancing Trade and Investment, Supporting Jobs, Economic Growth and Development: Outlines of the Trans-Pacific Partnership Agreement*, OFFICE OF THE U.S. TRADE REPRESENTATIVE, http://www.ustr.gov/about-us/press-office/fact-sheets/2011/november/outlines-trans-pacific-partnership-agreement (last visited Oct. 26, 2014). Countries currently negotiating the TPP include Australia, Brunei, Canada,

version, made available by Wikileaks rather than the *New York Times*, the TPP includes important free flow of data obligations that facilitate free speech, but also includes a chapter on intellectual property that would require member states to adopt strict intermediary liability obligations for Internet service providers.[145] We focus here on that latter chapter.[146]

A close reading of the leaked draft of this chapter reveals SOPA-like ambitions.[147] The leaked TPP proposal would require that states provide "legal incentives for service providers to cooperate with copyright owners in deterring the unauthorized storage and transmission of copyrighted materials."[148] The focus here is on *deterrence*—not notice and takedown, which happens after the fact. How might we provide a legal incentive for service providers to deter infringement? An ideal formulation of such a "legal incentive" for deterrence regime is SOPA—which in section 104 would have provided "immunity for taking voluntary action against sites dedicated to theft."[149] Rather than rely on copyright holders to notify the intermediary of the alleged infringement, the intermediary would itself police its site, deleting material that some might claim was infringing. Fair use would be at the mercy of speech intermediaries that had a legal incentive only to take material down, not to keep it up—a legal incentive, that is, to censor material, not to publish it.

The U.S.' goal in this provision is not simply to export DMCA title II, with its safe harbors for well-behaved intermediaries that take down allegedly infringing material following appropriate notice. Indeed, the TPP makes this clear: the "legal incentives" for deterrence are *in addition to* DMCA title II-like safe harbors.[150] By creating a legal regime that encourages providers to prevent potentially infringing activity, the proposed TPP intellectual property chapter risks transforming Internet providers into Internet censors.

Thus, the threats from SOPA are alive, global, and unfortunately, avoiding public engagement. Unlike the SOPA discussion, where the collective power of

Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam, and the United States. *Trans-Pacific Partnership (TPP)*, OFFICE OF THE U.S. TRADE REPRESENTATIVE, http://www.ustr.gov/tpp (last visited Oct. 26, 2014).

145. WIKILEAKS, SECRET TPP TREATY: ADVANCED INTELLECTUAL PROPERTY CHAPTER FOR ALL 12 NATIONS WITH NEGOTIATING POSITIONS (2013) [hereinafter TPP IP PROPOSAL 2013], *available at* https://wikileaks.org/tpp/static/pdf/Wikileaks-secret-TPP-treaty-IP-chapter.pdf. The United States's own IP proposal to the TPP was leaked on Feb. 10, 2011. KNOWLEDGE ECOLOGY INT'L, TRANS-PACIFIC PARTNERSHIP INTELLECTUAL PROPERTY RIGHTS CHAPTER (2011) [hereinafter U.S. TPP IP PROPOSAL], *available at* http://keionline.org/sites/default/files/tpp-10feb2011-us-text-ipr-chapter.pdf.

146. For a comprehensive analysis of the U.S. TPP IP Proposal, see generally Sean M. Flynn et al., *The U.S. Proposal for an Intellectual Property Chapter in the Trans-Pacific Partnership Agreement*, 28 AM. U. INT'L L. REV. 105 (2012).

147. *See generally* TPP IP PROPOSAL 2013, *supra* note 145.

148. *Id.* at 86. *Compare id.*, *with* U.S. TPP IP PROPOSAL, *supra* note 145, at 32 (requiring that states provide "legal incentives for service providers to cooperate with copyright owners in deterring [copyright infringement]").

149. H.R. 3261, 112th Cong. § 104 (2011).

150. TPP IP PROPOSAL 2013, *supra* note 145, at 86.

individual speech was demonstrated, the negotiations towards a TPP are reserved for speech by a select few. As for the transatlantic agreement, we will likely have to wait for the next revelation by Wikileaks to learn whether TTIP poses the same dangers to speech.

B. CRIMINAL DOMAINS: MEGAUPLOAD AND ROJADIRECTA

The day after the massive protest that doomed SOPA, authorities around the world descended on the cloud service Megaupload.[151] In Hong Kong, a hundred policemen entered luxury hotel suites, homes, and offices, seizing computer servers and millions of dollars in cash.[152] In the United States, authorities seized ten domain names associated with the service.[153] Meanwhile, police in New Zealand descended by helicopter at the home of Megaupload's flamboyant founder, Kim Dotcom, cutting their way into his panic room.[154] On January 20, 2012, users who had posted material to the Megaupload storage lockers, or others who sought access to those materials, now encountered an FBI anti-piracy warning.

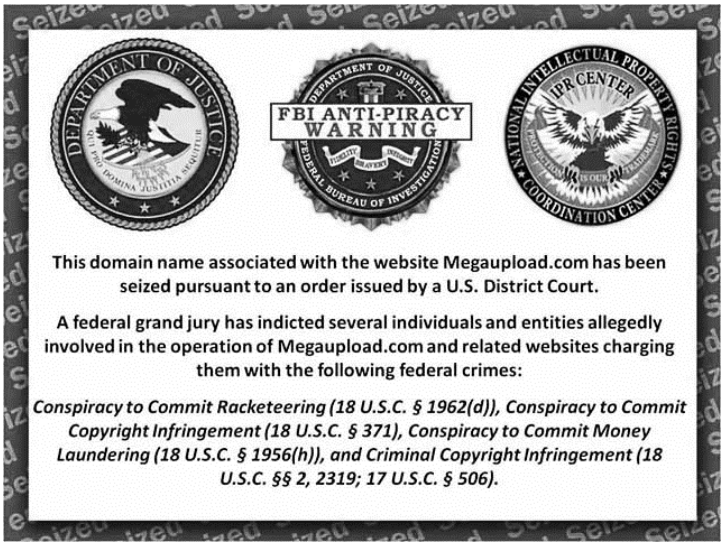
151. Press Release, Office of Pub. Affairs, U.S. Dep't of Justice, Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement (Jan. 19, 2012), *available at* http://www.justice.gov/opa/pr/2012/January/12-crm-074.html.

152. *HK Customs-US Authorities Co-operation Smashes a Transnational Piracy Syndicate with over HK$300 Million Worth of Crime Proceeds Restrained*, NEWS.GOV.HK (Jan. 20, 2012, 11:32 PM), http://www.info.gov.hk/gia/general/201201/20/P201201200626.htm; *HK Seizes $330 M in Megaupload Raids*, RADIO TELEVISION HONG KONG (Jan. 21, 2012), http://www.rthk.org.hk/rthk/news/englishnews/news.htm?all&20120121&56&813245.

153. The names were all ".coms." *See* Application for a Warrant to Seize Property Subject to Forfeiture at 2, United States v. Dotcom, No. 1:12-cr-3, 2012 WL 4788433 (E.D. Va. filed Nov. 15, 2012), ECF No. 145-1, *available at* http://www.eff.org/files/filenode/145.1_search_warrant_partially_unsealed_11.15.12.pdf.

