OLD-SCHOOL/NEW-SCHOOL SPEECH REGULATION

Jack M. Balkin[*]

INTRODUCTION: DANCING IN THE STREETS

New York Times Co. v. Sullivan[1] and *New York Times Co. v. United States*[2] (*Pentagon Papers*) are two famous examples of a great flowering of First Amendment jurisprudence during the middle of the twentieth century. The philosopher Alexander Meiklejohn declared *Sullivan* to be "an occasion for dancing in the streets."[3] *Sullivan* recognized that "the central meaning of the First Amendment" was that the state could not punish criticism of public officials made without malice either directly through the criminal law or indirectly through civil damages for defamation.[4] *Pentagon Papers* reaffirmed the central First Amendment principle against prior restraints;[5] Justice Stewart's concurring opinion added that the government could not suppress disclosure of sensitive information unless it would "surely result in direct, immediate, and irreparable damage to our Nation or its people."[6] Together these two decisions celebrated the crucial role of the press in a democratic society, and stood for the principle that the circulation of public discourse is crucial to democratic legitimacy.[7] Half a century later, the impact of these two decisions has been weakened by significant changes in the practices and technologies of free expression, changes that concern a revolution in the infrastructure of free expression. That infrastructure, largely held in private hands, is the central battleground over free speech in the digital era.

Government practices have also changed in the past fifty years. To be sure, governments still regulate speech through fines, criminal penalties,

---

[*] Knight Professor of Constitutional Law and the First Amendment, Yale Law School. My thanks to Yochai Benkler, Martin Lederman, Sanford Levinson, Dawn Nunziato, Robert Post, David Pozen, and David Schulz for their comments on previous drafts.

[1] 376 U.S. 254 (1964).

[2] 403 U.S. 713 (1971) (per curiam).

[3] Harry Kalven, Jr., *The New York Times Case: A Note on "The Central Meaning of the First Amendment,"* 1964 SUP. CT. REV. 191, 221 n.125 (internal quotation marks omitted) (quoting Meiklejohn).

[4] *Sullivan*, 376 U.S. at 273.

[5] *Pentagon Papers*, 403 U.S. at 714.

[6] *Id.* at 730 (Stewart, J., concurring); *see also id.* at 726–27 (Brennan, J., concurring) (concurring to explain that prior restraint is permitted only under an "extremely narrow class of cases" involving the most extreme circumstances, *id.* at 726, and that "only governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order," *id.* at 726–27).

[7] As Justice Brennan put it, constitutional guarantees of free speech and free press presuppose "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." *Sullivan*, 376 U.S. at 270.

and injunctions; they still engage in predigital practices of surveillance. But new techniques have supplemented traditional modes of control over speech and traditional modes of surveillance. Like speech itself, the regulation and surveillance of speech require an infrastructure. Increasingly, speech regulation and surveillance are technologically imposed and involve cooperation between governments and the private entities that control the infrastructure of free expression.

Thus, a significant feature of the early twenty-first century is that the infrastructure of free expression increasingly is merging with the infrastructure of speech regulation and the infrastructure of public and private surveillance. The technologies and associated institutions and practices that people rely on to communicate with each other are the same technologies and associated institutions and practices that governments employ for speech regulation and surveillance.

Consider a mid-twentieth-century newspaper like the petitioner in *New York Times Co. v. Sullivan*. To reach its audience, the *Times* depended on an infrastructure of technologies and institutions: printing presses, labor unions, delivery trucks, newsstands, and advertisers. These features of the *Times*'s business may have been regulated by the government in various ways — in trucking regulations, labor law, and so on. But for the most part the government's capacities for control and surveillance of speech were not built into the very technologies and practices that the *Times* used to communicate with its audience. The government did not have a long-distance switch that allowed it silently and inexpensively to control the *Times*'s printing presses or prevent certain articles from appearing in its pages. The government did not require that members of labor unions operating the *Times*'s printing presses wear hidden microphones and cameras so that the government could learn about any potentially subversive or infringing materials. That is why it was necessary for the government to seek an injunction in the *Pentagon Papers* case. Of course, the government did control the public streets. Arguably it could have created roadblocks throughout New York City to search for and stop the *Times*'s delivery trucks, but this would have been highly visible, logistically difficult, and costly in terms of legitimacy.

The digital era is different. Governments can target for control or surveillance many different aspects of the digital infrastructure that people use to communicate: telecommunications and broadband companies, web hosting services, domain name registrars, search engines, social media platforms, payment systems, and advertisers. The very forces that have democratized and decentralized the production and transmission of information in the digital era have also led to new techniques and tools of speech regulation and surveillance that use the same infrastructure. These tools of regulation and surveillance often work automatically and in the background; they may harness the cooperation or coercion of private owners of infrastructure to achieve the government's regulatory goals. Low salience and use of private parties can help governments preserve legitima-

cy even as their policies block, limit, or spy on expression. This is the big story about the freedoms of speech, press, and association in the digital age.