154. Charles Graeber, *Inside the Mansion—and Mind—of Kim Dotcom, the Most Wanted Man on the Net*, WIRED (Oct. 18, 2012, 6:30 AM), http://www.wired.com/2012/10/ff-kim-dotcom/all. The luxury cars seized during the arrest bore license plates such as "Hacker," "V," "CEO," "Mafia," "Stoned," and "Police." Robin Wauters, *Downfall: Photos of MegaUpload Founder's Valuable Cars Getting Seized*, TECHCRUNCH (Jan 20, 2012), http://techcrunch.com/2012/01/20/downfall-photos-of-megaupload-founders-valuable-cars-getting-seized/.

Figure 2. The anti-piracy warning posted by the FBI on the Megaupload website, January 2012.



A year earlier, the U.S. government had seized Rojadirecta.com and Rojadirecta.org, domain names operated by Puerto 80, a Spanish company. The authorities accused the sites of facilitating copyright infringement by collecting links to often unauthorized videos of sporting events around the world. The seizure occurred without prior notice to the website owners, and without any adversarial hearing.[155]

To seize the domain names in both cases, the United States relied on civil seizure and forfeiture triggered on the claim that the domain names "had been used to commit and facilitate . . . criminal copyright infringement."[156] The law permitting seizure did not require either Megaupload or Rojadirecta themselves to have committed a crime, only that the domain names were "used, or intended to be used, in any manner or part to commit or facilitate" copyright infringement.[157] The Megaupload and Rojadirecta seizures followed the model of earlier actions,[158] in

155. *See* Opening Brief and Special Appendix for Petitioner-Appellant Puerto 80 Projects, S.L.U. at 26, Puerto 80 Projects, S.L.U. v. United States, No. 11-3390-cv, 2011 WL 4440567 at *17 (2d Cir. filed Sept. 16, 2011), ECF No. 38.

156. Brief for the United States of America at 12–13, *Puerto 80 Projects*, 2011 WL 5833572, at *2, *5 (2d Cir. filed Sept. 15, 2011), ECF No. 70, *available at* http://www.eff.org/files/filenode/Puerto80.Govt_.Brief_.pdf; *see also* 17 U.S.C. § 506(a)(1)(A), (C) (2012); 18 U.S.C. §§ 2, 981(b), 2319(b), (d)(2), 2323 (2012); Indictment at 2, 9–10, *Dotcom*, 2012 WL 4788433 (E.D. Va filed Jan 5, 2012), ECF No. 1, *available at* http://www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf.

157. 18 U.S.C. § 2323(a)(1)(B).

158. Prior to the seizure of Megaupload, the government's Internet anti-copyright infringement program, titled "Operation in Our Sites," had already seized 350 domain names. *Operation in Our Sites Protects American Online Shoppers, Cracks Down on Counterfeiters*, U.S. IMMIGRATION & CUSTOMS

which the U.S. government seized domain names, mainly by targeting VeriSign, a Virginia company that manages .com, .net, .cc, and .tv top-level domains, and the Public Interest Directory, a Virginia company that manages .org.[159] This combination revealed that the United States already had an authority proposed in SOPA—the power to shut down at least some foreign websites accused of facilitating infringement without trial in ex parte proceedings.[160]

The seizures harmed speech, and in some cases, permanently destroyed it. Rojadirecta, for example, not only hosted links to video streams, but also provided forums for sports discussions. The seizure thus denied its 865,000 registered users access to discussion forums, and given that Rojadirecta ranked among the top 100 most trafficked websites, interfered with many users' access to information.[161] On the other hand, the seizure actually destroyed speech in Megaupload's case. Megaupload's 5.86 million registered users[162] could no longer access their writing, photos, videos, or audio recordings in Megaupload's cloud—an astonishing 40 petabytes' worth of material.[163] Neither could others who might want to access or download material posted by the registered users, whether it was a song parody, a document, or a cute cat video. Certainly, a significant percentage of the material was likely to be copyright infringing, but the seizure indiscriminately barred access

ENFORCEMENT (Nov. 28, 2011), http://www.ice.gov/news/releases/1111/111128washingtondc.htm.

159. *See* David Kravets, *Uncle Sam: If It Ends in .Com, It's .Seizable*, WIRED (Mar. 6, 2012, 6:30 AM), http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/ ("[T]he U.S. government . . . has the right to seize any .com, .net and .org domain name because the companies that have the contracts to administer them are based on United States soil . . . ." (paraphrasing Nicole Navas, U.S. Immigration and Customs Enforcement spokeswoman)).

160. Civil forfeiture is problematic even outside the free speech context. *See* Sarah Stillman, *Taken*, NEW YORKER (Aug. 12, 2013), http://www.newyorker.com/magazine/2013/08/12/taken (describing use of civil forfeiture by police departments across the country to bolster falling budgets by seizing cars and cash).

161. Opening Brief and Special Appendix for Petitioner-Appellant Puerto 80 Projects, S.L.U., *supra* note 155, at 14–15.

162. According to the U.S. government, Megaupload has 66.6 million total registered users, and 5.86 million who have ever uploaded a file. Introduction and Summary of Evidence at 15, United States v. Dotcom, No. 1:12-cr-3, 2012 WL 4788433 (E.D. Va. Nov. 22, 2013), *available at* http://www.justice.gov/usao/vae/victimwitness/mega_files/Mega%20Evidence.pdf. Compare with the number of registered users of 180 million claimed by Megaupload. *Id.* at 2.

163. Cyrus Farivar, *Kim Dotcom Says Dutch Firm Deleted "At Least 40 Petabytes" of Megaupload Data*, ARS TECHNICA (June 26, 2013, 6:36 PM), http://arstechnica.com/tech-policy/2013/06/kim-dotcom-says-dutch-firm-deleted-at-least-40-petabytes-of-megaupload-data/. Users could attempt to retrieve their data through MegaRetrieval, a joint project created by third party Carpathia Hosting, Megaupload's hosting service provider, and the Electronic Frontier Foundation. Press Release, Carpathia Hosting, Inc., Carpathia Hosting to Assist Electronic Frontier Foundation: Website to Help Connect End-Users with EFF to Assess Options (Jan. 31, 2012), *available at* http://www.megaretrieval.com/files/Carpathia_PressRelease_Jan3112.pdf. While the district judge ordered the preservation of the seized data, there was no facility provided to pay for the hosting service for maintaining this enormous amount of data. *See* Greg Sandoval, *Judge Wants MegaUpload User Data Preserved for Now*, CNET (Apr. 13, 2012, 8:36 AM), http://news.cnet.com/8301-1023_3-57413693-93/judge-wants-megaupload-user-data-preserved-for-now/.

to both infringing and non-infringing content. The Department of Justice offered that a user could retrieve data where he could "demonstrate whether he has an interest in any property seized," which "may require the testimony of numerous witnesses, including potential expert witnesses."[164] Given the site's 5.86 million users storing files on the Megaupload clouds, sorting through legitimate and illegitimate claims might seem a formidable task. Denied its domain name and access to its bank accounts, Megaupload could no longer finance its hosting service to continue keeping the data (a reported cost of at least $9000 per day) while it fought the case in the courts.[165] Users have not recovered their lost files as of this writing and many will never recover it at all. Denounced as "the largest data massacre in the history of the [I]nternet," Megaupload's 630 servers of data have been wiped clean by one of its hosting service providers.[166] Nineteen petabytes of data were destroyed, the equivalent of 1945 times the U.S. Library of Congress print collection.[167] The fate of another 1103 servers, containing 25 petabytes, remains uncertain.

Puerto 80 argued that the domain name seizure amounted to an unconstitutional "prior restraint on speech."[168] The district court rejected Puerto 80's efforts to have the domain names restored, pending review on the merits.[169] District Judge Paul Crotty observed, "[a]lthough some discussion may take place in the forums, the fact that visitors must now go to other websites to partake in the same discussions is clearly not the kind of substantial hardship that Congress intended to ameliorate."[170] Puerto 80 could, and did, transfer its service to other domains (.es, .me, and .in, for example), but this interrupted user access and likely lost users in the process.[171] Puerto 80, in fact, pleaded with its users, "¡SPREAD

164. Brief of the United States Regarding the Breadth and Format of a Hearing to Determine the Applicability of Federal Rule of Criminal Procedure 41(g) at 1, 6, *Dotcom*, 2012 WL 4788433 (E.D. Va. filed Oct. 30, 2012), ECF No. 136, *available at* http://www.wired.com/images_blogs/threatlevel/2012/10/fedsbrief.pdf.

165. Timothy B. Lee, *ISP: Storing 25 Petabytes of Megaupload Data Costs Us $9,000 a Day*, ARS TECHNICA (Mar. 22, 2012, 1:45 PM), http://arstechnica.com/tech-policy/2012/03/isp-storing-25-petabytes-of-megaupload-data-costs-us-9000-a-day/.

166. Nathan Olivarez-Giles, *Kim Dotcom Tweets Outrage After LeaseWeb Deletes All Megaupload Data*, VERGE (June 19, 2013, 3:13 PM), http://www.theverge.com/2013/6/19/4445660/leaseweb-megaupload-kim-dotcom-dispute-twitter.

167. SAS INST. INC., BIG DATA MEETS BIG DATA ANALYTICS 1 (2012), *available at* http://www.sas.com/resources/whitepaper/wp_46345.pdf ("[Ten] terabytes could store the entire US Library of Congress print collection.").

168. Opening Brief and Special Appendix for Petitioner-Appellant Puerto 80 Projects, S.L.U., *supra* note 155, at 22.

169. *Id.* at 18.

170. Order at 4, Puerto 80 Projects, S.L.U. v. United States, No. 11-cv-04139-PAC (S.D.N.Y. filed Aug. 4, 2011), ECF No. 15, *available at* http://www.scribd.com/fullscreen/61674939.

171. *See* MGEF, *Update: Rojadirecta.org Is Now Rojadirecta.es*, TUMBLR (Feb. 1, 2011, 3:15 PM), http://megustaelfutbol.tumblr.com/post/3053958553/update-rojadirecta-org-is-now-rojadirecta-es. By contrast, Megaupload could not transfer its service to another domain name because its monies had also been seized.

our new address!"[172] On appeal to the U.S. Court of Appeals of the Second Circuit, the government acknowledged the users' free "speech rights in Rojadirecta's chat forums" but argued that they could be exercised elsewhere.[173] The government relied upon a Supreme Court decision upholding the incidental burden on speech imposed by the closure of an adult bookstore.[174] But the bookstore case was inapposite because it did not involve a prior restraint; the bookstore had been found to be hosting illegal prostitution in a contested proceeding. The Rojadirecta case ended with a whimper. Eighteen months after the seizure, the U.S. government returned the domain names and abandoned its case without explanation.[175]

The domain name seizure seemed to fit the classic fact pattern for a prior restraint: "administrative and judicial orders forbidding certain communications when issued in advance of the time that such communications are to occur."[176] Such an order would be especially constitutionally suspect when the speech had been curtailed "without a prior judicial determination" of illegality.[177]

A domain name seizure operates both as a punishment for prior speech and a prior restraint on future speech. Domain name seizures are particularly troubling when they interfere with the access of thousands, or even millions of users, to forums for sharing information. Domain name seizures in this context almost invariably impinge on protected speech, with the real consequence of certainly destroying them. A blunderbuss approach to a problem, they are not narrowly tailored to target the actual offense. The First Amendment should require the use of "more sensitive tools"[178] than domain name seizures.

The United States cannot translate its de facto control of the most significant parts of the domain name space into a de facto system of licensing speech. Anyone placing material on a .com or a .org space should not have to worry that they might wake up to find their site disappeared for the offense it offered to the U.S. government. Yet through the TPP, the United States is globalizing this de facto system of speech licensing. In addition to the SOPA-like provisions that incentivize monitoring, both the U.S. proposal and the official TPP proposal would

172. *Id.*

173. Brief for the United States of America, *supra* note 156, at 32.

174. *Id.* at 25–27, 29–30, 32; *see* Arcara v. Cloud Books, Inc., 478 U.S. 697, 702 (1986).

175. Mike Masnick, *Oops: After Seizing & Censoring Rojadirecta for 18 Months, Feds Give Up & Drop Case*, TECHDIRT (Aug. 29, 2012, 12:45 PM), http://www.techdirt.com/articles/20120829/12370820209/oops-after-seizing-censoring-rojadirecta-18-months-feds-give-up-drop-case.shtml.

176. Alexander v. United States, 509 U.S. 544, 550 (1993) (emphasis omitted) (internal quotation marks omitted) (citing MELVILLE B. NIMMER, NIMMER ON FREEDOM OF SPEECH: A TREATISE ON THE THEORY OF THE FIRST AMENDMENT § 4.03 (1984)).

177. *Id.* at 551; *see also* N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (holding as unconstitutional prior-restraint effort to censor publication of national security information without legal hearing).

178. *See* Speiser v. Randall, 357 U.S. 513, 525 (1958) (noting that separating legitimate from illegitimate speech requires "sensitive tools").

add aiding-and-abetting liability for criminal copyright infringement[179] to civil forfeiture—the main legal basis behind these high profile domain seizures.[180] Introduced in the U.S. Copyright Act of 1909,[181] aiding-and-abetting liability for copyright infringement was actually removed in the Copyright Act of 1976.[182] Nevertheless, the United States charged Megaupload under both a direct criminal copyright theory and for aiding and abetting such infringement, using the general aiding-and-abetting statute coupled with the underlying criminal copyright infringement offense.[183] That case remains unresolved with regards to aiding-and-abetting liability.