Traditional or "old-school" techniques of speech regulation have generally employed criminal penalties, civil damages, and injunctions to regulate individual speakers and publishers. The landmark decisions in *Sullivan* and *Pentagon Papers* responded to old-school speech regulation: in both cases, the state had used penalties and injunctions directed at speakers and publishers in order to control and discipline their speech.

These methods have hardly disappeared in the twenty-first century. But now they are joined by "new-school" techniques of speech regulation. The latter regulate speech through control over digital networks and auxiliary services like search engines, payment systems, and advertisers; instead of focusing directly on publishers and speakers, they are aimed at the owners of digital infrastructure.[8]

These new-school techniques have three characteristic features that often operate together. None of these features is entirely new.[9] Each has counterparts or precedents in the predigital world, but each has been reshaped to fit the demands of a new technological environment.

The first feature is *collateral censorship*, in which the state regulates party A in order to control speaker B. The digital age enables a vast number of people to communicate widely across the country and around the world. Because there are so many speakers, who are often anonymous, difficult to co-opt, or otherwise beyond the government's effective control, the state aims at Internet intermediaries and other owners of digital infrastructure — threatening liability to induce them to block, limit, or censor speech by other parties.

Second, and relatedly, *public/private cooperation and co-optation* are hallmarks of new-school speech regulation. To the extent that the government does not own the infrastructure of free expression, it needs to coerce or co-opt private owners to assist in speech regulation and surveillance — to help the state identify speakers and sites that the government seeks to watch, regulate, or shut down. To this end, the government may offer a combination of carrots and sticks, including legal immunity for assisting the government's efforts at surveillance and control. Owners of private infrastructure, hoping to reduce legal uncertainty and to ensure an uncompli-

---

[8] Professor Derek Bambauer has described several of these new-school techniques as examples of what he calls an emerging form of "soft censorship," which he believes is less legitimate because it is less overt. *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 867–68 (2012). As I describe in Part IV, new-school techniques often emphasize prevention over deterrence, and seek low salience or even invisibility.

[9] *See* Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 1–3 (2004) (arguing that "[i]nstead of focusing on novelty, we should focus on salience" to understand the consequences of technological change for constitutional interpretation, *id.* at 2).

cated business environment, often have incentives to be helpful even without direct government threats.

Third, governments have devised new forms of *digital prior restraint*. Many new-school techniques of speech regulation have effects similar to prior restraints, even though they may not involve traditional licensing schemes or judicial injunctions. In addition, prior restraints are especially important to the government's expansive surveillance practices in the National Surveillance State. As I explain in Part III, prior restraints directed at owners of private infrastructure are now ubiquitous in the United States; gag orders have become fully normalized and bureaucratized elements of digital surveillance, as routine as they are invisible.

Throughout this Essay, I will use the expression "speech regulation" rather than the term "censorship" — the major exception being the discussion of "collateral censorship," which is a term of art. I prefer the term "speech regulation" for three reasons. First, people generally consider "censorship" as presumptively impermissible, but not all regulation of speech is unjustified.[10] A key question for civil liberties today is which of the new-school techniques identified in this Essay *should* be understood as censorship.[11] Before *New York Times Co. v. Sullivan*, the traditional common law of defamation was not generally recognized *as* censorship. The genius of Herbert Wechsler's argument in *Sullivan* was showing that application of longstanding common law rules had effects similar to paradigmatic cases of censorship.[12] As noted above, I argue that many new-school techniques operate like prior restraints, whether or not they require government licenses or employ judicial injunctions.

Second, as I use the term, "speech regulation" concerns primarily state regulation, state action that partners with or co-opts private parties, or state regulation that leverages private control of infrastructure to achieve state ends. Practices of "censorship," by contrast, need have no connection to the state. They may be cultural or disciplinary and they are ubiquitous in civil society.[13] Indeed sometimes the more ubiquitous these practices are, the less people treat them as normatively improper.

Third, the term "censorship" is underinclusive because some practices of speech regulation, even when unlawful, may not be widely acknowledged as "censorship." For example, digital surveillance is an important element of new-school techniques. Surveillance practices may indirectly

---

[10] As noted below, not all collateral censorship is unjustified. *See infra* TAN 45–47.

[11] *Cf.* Bambauer, *supra* note 8, at 873 (offering a technical definition of "censorship" that "concentrates upon the *method* a government uses to control information and defers analysis of the *legitimacy* of such measures to a separate step" because not all censorship is illegitimate).

[12] *See* Brief for Petitioner at 30–31, 44–51, *Sullivan*, 376 U.S. 254 (No. 39) (comparing Alabama's defamation law with the Sedition Act of 1798 and judicial contempt citations subject to the clear and present danger standard).

[13] *See generally* CENSORSHIP AND SILENCING (Robert C. Post ed., 1998) (describing various cultural practices of expressive control).

regulate speech and association, and they may also facilitate or lead to other forms of speech regulation. In fact, some speech regulation today may be quite difficult without pervasive digital surveillance. Yet even if surveillance practices have serious effects on expressive activity, people may still distinguish them from direct censorship.