The fundamental concern is that broad criminal aiding-and-abetting liability for copyright infringement will drive speech intermediaries to censor broadly, lest they be held criminally responsible for the speech of their users. The threat of aiding-and-abetting criminal copyright liability might render the DMCA title II safe harbors meaningless because companies could still be indicted as aiders and abettors.[184] Incentivizing monitoring obligations, increasing criminal liability, and displacing safe harbor protection effectively negate the goal of the DMCA safe harbors "not [to] give the online service providers an excessive incentive to censor."[185]

C. THE UNITED NATIONS OF CENSORS

When governments have censored speech, they have often been criticized both by other governments and civil society.[186] What if a government could cite an

179. *U.S. TPP IP Proposal*, *supra* note 145, at 30 ("Parties shall ensure that criminal liability for aiding and abetting is available under its law."); *see also TPP IP Proposal 2013*, *supra* note 145, at 79 ("Parties shall ensure that criminal liability for aiding and abetting is available under its law.").

180. *TPP IP Proposal 2013*, *supra* note 145, at 80 ("[J]udicial authorities shall have the authority to order the forfeiture or destruction of . . . materials and implements . . . used in the creation of pirated copyright goods . . . .").

181. Copyright Act of 1909 § 28, Pub. L. No. 60-349, 35 Stat. 1075, 1082 (repealed 1976) ("That any person . . . who shall knowingly and willfully aid or abet such infringement, shall be deemed guilty of a misdemeanor . . . .").

182. *See* Mary Jane Saunders, *Criminal Copyright Infringement and the Copyright Felony Act*, 71 DENV. U. L. REV. 671, 674 (1994); *see also* Irina D. Manta, *The Puzzle of Criminal Sanctions for Intellectual Property Infringement*, 24 HARV. J.L. & TECH. 469, 481 (2011).

183. 17 U.S.C. § 506 (2012) (direct copyright infringement); 18 U.S.C. § 2319 (direct copyright infringement); Indictment, *supra* note 156, at 62 (citing 18 U.S.C. § 2) (aiding and abetting).

184. DMCA title II bars monetary or equitable relief against those who come within its safe harbors. 17 U.S.C. § 512.

185. 144 CONG. REC. H10,618 (daily ed. Oct. 12, 1998) (statement of Rep. Barney Frank).

186. *See generally* FREEDOM HOUSE, FREEDOM ON THE NET 2012: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA (Sanja Kelly et al. eds., 2012), *available at* http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report_0.pdf; Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010) (transcript available at www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm); Press Release, Human Rights First, Key Questions Remain After Syria's Internet Goes Black (Nov. 29, 2012), *available at* http://www.humanrightsfirst.org/press-release/key-questions-remain-after-syria%E2%80%99s-internet-goes-black;

international treaty authorizing Internet censorship? Before a United Nations ITU conference in Dubai in 2012, China, Russia, and Saudi Arabia proposed precisely this.[187] They sought international authority for every state to restrict Internet access where it might "interfer[e] in the internal affairs or undermin[e] . . . national security [or] public safety . . . or . . . divulge information of a sensitive nature."[188]

National security, of course, is often invoked by governments seeking to censor information they find undesirable. This provision would have authorized both a kill switch, allowing governments to shut down the Internet, and more targeted censorship, barring particular information that a government declares forbidden. By seeking such constraints at the telecommunications level (the realm of the ITU), Russia and other states sought to build censorship into the infrastructure of the Internet—and receive international blessing to do so. They also sought to build in surveillance. Russia proposed that a state "have the right, where necessary, to know the actual course of a route, for the purposes of ensuring security and combating fraud"[189] and even sought to "ensure that operating agencies duly identify the subscriber."[190]

Concerns over the free speech implications of these provisions led the ITU ultimately to reject these changes to the International Telecommunications Regulations,[191] at least for now.[192] The ITU did require states to "endeavour to

News Media and Internet Totally Censored in Kashmir, REPORTERS WITHOUT BORDERS (Feb. 13, 2013), http://en.rsf.org/india-news-media-and-internet-totally-13-02-2013,44066.html.

187. The proposals originated from Russia, United Arab Emirates, China, Saudi Arabia, Algeria, Sudan, and Egypt. WORLD CONFERENCE ON INT'L TELECOMMS., DOCUMENT DT-X, PROPOSALS FOR THE WORK OF THE CONFERENCE 1 (2012), *available at* http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf.

188. COUNCIL WORKING GRP. TO PREPARE FOR THE 2012 WORLD CONFERENCE ON INT'L TELECOMMS., DOCUMENT CWG-WCIT12/DT-62 REV.2-E, DRAFT COMPILATION OF PROPOSALS WITH OPTIONS FOR REVISIONS TO THE ITRS 180 (2012), *available at* http://files.wcitleaks.org/public/T09-CWG.WCIT12-120620-TD-PLEN-0062R2.pdf. These states proposed the following treaty language: "Member States shall ensure unrestricted public access to international telecommunication services and the unrestricted use of international telecommunications, except in cases where international telecommunication services are used for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other States, or to divulge information of a sensitive nature." *Id.* at 180–81.

189. *Id.* at 89. Russia proposed modified language: "Member States/operating agencies shall have the right to know which international routes are used for carrying traffic." *Id.* The Arab States similarly proposed: "A Member State has the right to know how its . . . traffic is routed." *Id.* at 87. Russia proposed additional language: "Member States shall ensure that operating agencies duly identify the subscriber when providing international telecommunication services, and shall ensure the appropriate processing, transmission and protection of identification information in international telecommunication networks." *Id.* at 181.

190. *Id.* at 181.

191. *See, e.g.*, ACCESS, FREEDOM OF EXPRESSION ONLINE AND REVISING THE INTERNATIONAL TELECOMMUNICATION REGULATIONS 1 (2012), *available at* https://www.accessnow.org/page/-/docs/FreedomofExpressionOnlineandRevisingtheITRs.pdf; CTR. FOR DEMOCRACY & TECH., SECURITY PROPOSALS TO THE ITU COULD CREATE MORE PROBLEMS, NOT SOLUTIONS 2, 4–8 (2012), *available at* https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf ("This paper focuses on the proposed changes to the [International Telecommunication Regulations] . . . explaining how these

ensure the security and robustness of international telecommunication networks," potentially raising censorship-via-security-rationale concerns—though not with the same force as the more direct censorship and surveillance proposals.[193]

Governments may not need the cover of the United Nations to try to impose greater control over information on the Internet. Countries around the world are seeking to keep data about their citizens from leaving their borders and increasing their ability to monitor their citizens in the process.[194] Vietnam's Decree 72 now requires a local copy of all information about Vietnamese users;[195] Germany proposed a parallel Internet infrastructure to keep information within Europe;[196] Brazil considered (and ultimately rejected) a *Marco Civil Provision* that would allow the executive to ban any information from leaving the country.[197]

D. EUROPE'S FORGETTING PILL

The elephantine memory of computer systems combined with the rise of digitized expression and interaction has led many to propose a legal tool to compel the deletion of personal information from databases.[198] The European Commission

proposals could threaten Internet users' right[s] to privacy and free expression."); Guy Berger, Dir. for Freedom of Expression & Media Dev., UNESCO, Speech at the Budapest Conference on Cyberspace 3 (Oct. 4–5, 2012), *available at* http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/speech_berger_budapest.pdf (observing that the term "sensitive" offered a "problematic novel rationale for controlling content").