The remainder of this Essay proceeds as follows: Part I develops the central idea of the infrastructure of freedom of expression on which the practical freedoms of speech and press depend. This infrastructure is the focus of new-school speech regulation. Part II then describes a variety of new-school techniques, comparing them with traditional or old-school methods of speech regulation. In particular, this Part explains how many of the traditional problems of prior restraint reappear in new-school strategies. It also explains how the "soft power" of government influence can sometimes substitute for direct regulation of owners of private infrastructure.

Part III builds on these ideas to discuss a remarkable example of new-school speech regulation: the tens of thousands of gag orders issued each year that accompany national security letters (NSLs). This practice is a side effect of the burgeoning National Surveillance State. The government needs the assistance of owners of private infrastructure to engage in effective surveillance, and it wants to keep the nature and extent of that assistance secret. As a result, the government has created a routinized, bureaucratically enforced system of prior restraint that is largely isolated from traditional First Amendment doctrine.

Part IV concludes by pointing out that new-school speech regulation emphasizes prevention rather than deterrence, and low salience (or invisibility) rather than chilling effects. Both the state and the owners of private infrastructure may prefer that filtering, blocking, and surveillance be largely invisible to the general public, so that their operations appear normal, unobtrusive, and inoffensive. Secrecy assists in this goal, while publicity undermines it. Traditional free speech doctrine has often been concerned with the chilling effects of speech regulation on innocent parties; in the National Surveillance State, however, the government may simply want most people to chill out.

I. THE INFRASTRUCTURE OF FREE EXPRESSION

The freedoms of speech and press require more than freedom from direct state prohibition. In practice, freedom of speech and freedom of the press require an *infrastructure of free expression*.[14]

---

[14] Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 432 (2009) ("A system of free speech depends not only on the mere absence of state censorship, but also on an infrastructure of free expression. The infrastructure of free expression includes the kinds of media and institutions for knowledge, creation, and dissemination that are available at any point in time."

What is the infrastructure of free expression? Take the motion picture industry as an example. That industry would be greatly hampered without public access to movie projectors, movie theaters, DVD players, and contemporary movie distribution systems. More generally, we speak of the motion picture industry as an *industry*. It includes an array of technologies, artists, artisans, institutions, business organizations, contractual arrangements, and customs and conventions for creating, constructing, producing, and distributing motion pictures. These elements, in turn are surrounded by an even larger network of supporting institutions. Similarly, the *New York Times* of the mid-twentieth century featured in *Sullivan* and *Pentagon Papers* was not simply a set of pages with ink. It was the cumulative product of editors, reporters, newsrooms, bureaus, wire services, printing machines, labor unions, delivery trucks, and subscription services; and it too depended on a larger set of businesses, contractual arrangements, customs, and conventions to produce "[a]ll the news that's fit to print."[15]

From an even broader perspective, we can see that the democratic model of free expression celebrated in *Sullivan* and *Pentagon Papers*, and the public sphere of knowledge and opinion that legitimates democracy, depend on a variety of institutions like telephone companies, public libraries, bookstores, schools, universities, post offices, subsidized postal rates, broadband services, and so on. Once we shift our focus from the moment of expression to the technological, economic, and social infrastructure that supports and enables expression, we can understand how crucial infrastructure is to the freedoms of speech and press.[16]

The role of infrastructure is apparent in the words of the First Amendment itself. The Amendment protects not only "speech" but also "free exercise" of religion, "press," "petition," and "assembl[y]."[17] The word "press" has the dual signification of an institution for creating and distributing content and a technology for creating and distributing content. At the Founding it referred to the freedom to use the key mass communication technology of the day — the printing press.[18] One may debate

---

(footnote omitted)); Balkin, *supra* note 9, at 52–54; *see also* Yochai Benkler, *Property, Commons, and the First Amendment: Towards a Core Common Infrastructure* 3 (White Paper for the First Amendment Program, Brennan Center for Justice at NYU Law School, 2001), *archived at* http://perma.cc/5DDR-WU5M.

15 *See* W. Joseph Campbell, *Story of the Most Famous Seven Words in US Journalism*, BBC NEWS (Feb. 10, 2012), http://www.bbc.co.uk/news/world-us-canada-16918787, *archived at* http://perma.cc/G6B7-DW3A (internal quotation marks omitted) (recounting the history of the *New York Times*'s famous motto).

16 It is worth emphasizing that this conception of infrastructure as consisting of supporting institutions and technologies overlaps with a purely economic theory of infrastructure, but it is not necessarily identical with it. *See generally* BRETT M. FRISCHMANN, INFRASTRUCTURE (2012).

17 U.S. CONST. amend. I.

18 *See* 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, 462–63 (2012) (arguing that at the Founding the freedom of "the press" referred to everyone who could use or be published by a printing press, rather

whether the contemporary meaning of "press" should refer to technology or to the practice of journalism.[19] But surely the two are deeply connected. Technologies enable certain practices of content production and certain organizational models, while practices of content production depend on the affordances of technologies and the support of institutions. Changes in what we now call "journalism" have often been shaped by changes in technology and the economics of mass communication.[20]

Similarly, the right of "petition" inevitably involves institutions, technologies, and practices. "Assembly" is more than the gathering of bodies in space. It requires access to a place to assemble and methods of gathering and organizing the assembly. (Today those methods of assembly and organization may include social media.) The freedom of association, recognized as an auxiliary right in twentieth-century doctrine,[21] not only supports the other freedoms as a sort of infrastructure of its own, but itself depends on infrastructure. Like the right of free speech, the right of free exercise of religion also depends on an infrastructure.[22] Even Meiklejohn's call for dancing in the streets requires an infrastructure of streets in which to dance.

Freedoms that rely on infrastructure can be attacked or controlled by attacking or controlling the infrastructure that supports them. These free-

---

than to the institution of journalism); *see also* David A. Anderson, *Freedom of the Press*, 80 TEX. L. REV. 429, 446–47 (2002) ("To the generation of the Framers of the First Amendment, 'the press' meant 'the printing press.' It referred less to a journalistic enterprise than to the technology of printing and the opportunities for communication that the technology created." *Id.* at 446.); *id.* at 446 n.90 ("Contemporaneous references uniformly indicate that freedom of the press meant freedom to express one's views through use of the printing press."); Edward Lee, *Freedom of the Press 2.0*, 42 GA. L. REV. 309, 315–16, 339–56 (2008) (arguing the "press" referred to the printing press and that "freedom of the press" was designed to protect "speech technology," *id.* at 345). *But see* Patrick J. Charles & Kevin Francis O'Neill, *Saving the Press Clause from Ruin: The Customary Origins of a "Free Press" as Interface to the Present and Future*, 2012 UTAH L. REV. 1691, 1769–70 (criticizing an exclusive focus on technology and emphasizing the Founders' conception of the press as crucial to investigating and reporting on government activities, thus implying rights of access to newsworthy events and to government information).

19 *See, e.g.*, Potter Stewart, *"Or of the Press,"* 26 HASTINGS L.J. 631, 633–34 (1975) (arguing that the "publishing business," *id.* at 633, enjoys special constitutional protection); Sonja R. West, *Awakening the Press Clause*, 58 UCLA L. REV. 1025, 1031 (2011) (arguing that the Press Clause gives a narrowly defined institution of the press special constitutional recognition, and "allow[s] journalists additional and unique protections, primarily with respect to newsgathering").

20 *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006).

21 *See, e.g.*, NAACP v. Alabama, 357 U.S. 449, 460 (1958) ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.").

22 *See* Richard W. Garnett, *Do Churches Matter? Towards an Institutional Understanding of the Religion Clauses*, 53 VILL. L. REV. 273, 274 (2008); Richard W. Garnett, *The Political (and Other) Safeguards of Religious Freedom*, 32 CARDOZO L. REV. 1815, 1824–25 (2011); Jack M. Balkin, *The Infrastructure of Religious Freedom*, BALKINIZATION (May 5, 2007, 3:15 PM), http://balkin.blogspot.com/2007/05/infrastructure-of-religious-freedom.html, *archived at* http://perma.cc/5EDD-9Q4L.

doms become vulnerable when the government uses that infrastructure, or its limitations, as leverage for regulation or surveillance. In fact, many famous First Amendment cases involve government attacks on the infrastructure of free expression, or, in the alternative, attempts to leverage weaknesses or limitations of the infrastructure in order to control speech. In *Hague v. CIO*,[23] for example, the government sought to prevent assembly by denying labor protesters access to public streets and parks; in *Schneider v. State*,[24] New Jersey attempted to ban the distribution of handbills; in *Grosjean v. American Press Co.*,[25] Louisiana sought to tax newspapers.

The hallmark of the digital age is a revolution in the infrastructure of free expression. That infrastructure includes the domain name system (DNS), Internet protocols, technological standards for storage and transmission of information, the Internet backbone, broadband networks and broadband companies, web hosting companies, and cloud services for storing, creating, displaying, and transmitting documents. It includes a wide variety of platforms and social media for creating, publishing, transmitting, and sharing content. It includes hardware platforms: computers, tablets, and especially smartphones, which have become all-purpose information and communication devices. It includes software applications of all types, including both systems that are open (like Linux and its variants including Apache and Android) and closed (like Apple's iOS system for phones and tablets). It includes distributed and networked systems of cameras, face-recognition systems, sensory-input devices, and information-collection devices. Finally, it includes a range of auxiliary services that support digital communication: (1) search engines, without which most information would be lost; (2) payment companies like PayPal, MasterCard, and Visa, who facilitate transactions with digital speakers; and (3) advertisers, who support and subsidize much of the Internet's free platforms, content production, and applications.