192. Changes to the ITU's constitution, not just its regulations, are on the agenda for the ITU plenipotentiary in October 2014. *Correspondence Group on the Elaboration of a Working Definition of the Term "ICT,"* INT'L TELECOMM. UNION, http://www.itu.int/ITU-D/study_groups/SGP_2010-2014/groups/definition/ (last visited Oct. 26, 2014).

193. INT'L TELECOMM. UNION, FINAL ACTS: WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS (DUBAI, 2012), art. 5A, § 41B (2012), *available at* http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf. Other revisions potentially extend future ITU governance to Internet-related matters. Of the 144 delegations with voting rights, 55 did not sign the revised regulations, and thus, are bound only by the original International Telecommunications Regulations. *Signatories of the Final Acts: 89*, INT'L TELECOMM. UNION, http://www.itu.int/osg/wcit-12/highlights/signatories.html (last visited Oct. 26, 2014).

194. Anupam Chander & Uyên P. Lê, *Breaking the Web: Data Localization vs. the Global Internet*, 64 EMORY L.J. (forthcoming 2015) (manuscript at 3) (UC Davis Legal Studies Research, Paper No. 378, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

195. *Nghi Dinh Quan Ly, Cung Cap Su Dung Dich Vu Internet Va Thong Tin Tren Mang* [Decree on Management, Provision and Use of Internet Services and Online Information], No. 72/2013/ND-CP, art. 22 (July 15, 2013) (Viet.), *translated in* http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf.

196. Interview by Louisa Schaefer with Phillipp Blank, Corporate Blogger, Deutsche Telekom (Oct. 18, 2013), *available at* http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891.

197. *Compare* Substitutivo ao Projeto de Lei No. 2.126, art. 12, de 12 de fevereiro de 2014 (Braz.), *available at* http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=606238 (follow "Inteiro teor" hyperlink), *translated in* http://www.ip-watch.org/weblog/wp-content/uploads/2013/11/MC_Eng_CR_Nov_13_2013.docx, *with* Lei No. 12.965, de 23 de abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014 (Braz.).

198. *See* Viviane Reding, Vice-President, European Union Justice Comm'r, European Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection

proposes such a right across Europe, defining a "right to be forgotten" as "the right of individuals to have their data . . . deleted when [it is] no longer needed for legitimate purposes."[199] The proposed Data Protection Regulation not only gives you the right to remove what you have said from others' computers, but also what they have said about you.[200] To assuage concerns about expression, the proposed regulation provides exceptions for free speech, public health, research, journalism, and art.[201] While these exceptions might seem to insulate the regulation from speech concerns, one needs only imagine an effort by an individual, Jack, to erase an earlier intemperate Facebook post that had been shared by Jill. Should Facebook eliminate this posting from Jill's page as the quintessential kind of activity that a person might desire to be forgotten? Or should Facebook declare Jill's sharing "free expression"? One suspects that the Facebook employee, faced with such concerns, might simply press "delete," though it may be hard to know whether Jack or Jill will be more aggravated by a decision one way or another. The employee would keep the following fact in mind: *Liability for noncompliance with the right to be forgotten runs only if one refuses to delete, not if one deletes at the drop of a hat*. Removing art and free expression carelessly does not carry any sanction. And the liability for failure to delete is fearsome: a fine of up to two

Rules in the Digital Age 5–6 (Jan. 22, 2012) (transcript available at http://europa.eu/rapid/press-release_SPEECH-12-26_en.pdf).

199. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 8, COM (2010) 609 final (Nov. 4, 2010), *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf. Article 17 of the 2012 proposal serves to elaborate and clarify the "right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten." *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 9, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter *Proposed Data Regulation*]. Article 17 states:

> The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data . . . .
>
> . . . .
>
> Where the controller . . . has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

Id. at 51.

200. *Proposed Data Regulation*, *supra* note 199, at 51.

201. *Id.* at 94–95. Article 17 would provide a "[r]ight to be forgotten and to erasure" granting "[t]he data subject . . . the right to obtain from the controller the erasure of personal data relating to them." *Id.* at 51.

percent of Facebook's annual worldwide income,[202] or more than $100,000,000 based on 2012 figures.[203]

The right to be forgotten transforms Facebook, Google, Reddit, and Twitter into censors, charged with evaluating whether a particular expression has artistic or journalistic merit or otherwise constitutes free expression. It renders them art curators and masters of literary value.[204] It imposes difficult burdens on Web 2.0[205] enterprises, including the potential requirement to identify how personal data has been shared through their platform, which might require a kind of tracking mechanism for data. This policing burden arises from the requirement that a data controller is responsible "[w]here the controller . . . has made the personal data public," for example, by "authoris[ing] a third party publication of personal data."[206] Because authorizing might include providing a "share" button, Internet intermediaries might find their burden here impossibly heavy. The proposed Data Protection Regulation has been overwhelmingly backed by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs late last year and is currently being negotiated in the Council of the EU.[207]

The European Court of Justice considered the issue in the case of *Google Spain v AEPD and Mario Costeja González*. In this case, a data subject sued Google for displaying incriminating information about him, which was made available online by a third party and then indexed by Google. When the case was being heard, the Advocate General of the European Court of Justice, Niilo Jääskinen, advised the court[208] that the 1995 Directive[209] does not provide citizens

202. *See id.* at 93–94.

203. *See* FACEBOOK, INC., FACEBOOK ANNUAL REPORT 2012, at 71 (2012), *available at* http://materials.proxyvote.com/Approved/30303M/20130409/AR_166822/ (listing 2012 revenue as $5,089,000,000).

204. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90–92 (2012), *available at* http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf.

205. *See infra* note 220 and accompanying text.

206. *Proposed Data Regulation*, *supra* note 199, at 51.

> Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has *authorised* a third party publication of personal data, the controller shall be considered responsible for that publication.

Id. (emphasis added).

207. Press Release, European Comm'n, LIBE Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.pdf. At this meeting, "[t]he LIBE vote [gave] a mandate to the Rapporteurs . . . to negotiate with the Council of the EU." *Id.* "To become law, the proposal[] must be approved by" the European Parliament (LIBE decision), the Council of the EU, and the European Council. Press Release, European Comm'n, Data Protection Day 2014: Full Speed on EU Data Protection Reform (Jan. 27, 2014), *available at* http://europa.eu/rapid/press-release_MEMO-14-60_en.pdf.

208. Opinion of Advocate General Jääskinen ¶ 6, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex 62012CC0131 (June 25, 2013).

the general right to be forgotten. But when asked whether the right to be forgotten could be derived from Article 7 of the European Union Charter, Jääskinen said:

> [T]he right to search information published on the internet by means of search engines is one of the most important ways to exercise that fundamental right. . . . An internet user's right to information would be compromised if his search for information concerning an individual did not generate search results providing a truthful reflection . . . .[210]

At the same time, Jääskinen recognized that the "search engine service provider lawfully exercises . . . his . . . freedom of expression when he makes available internet information location tools relying on a search engine."[211] Echoing the reasoning of *Sullivan*, Jääskinen advised that "any unregulated 'notice and take down procedure' . . . would amount to the censuring of [the website's] published content by a private party."[212]

The Court of Justice of the European Union decided this case on May 13, 2014, ruling that Internet search engines must consider an individual's requests to remove links resulting from a search of his name and must remove "from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person."[213] The judgment establishes a right to be forgotten based on Articles 7 and 8 of the EU Charter for data that "appear to be inadequate, irrelevant . . . or excessive."[214] The judgment also distinguishes between private information and information tightly bound to the "legitimate interest of internet users."[215] Without additional guidance, search engines are obligated to arbitrate what information is inadequate, irrelevant, of the public interest, and whose interests should override. To comply with the judgment, Google offered EU citizens the ability to file data

209. *See supra* note 82 and accompanying text.

210. Opinion of Advocate General Jääskinen, *supra* note 208, ¶ 131.

211. *Id.* ¶ 132.

212. *Id.* ¶ 134 (citation omitted).

213. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex 62012CJ0131 ¶ 88 (2014).

214. *Id.* ¶ 93; *id.* ¶ 69 (noting the requirements of Article 7 and 8 are implemented through several other articles and Directive 95/46).

215. *Id.* ¶ 81.

> However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

Id.

removal requests.[216] Within 24 hours, the search engine received right to be forgotten requests from at least 12,000 individuals.[217] Not only can search engines interfere with third parties' social and political opinions relating to an individual, they can severely curtail billions of Internet users' access to knowledge and speech. While individuals can file requests for removal, Internet users and third party speakers have no recourse to have search engines reinstate the links to writings and publications. The European Court of Justice approach does not give due attention to the importance of search services to free speech. Imagine the burden on speech if a library were to tell you that information might be found in its vast, unorganized stacks, but that it could not offer an index to assist the search for information.

A right to be forgotten law, limited to children, was proposed in California,[218] but ultimately, the version of the bill that was passed, the Privacy Rights for California Minors in the Digital World Act, only narrowly allowed children to delete information they had posted from their own streams, not from those of others.[219] This is a right that most services already provide to users.

E. WEB 3.0 AND THE INTERNET OF THINGS

Free speech gave life to Web 2.0, and it will also be critical to Web 3.0. While Web 2.0 could be captured by Facebook's mission statement—"to give people the power to share and make the world more open and connected"[220]—Web 3.0 seeks to create a world where the devices we use share, process, and "comprehend" data in a way that makes them in some sense aware.[221] Conceptualized by the World Wide Web inventor Tim Berners-Lee as a "Semantic Web," Web 3.0 consists of an intelligent network with growing ontologies for information, allowing computers

216. *Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited Oct. 26, 2014).

217. Charles Arthur & Samuel Gibbs, *Google Allows Europeans to Ask for Links to Be Removed*, GUARDIAN (May 30, 2014, 2:32 PM), http://www.theguardian.com/technology/2014/may/30/privacy-activists-welcoming-google-allowing-links-to-be-removed.

218. S.B. 568, 2013–2014 Leg., Reg. Sess. (Cal. 2013) (as introduced, Feb. 22, 2013).

219. CAL. BUS. & PROF. CODE § 22581(a)(1) (West 2014).

> An operator of an Internet Web site, online service, online application, or mobile application directed to minors or an operator of an Internet Web site, online service, online application, or mobile application that has actual knowledge that a minor is using its Internet Web site, online service, online application, or mobile application shall do all of the following: (1) Permit a minor who is a registered user of the operator's Internet Web site [and other services] . . . to remove or, if the operator prefers, to request and obtain removal of, content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the user . . . .

Id.

220. *About*, FACEBOOK, https://www.facebook.com/facebook/info (last visited Oct. 26, 2014).

221. Tim Berners-Lee et al., *The Semantic Web: A New Form of Web Content That Is Meaningful to Computers Will Unleash a Revolution of New Possibilities*, SCI. AM. (May 17, 2001), http://www.cs.umd.edu/~golbeck/LBSC690/SemanticWeb.html (contemplating a world where web-connected devices and web applications interpret data and complete tasks and transactions originally handled by users).

to better "understand" digitized information.[222] With this metadata, Web applications, smartphones, and perhaps even a humble toaster will be able to mine and interpret the massive quantity of data generated on the Web. The ontologies help define the ways that information can be related or its possible range of (computer-accessible) meanings. These ontologies will not only enable, but they will also condition speech. They are intended to help computers, and the people behind them, to understand the world through its digitized ephemera. But representations of information can also limit the kinds of information that is acceptable—they can constrain as much as enable.[223]

Web 3.0 implicates computer-mediated information sharing—or speech—to an extent never before possible. Let us anticipate an objection in our characterization of this as speech. Computers, of course, are not "persons" for purposes of the First Amendment, but their owners are. The people who devise the ontologies, or who program the computer, are speaking. Our speech is no less our own if it is processed by a computer we direct through a word processor or a web server. In *Sorrell*, as we have observed, the Court declared expansively, "[I]nformation is speech."[224] Information about information (metadata, or even the higher-level ontologies that define the form and content of metadata) is also speech, even if it is to be used by computers in the service of people.[225] Chief Judge Jon Newman's holding for the Second Circuit that "computer code conveying information is 'speech' within the meaning of the First Amendment" holds true here as well.[226] As we press forward with the frameworks for information representation and connection, we have to be careful to allow for ontologies that do not unduly constrain speech, especially in ways that favor the government.

Perhaps an even graver concern is the possibility that Web 3.0 will assist government surveillance, allowing governments to more accurately assess the content of speech using automatic means. Surveillance will grow even more ubiquitous through the rapid deployment of what has come to be known as the "Internet of Things"—the rise of objects embedded with sensors connected to the

222. *Id.*

223. Julien Mailland, *The Semantic Web and Information Flow: A Legal Framework*, 11 N.C. J.L. & TECH. 269, 290, 296 (2010) (noting that the Semantic Web could be utilized as a tool for enhanced information control).

224. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011).

225. Andrew Tutt suggests that *Brown v. Entertainment Merchants Ass'n*, 131 S. Ct. 2729 (2011), which characterized video games as protectable speech, limits speech for First Amendment purposes to speech that is "analogous in presentation and mode to 'old speech.'" Andrew Tutt, Note, *Software Speech*, 65 STAN. L. REV. ONLINE 73, 75 (2012), *available at* http://www.stanfordlawreview.org/sites/default/files/online/articles/Tutt-65-SLRO-73.pdf. The Supreme Court was not devising a general test for digital speech, but making the straightforward conclusion that videogames—like movies—constitute speech.

226. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449–50 (2d Cir. 2001).

Internet.[227] Cisco projects that there will be 50 billion such devices by 2020,[228] connecting and communicating with each other and other software agents on the Internet. [229]

The speech concern raised by the Internet of Things is that people may censor themselves, knowing that their environment and the devices they use are blabbing about them. Jerry Kang and Dana Cuff ask, "How likely are you to walk through the gay and lesbian studies section of [a bookstore] if you are closeted and know that RFID [radio frequency identification] readers are locked on your body?"[230] This concern can be ameliorated by careful construction and deployment of the underlying technologies.[231] We turn to the crucial issue of surveillance in the next Subpart.