A widely noted and characteristic feature of the digital age is the democratization of information production, and therefore the democratization of opportunities to speak and express one's self. The "disintermediation" often associated with the Internet does not involve the abolition of media gatekeepers but rather the substitution of one kind of infrastructure for another. This democratization is well symbolized by the transformation of media companies. In the middle of the twentieth century, the most powerful media companies were publishers who distributed content that they created or edited: motion picture companies, book publishers, newspapers,

---

[23] 307 U.S. 496 (1939).
[24] 308 U.S. 147 (1939).
[25] 297 U.S. 233 (1936).

and broadcasters. The public sphere was largely organized as a series of audiences for the content produced by these publishers.

In the second decade of the twenty-first century, the most powerful media companies are platforms like Google and Facebook. These platforms are not primarily designed to publish what the platform owner creates. Instead they create opportunities for end users to publish (Blogger, Tumblr, Twitter), send email and private messages (Gmail, Yahoo! Mail), upload content (YouTube, Pinterest), and share content (Facebook); and they make it easy for end users to find content created by others (Google, Bing). Mass audiences still exist, but now many of them are also end users who share and transform content; in many cases, they are active creators of content. The movement from publishers to platforms is both an effect and a cause of the revolution in the infrastructure of free expression.

The shift from publishers to platforms complicates the regulation of speech. Individuals who disseminate content that the state wants to control may be anonymous or pseudonymous, or located beyond the reach of territorial governments. Therefore states increasingly target digital infrastructure not only because most people are speaking through it, but also because targeting infrastructure is the easiest method of control.

Many of the same features of the digital infrastructure that democratize speech also make the digital infrastructure the most powerful and most tempting target for speech regulation and surveillance. Although the digital infrastructure frees speakers from dependence on older media gatekeepers, it does so through the creation of new intermediaries that offer both states and private parties new opportunities for control and surveillance.

Not surprisingly, both private parties and states seek to shape the infrastructure so that it better facilitates control and surveillance. Through this process, the democratized digital infrastructure of speech also becomes the infrastructure of surveillance and speech regulation. Two examples are (1) the movement toward cloud computing, in which end users and businesses alike are encouraged to store more and more of their information — emails, documents, photographs, and personal data — on huge networks of privately owned servers; and (2) the dissolving of traditional telephone services into a host of digital services, best symbolized by the ubiquity of smartphones as the personal computer of choice for many people.

Both of these trends have made it easier for governments to focus their attention on a smaller number of large enterprises like the owners of the Internet backbone; broadband providers; telecommunications companies; platform owners like Google, Yahoo, and Facebook; web hosting services like Amazon; registrars like GoDaddy and Network Solutions; and owners of payment systems like Visa, MasterCard, and PayPal, in order to block or force the takedown of content or to search and analyze content.

Because the infrastructure of free expression is held largely in private hands, it becomes crucial for governments to enlist private parties — willingly or unwillingly — in its efforts at control and surveillance. Infrastructures of surveillance and speech regulation require new forms of pub-

lic/private cooperation or co-optation. Some private organizations actively seek increased government control and surveillance of the infrastructure. Other private organizations are pressed into service when the government threatens liability orpromises immunity.

The long-term trend has been the merger of the infrastructures of speech, speech regulation, and surveillance. At the beginning of the Internet age, John Gilmore argued that "[t]he Net interprets censorship as damage and routes around it."[26] By 2014, we can say that the Internet treats speech regulation and surveillance as design requirements and builds them into the system. Similarly, the battle cry of cyberactivists in the early twenty-first century was Stewart Brand's aphorism that "information wants to be free."[27] We now understand that information also wants to be collected, collated, analyzed, and used for surveillance and control.[28]

II. OLD-SCHOOL/NEW-SCHOOL SPEECH REGULATION

Changes in the infrastructure of free expression give rise to new modes of speech regulation. For convenience, we can distinguish between "old-school" and "new-school" speech regulation.

Old-school speech regulation is normally directed at (1) people, (2) spaces, and (3) predigital technologies of mass distribution. The state arrests, detains, or deports people; it controls access to public spaces for assembly and protest; and it monopolizes, regulates, seizes, or destroys capacities and technologies for publication and transmission like printing presses, broadcast facilities, movie projectors, videotapes, handbills, and books.

The twenty-first century features "new-school" speech regulation — techniques that regulate speech through the control of digital networks. They are often aimed at the intermediaries and supporting institutions that are crucial to Internet speech. The targets of new-school speech regulation range from ISPs and broadband providers to domain name registrars, host-

---

[26] Philip Elmer-DeWitt & David S. Jackson, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62 (quoting John Gilmore). There are many versions of this famous quote; *see, e.g.*, John Perry Barlow, *Censorship 2000*, ON THE INTERNET, http://www.isoc.org/oti/articles/1000/barlow.html (last visited May 10, 2014), *archived at* http://perma.cc/SHA2-CLR4 (quoting John Gilmore's remark at the Second Conference on Computers, Privacy, and Freedom that "[t]he Internet treats censorship as though it were a malfunction and routes around it").