F. SURVEILLANCE

> "An inspecting gaze, a gaze which each individual under its weight will end by interiorising to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost."
>
> *Michel Foucault*, *Power/Knowledge*[232]

227. The International Telecommunication Union defines the Internet of Things as "[a] global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies." *New ITU Standards Define the Internet of Things and Provide the Blueprints for Its Development*, INT'L TELECOMM. UNION (July 4, 2012, 11:00 AM), http://www.itu.int/ITU-T/newslog/New+ITU+Standards+Define+The+Internet+Of+Things+And+Provide+The+Blueprints+For+Its+Development.aspx.

228. DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

229. Each of these devices transmits personal data or impersonal data, likely to be aided by the deployment of the IPv6 addressing scheme. Each data stream created or accessed by these devices employs an ontology that permits processing by other computers. By expanding by orders of magnitude the number of available addresses, IPv6 offers the possibility of assigning every object a permanent and unique IP address. Currently, each Internet-capable device has a unique, hardcoded Machine Access Control ("MAC") number, but that address is not shared beyond the individual's router—though it becomes available to local wireless network routers one happens upon. *See* Matt Brian, *Smart Trash Can Knows How Fast You Walk and Which Smartphone You Use*, THE VERGE (Aug. 9, 2013, 8:09 AM), http://www.theverge.com/2013/8/9/4604980/smart-uk-trash-cans-smartphone-speed-proximity-wifi; Siraj Datoo, *This Recycling Bin Is Following You*, QUARTZ (Aug. 12, 2013), http://qz.com/112873/this-recycling-bin-is-following-you/.

230. Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 127 (2005).

231. *See* LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE 74–75 (2009).

232. Michel Foucault, *The Eye of Power*, *in* POWER/KNOWLEDGE: SELECTED INTERVIEWS AND OTHER WRITINGS 1972–1977, at 146, 155 (Colin Gordon ed., Colin Gordon et al. trans., 1980).

"Surveillance . . . breeds conformity," Glenn Greenwald observed in the wake of the recent disclosures of widespread electronic surveillance by the United States.[233] "[S]urveillance leads to self-censorship," Jerry Kang similarly warned early in the Internet Age.[234] Even earlier, Jennifer Granholm, who would go on to become governor of Michigan, worried that surveillance on the streets might suppress the inclinations of "[l]ight-hearted pedestrians" who might otherwise "sing out loud, dance a few steps in the street, or impulsively . . . hug a friend."[235] Meiklejohn's "dancing in the streets" after *Sullivan*[236] might yield to the sober business of getting from point A to point B with coats drawn closed. Daniel Solove, too, noted that "[s]urveillance can lead to self-censorship and inhibition. Because of its inhibitory effects, surveillance is a tool of social control."[237] In 1981, Vincent Blasi described the speech implications of self-censorship as follows: "Speakers, listeners, and society at large all suffer when . . . a regulatory scheme . . . causes [persons] to forgo protected expression rather than get themselves enmeshed in the scheme."[238]

Ubiquitous surveillance poses a mortal risk to free speech. Surveillance scholars point to Michel Foucault's observation that surveillance functions most effectively when it is internalized by its subjects, who conform to the preferences of the watchers, even without need for individual discipline.[239] Foucault described the physical architecture of the Panopticon, which can regulate without lifting a finger. As Foucault noted:

233. Natasha Lennard, *"Surveillance Breeds Conformity": Salon's Glenn Greenwald Interview*, SALON (Jan. 3, 2014, 7:45 PM), http://www.salon.com/2014/01/03/the_salon_glenn_greenwald_interview_surveillance_breeds_conformity/. For reports on this surveillance, see, for example, Barton Gellman, *NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.
html; Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

234. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998); *cf.* DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 26 (1994) ("In modern societies people are increasingly watched, and their activities documented and classified with a view to creating populations that conform to social norms.").

235. Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687, 708 (1987).

236. *See* Kalven, *supra* note 5, at 221 n.125.

237. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 493 (2006) (footnote omitted).

238. Vincent Blasi, *Toward a Theory of Prior Restraint: The Central Linkage*, 66 MINN. L. REV. 11, 24 (1981).

239. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 76–77 (2013).

> The genius of the Panopticon is that the surveillance itself disciplines: 'He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principal of his own subjection.'[240]

Yet, because of the diffuseness of the chilling effect, it may be difficult to make out a First Amendment case against public surveillance.[241] In 1967, civil rights activists challenged the U.S. Army's extensive monitoring of their public activities, arguing that it "chilled" speech. [242] In *Laird v. Tatum*, the Supreme Court held that the plaintiff lacked standing because the injury was too "speculative."[243] In his dissent, Justice William O. Douglas compared the U.S. Army's actions with those of the Russian authorities:

> When an intelligence officer looks over every nonconformist's shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the image which Jefferson and Madison designed, but more in the Russian image . . . .[244]

Justice Douglas even quoted from a letter from Alexander Solzhenitsyn, the Soviet dissident and scholar of totalitarianism, noting the "forbidden, contaminated zone" that surveillance had created around his family, placing everyone with whom they were in contact at risk of reprisal.[245] The courts have largely continued in *Laird*'s vein, most recently in a federal district court's dismissal of a claim against the surveillance of mosques by the New York City Police.[246] In *Hassan v. City of New York*, the district judge believed that the harm only arose when the plaintiffs learned of the surveillance from the media and would not have occurred if the surveillance had remained hidden.[247] But if individuals come to believe that their every move is in fact being watched, the chilling effect has already arrived. Given the real harms of such surveillance, Neil Richards has argued that "a reasonable fear of government surveillance that affects the subject's intellectual

240. Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 10 (2011) (quoting MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 202–03 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977)).

241. *See generally* Scott Michelman, *Who Can Sue over Government Surveillance?*, 57 UCLA L. REV. 71 (2009) (arguing that unclear standing jurisprudence prevents surveillance cases from reaching the merits).

242. *See* Laird v. Tatum, 408 U.S. 1, 10 (1972).

243. *Id.* at 13.

244. *Id.* at 28–29 (Douglas, J., dissenting).

245. *Id.* at 37.

246. Hassan v. City of New York, No. 2:12-3401(WJM), 2014 WL 654604, at *1 (D.N.J. Feb. 20, 2014); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1943 (2013) (noting that "[m]ore recent surveillance cases have followed the lead of the *Laird* Court").

247. *Hassan*, 2014 WL 654604, at *4.

activities (reading, thinking, and communicating) should be recognized as a harm sufficient to prove an injury in fact under standing doctrine."[248]

Many readers will agree with this critique of omnipresent government surveillance made possible by the digital medium. But readers may note that surveillance comes in additional forms. Surveillance by corporations, or corporate "dataveillance," is an increasingly commonplace feature of digital life, and indeed, as we have suggested, a key to the *free* speech made possible by the Web. Corporations amass as much data as possible about an individual, then mine the data for marketing purposes. While such information helps tailor advertising to the individual tastes of the user, many worry about the possible manipulation of consumers made possible by the greater knowledge of their habits.[249]

Fearing that Big Brother is watching, individuals will comport themselves accordingly.[250] Self-censorship will become the norm, as it is in authoritarian societies today.

IV. CONCLUSION:

#Inauguration, #BostonMarathon, #StandWithWendy, #DOMA, #Prop8, #MalalaDay, #MarchOnWashington, #GovernmentShutdown, #IranTalks, #RIPMandela. These are the issues that occupied the nation's attention in 2013, as reflected in what we spoke about on Twitter.[251] The zeitgeist of an age is perhaps more likely to be reflected on Twitter than either the *New York Times* or CBS. When Nelson Mandela passed away, many took to the streets, but even more took to social media. On Twitter, their messages might appear in the newsfeeds of their followers, and also in the results for anyone searching for conversations about Mandela through hashtags. The hashtag served as a democratizer of speech, allowing anyone to have her thoughts echoed around the world. Thus, the hashtag facilitates a bottom-up commentary on the issues of the moment. But Twitter did not invent the hashtag. Instead, it was the community of users who found a need to connect thoughts from disparate individuals.[252] But the hashtag granted an extraordinary power—it helped give ordinary people the power to engage the world on whatever topic they choose. And it gave individuals the ability to hear what their fellow human beings wanted to say on a particular subject. Reflecting

248. Richards, *supra* note 246, at 1964.

249. *See generally* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Tanzina Vega, *New Ways Marketers Are Manipulating Data to Influence You*, N.Y. TIMES (June 19, 2013, 9:49 PM), http://bits.blogs.nytimes.com/2013/06/19/new-ways-marketers-are-manipulating-data-to-influence-you/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1.

250. *Cf.* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 758 (2008) (suggesting that government surveillance may chill association).

251. *#2013*, TWITTER, https://2013.twitter.com/#category-2013 (last visited Oct. 26, 2014).

252. A tweet in 2007 proposed the use of hashtags (then simply termed "pounds"): "'how do you feel about using # (pound) for groups. As in #barcamp [msg]?'" Liz Gannes, *The Short and Illustrious History of Twitter #Hashtags*, GIGAOM (Apr. 30, 2010, 4:44 PM), http://gigaom.com/2010/04/30/the-short-and-illustrious-history-of-twitter-hashtags.

on the year just ending, Twitter itself observed, "[t]his year's most-retweeted Tweets showed the world coming together in loss, love, and celebration."[253] No one has the power to exclude someone from a conversation. No one can un-hashtag someone else's speech. The hashtag is free and open, not trademarked or copyrighted. When Mitt Romney supporters created the hashtag #AreYouBetterOff, Barack Obama supporters joined in the conversation, outnumbering Romney supporters by a margin of three to one.[254] While the services do give a user the power to block others, this only blocks those users from one's own newsfeed—not from the general public.[255]

One day in 2013, a false rumor, circulated on Twitter, caused the stock market to lose $200 billion in value.[256] Someone hijacking the Associated Press Twitter account had falsely reported injury to the President, sending the market into a swoon.[257] Lawsuits for damages would have spelled the death of Twitter. Yet, no lawsuits were forthcoming, clearly futile because of the law. Outrageous conduct by users of Facebook, Google, Reddit, Tumblr, or Yelp might have spelled the death of social media without a law insulating these companies from liability for facilitating the speech of users.

On the Internet, speech, technology, and business are inextricably bound. Free speech and its limits are now debated in the *MIT Technology Review*.[258] The central organizing principles of the Internet revolve around speech and freedom. Consider the famous maxims: "Information wants to be free"[259] or "The Net interprets censorship as damage and routes around it."[260] Even the Internet's best-

253. *Golden Tweets*, TWITTER, https://2013.twitter.com/#month-golden-tweets (last visited Oct. 26, 2014).

254. Agence France-Presse, *Election 2012 Fought with Tweets, Hashtags, Facebook Updates and Emails in a Battle for Digital Supremacy*, RAW STORY (Oct. 14, 2012, 9:13 AM), http://www.rawstory.com/rs/2012/10/14/election-2012-fought-with-tweets-hashtags-facebook-updates-and-emails-in-a-battle-for-digital-supremacy.

255. *See Blocking Users on Twitter*, TWITTER, https://support.twitter.com/articles/117063-blocking-users-on-twitter (last visited Oct. 26, 2014) (explaining that blocked users may still view Tweets that the blocker makes available to the public). Twitter itself can purge individuals from the service, but it seems to exercise this power largely on spam accounts. Erick Schonfeld, *Twitter Cracks Down on Spam Accounts, People Lose Followers*, TECHCRUNCH (July 24, 2009), http://techcrunch.com/2009/07/24/twitter-cracks-down-on-spam-accounts-people-lose-followers.

256. Tom Lauricella et al., *Twitter Hoax Sparks Swift Stock Swoon*, WALL ST. J. (Apr. 23, 2013, 7:33 PM), http://online.wsj.com/article/SB10001424127887323735604578441201605193488.html.

257. *Id.*

258. Jason Pontin, *Free Speech in the Era of Its Technological Amplification: A Letter to John Stuart Mill About the Limits of What May Be Shown or Said on the Web*, MIT TECH. REV. (Feb. 20, 2013), http://www.technologyreview.com/featuredstory/511276/free-speech-in-the-era-of-its-technological-amplification/.

259. This phrase is attributed to Stewart Brand. *See* Jennifer Lai, *Information Wants to Be Free . . . and Expensive*, FORTUNE (July 20, 2009, 2:00 PM), http://fortune.com/2009/07/20/information-wants-to-be-free-and-expensive.

260. This phrase was first coined by internet pioneer John Gilmore. *See* Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62, 64.

known joke—"On the Internet, nobody knows you're a dog"[261]—relies on the way that the Internet frees speech.

The latest incarnation of Silicon Valley can be attributed to a decision in 1789 and efforts to give it life two centuries later. When James Madison first proposed what became the First Amendment to the U.S. Constitution,[262] he could scarcely have imagined the world of Facebook, Flickr, Google, Pinterest, and Twitter. But the U.S. Constitution's free speech guarantee would help usher these companies into being at the dawn of the millennium. In turn, the free speech guarantee would itself be reincarnated, giving ordinary persons in the United States and the world the ability to talk to each other.

Yet, the same technology that gives us *free* speech lends itself to pervasive surveillance, unimaginable even by the Stasi.[263] A 21st-century free speech law must attend to the ways that Internet protocols and intermediaries regulate or liberate speech. We must be ever vigilant, lest additional years find us lamenting the loss of a golden age for *free* speech.

261. Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, NEW YORKER, http://www.condenaststore.com/-sp/On-the-Internet-nobody-knows-you-re-a-dog-New-Yorker-Cartoon-Prints_i8562841_.htm (last visited Oct. 26, 2014).

262. *See* Don R. Pember, *The Burgeoning Scope of "Access Privacy" and the Portent for a Free Press*, 64 IOWA L. REV. 1155, 1167 (1979); *James Madison*, FIRST AMENDMENT CTR., http://www.firstamendmentcenter.org/hall-of-fame/james-madison (last visited Oct. 26, 2014).

263. The "Stasi" was "[t]he East German secret police." *See* Julia Angwin, *You Know Who Else Collected Metadata? The Stasi.*, PROPUBLICA (Feb. 11, 2014, 4:02 PM), http://www.propublica.org/article/how-the-stasi-spied-on-social-networks.