[27] *Information Wants to Be Free*, WIKIPEDIA, http://en.wikipedia.org/wiki/Information_wants_to_be_free (last visited May 10, 2014), *archived at* http://perma.cc/N6LY-TSXN.

[28] The optimism symbolized by Gilmore and Brand was not universal. Professors Lawrence Lessig and James Boyle, among others, understood these problems early on. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (arguing that the Internet can be used as a means of regulation and control); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997) (arguing that the state could use privatized enforcement and state-backed technologies to control the Internet); *see also* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006) (arguing that nation states have multiple devices for regulating Internet content, including pressuring various Internet intermediaries).

ing services, search engines, advertisers, and credit card companies. New-school speech regulation often emphasizes ex ante prevention rather than ex post punishment, and complicated forms of public/private cooperation. It uses both sticks and carrots, and it is deeply connected to new techniques of digital surveillance by private parties and by the state.

New-school regulations of digital networks and intermediaries are layered on top of old-school techniques, which do not go away in a digital world. In fact, old- and new-school techniques of control and surveillance may support and supplement each other. For example, in response to revelations of classified documents by WikiLeaks, the government placed the suspected leaker, Private Bradley (now Chelsea) Manning, in solitary confinement and subjected Manning to various forms of harsh treatment even before a court martial was convened.[29] The hunt for Edward Snowden, who leaked secrets about American new-school surveillance practices,[30] featured old-school attempts at detention and control. After U.S. officials warned several Latin American countries not to harbor Snowden or allow him safe passage, European allies of the United States effectively forced the landing of the plane of the Bolivian President in the hopes of capturing Snowden.[31] In Great Britain, the government demanded that the *Guardian* destroy hard drives containing sensitive materials,[32] a twenty-first-century version of book burning. David Miranda, the partner of journalist Glenn Greenwald, who broke many of the stories concerning secret surveillance by the National Security Agency (NSA), was detained at Heathrow Airport for nine hours by British officials because he was suspected of being a courier.[33] Government Communications Headquarters (GCHQ) — the

---

[29] *See* Ed Pilkington, *Bradley Manning's Treatment Was Cruel and Inhuman, UN Torture Chief Rules*, THE GUARDIAN (Mar. 12, 2012, 9:41 AM), http://www.theguardian.com/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un, *archived at* http://perma.cc/5VZS-J6XY.

[30] *See generally Edward Snowden: Timeline*, BBC NEWS (Aug. 20, 2013, 3:21 PM), http://www.bbc.com/news/world-us-canada-23768248, *archived at* http://perma.cc/5LBT-9GQH; Bob Orr, *The Hunt for Edward Snowden*, CBS NEWS (June 25, 2013, 11:00 AM), http://www.cbsnews.com/news/the-hunt-for-edward-snowden/, *archived at* http://perma.cc/U6ZN-LVCU.

[31] Peter Baker & Ellen Barry, *Snowden, in Russia, Seeks Asylum in Ecuador*, N.Y. TIMES, June 23, 2013, http://www.nytimes.com/2013/06/24/world/asia/nsa-leaker-leaves-hong-kong-local-officials-say.html, *archived at* http://perma.cc/HJ6F-BV5D; Catherine E. Shoichet, *Bolivia: Presidential Plane Forced to Land After False Rumors of Snowden Onboard*, CNN (July 3, 2013, 8:26 AM), http://www.cnn.com/2013/07/02/world/americas/bolivia-presidential-plane/index.html, *archived at* http://perma.cc/9LQP-9QKG.

[32] Julian Borger, *NSA Files: Why the Guardian in London Destroyed Hard Drives of Leaked Files*, THE GUARDIAN (Aug. 20, 2013, 1:23 PM), http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london, *archived at* http://perma.cc/DRE5-8RMK.

[33] Steven Erlanger, *Britons Question Whether Detention of Reporter's Partner Was Terror-Related*, N.Y. TIMES, Aug. 19, 2013, http://www.nytimes.com/2013/08/20/world/europe/britain-detains-the-partner-of-glen-greenwald.html, *archived at* http://perma.cc/B5Q2-3X5L; Mark Hosenball, *British Accuse David Miranda, Glenn Greenwald's Partner, of 'Terrorism,'* HUFFINGTON POST (Nov. 2, 2013, 6:42 AM), http://www.huffingtonpost.com/2013/11/02

UK's equivalent of America's NSA — may have assumed that Greenwald and his associates recognized that digital networks were no longer safe for secure communications that would allow them to publish sensitive materials, and therefore had switched to an old-fashioned method of dissemination — couriers — in order to route around digital surveillance. This practice led to the GCHQ's attempt to cut off an alternative method of dissemination through the equally "old-school" method of arrest and detention.[34]

What follows is a guide to some of the key features of new-school speech regulation.

A. From Direct Regulation to Collateral Censorship

1. Old School: Regulation of Speakers, Spaces, and Traditional (Predigital) Technologies of Publication. — Old-school regulation aims at speakers and at predigital practices and technologies of organization and communication. These include public spaces, post offices, printing presses, movies, telegraphy, telephony, and radio and television broadcasting. States can exercise monopoly control over broadcast technologies, or they can use licensing schemes to restrict who may use these technologies.

Even without direct control, states may exercise indirect influence over publishers, broadcasters, and journalists. Webs of family, social, and economic connections between political elites and owners of broadcasting and publishing facilities can facilitate a kind of "soft power" that allows politicians and government officials to shape coverage and set agendas.[35] Politicians and government officials may seek to co-opt publishers, broadcasters, and journalists, who, in turn, may be anxious to maintain access to information from and curry favor with politicians and government officials.

2. New School: Collateral Censorship and Control over Digital Intermediaries and Platforms. — In the digital era, digital platforms and intermediaries join television, cable, and radio broadcasters. This greatly increases the number of possible speakers. It becomes increasingly difficult to co-opt so many speakers, making it harder to use soft power to control

---

/david-miranda-terrorism-glenn-greenwald-british_n_4199838.html, *archived at* http://perma.cc/F98Y-C6V5.

[34] The government may also use border searches of computers, cell phones, and other electronic devices to engage in electronic surveillance that would otherwise be prohibited by the Fourth Amendment. *See* United States v. Ramsey, 431 U.S. 606, 621 (1977) (noting that searches at the border are a "historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained"); *cf.* United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013) (recognizing the border-search exception but holding for the first time that a complete "forensic examination of [defendant's] computer required a showing of reasonable suspicion").

[35] *See* CHERIAN GEORGE, FREEDOM FROM THE PRESS (2012) (describing how the government of Singapore has controlled the privately owned media through a combination of licensing schemes and economic and family connections).

coverage and agenda setting.[36] Moreover, many speakers are anonymous, pseudonymous, or located overseas, beyond the reach of territorial governments. Therefore, states must turn to other devices. Instead of or in addition to targeting speakers, states can aim at intermediaries and owners of auxiliary services.

These techniques can range from the clumsy to the subtle. When all other methods are unavailing, states can attempt to shut down ISPs and broadband providers.[37] Instead of the old-school technique of cutting telephone or telegraph wires, states can temporarily jam or block cell phone access in order to prevent communication between activists or protesters.[38] But overt and excessive displays of power may delegitimate the state. It is far better to control digital networks in the background or behind the scenes, so that control and surveillance seem indistinguishable from normal conditions rather than singular or intermittent displays of extraordinary force.

To achieve these goals, states can either own Internet intermediaries or exert control over privately held intermediaries. The latter strategy leads directly to practices of *collateral censorship*, a characteristic technique of speech regulation in the digital age.

Collateral censorship occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech.[39] This will lead

---

[36] *Cf.* BENKLER, *supra* note 20, at 247 (2006) (arguing that "the networked public sphere provides broader intake, participatory filtering, and relatively incorruptible platforms for creating public salience"). The use of soft power to influence owners of digital infrastructure is described in section II.C.2.c, *infra* TAN 125–143.

[37] *See, e.g.*, James Glanz & John Markoff, *Egypt Leaders Found 'Off' Switch for Internet*, N.Y. TIMES, Feb. 15, 2011, http://www.nytimes.com/2011/02/16/technology/16internet.html, *archived at* http://perma.cc/Y2W3-D9VQ (describing how Egypt temporarily cut off Internet access during the Arab Spring protests); *Reaching for the Kill Switch*, THE ECONOMIST (Feb. 10, 2011), http://www.economist.com/node/18112043, *archived at* http://perma.cc/E9CW-G8RH (noting Internet cutoffs in Myanmar and Nepal).

[38] *See, e.g.*, Robert Barnes, *Public Safety, Technology and the First Amendment Collide in San Francisco's Subway*, WASH. POST (Aug. 28, 2011), http://www.washingtonpost.com/politics/public-safety-technology-and-the-first-amendment-collide-in-san-franciscos-subway/2011/08/26/gIQAfTIblJ_story.html, *archived at* http://perma.cc/L7GJ-F5S8 (describing the Bay Area Rapid Transit's (BART) decision to cut off cell phone service in order to stop a planned "flash-mob" protest that would have disrupted BART service); *see also* W. Danny Green, Comment, *The First Amendment and Cell Phones: Governmental Control over Cell Phone Use on Publicly Owned Lands*, 44 ARIZ. ST. L.J. 1355, 1358 (2012) (arguing that the BART shutdown violated the First Amendment).

[39] J.M. Balkin, Essay, *Free Speech and Hostile Environments*, 99 COLUM. L. REV. 2295, 2298 (1999); *see also* Christina Mulligan, *Technological Intermediaries and Freedom of the Press*, 66 SMU L. REV. 157, 160 (2013) (arguing that collateral censorship threatens freedom of the press). Professor Michael Meyerson coined the term. *See* Michael I. Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" Within the New Media*, 71 NOTRE DAME L. REV. 79, 118 (1995) (defining collateral censorship as "the silencing by a private party of the communication of others"); *see also* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem*

A to block B's speech or withdraw infrastructural support from B.[40] In fact, because A's own speech is not involved, A has incentives to err on the side of caution and restrict even fully protected speech in order to avoid any chance of liability.[41]

In this respect collateral censorship has affinities both to overbreadth and to systems of prior restraint. A acts without any prior judicial determination of the legality of B's speech, and B may have no prior notice of A's decision to block or withhold infrastructural services.[42] The state creates incentives for A to overcensor. Because A's and B's incentives are not aligned, A's actions will likely block or restrict access to much protected expression along with the unprotected.[43]

Although collateral censorship is not a new phenomenon,[44] it has become particularly important in the digital age. That is because so much speech travels through privately owned conduits like ISPs and broadband providers, appears on privately owned hosting services and platforms, rests on the efficient operation of the domain name system (including the ability to link from one site to another), depends on auxiliary services like search engines and social media in order to be discovered, or relies on online payment systems to finance operations through contributions from large numbers of individuals. Virtually every aspect of the digital infrastructure of free expression can be a potential target of collateral censorship.

Collateral censorship is not always troubling. It is least threatening to freedom of expression when it makes sense to treat A and B as the same entity or speaker for purposes of First Amendment law.[45] Collateral censorship is least constitutionally problematic when the case for the vicarious

---

of the Weakest Link, 155 U. PA. L. REV. 11, 11, 16 (2006) (coining the terms "proxy censorship" and "censorship by proxy").

40 The government can achieve similar effects through its "soft power" of influence, which operates as an informal method of collateral censorship. *See infra* section II.C.2.c, TAN 125–143.

41 Even though the censorship is by a private party, there is state action "because the government has created incentives for private parties to censor each other." Balkin, *supra* note 39, at 2299.

42 *Cf.* Mulligan, *supra* note 39, at 165 (comparing collateral censorship to prior restraint because the speaker has no say over whether he or she is blocked by the intermediary).

43 *See* Balkin, *supra* note 39, at 2303 (noting that in cases of collateral censorship speech is blocked regardless of its protected status); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 296 (2011) ("For example, imposing defamation liability on a message board operator for carrying defamatory content may well induce it to block a wide array of potentially defamatory content, including some which is in fact true or mere opinion, or otherwise not actionable.").

44 *See* Meyerson, *supra* note 39, at 116–17 (giving the examples of government pressure on charitable solicitors and distributors); Balkin, *supra* note 39, at 2302 ("The most obvious example occurs when courts and legislatures impose liability for harmful speech on a distributor, a common carrier, or some other conduit that is not part of the same business enterprise as the censored speaker, lacks the right to exercise editorial control, and lacks information about the nature of the content flowing through its channels.").

45 Balkin, *supra* note 39, at 2300–02.

liability of a publisher is the strongest.[46] That is why, for example, it is ordinarily not constitutionally troublesome if newspapers are generally held liable for the speech of their reporters, columnists, and advertisers, or if book publishers are held liable for the work of the authors they publish.[47]

When A and B are unrelated parties, however, and when the Bs of the digital world are producing enormous amounts of new content that may be difficult to supervise or edit individually, holding A responsible for B's speech is likely to lead to overblocking and unjustified interference with speech.[48] In the digital age, most of the digital infrastructure is owned by persons other than the speakers, and the relationship between the infrastructure owner and the speaker differs greatly from that between an author and a book publisher. Hence the opportunities for problematic forms of collateral censorship are ubiquitous.

What looks like a problem from the standpoint of free expression, however, may look like an opportunity from the standpoint of governments that cannot easily locate anonymous speakers and want to ensure that harmful or illegal speech does not propagate. Collateral censorship may be especially important for states that want to encourage filtering and blocking of content from overseas, because governments cannot generally control foreign intermediaries and speakers.

Intermediary liability is also a strategy for promoting public/private cooperation in speech regulation.[49] For example, states might want intermediaries to flag and delete suspicious content, develop or finance effective filtering technologies (which the state can then use), shut down accounts, or hand over private user information. These tasks may be resource intensive and governments may be unable to perform them easily on their own. Threats of intermediary liability — coupled with promises of immunity for compliance — help states persuade owners of private infrastructure to work with them and for them.

The problem of collateral censorship has made landmark decisions like *New York Times Co. v. Sullivan* increasingly inadequate in the digital age. Like much of traditional First Amendment law, *Sullivan* sought to protect speech by limiting direct suits or prosecutions against speakers and traditional publishers. Today, however, both the government and private parties are more likely to view the intermediary as the most tempting target for regulation.[50]

---

[46] *Id.* at 2301.

[47] *Id.* at 2301–02.

[48] *Id.* at 2302.

[49] *See infra* section II.C, TAN 111–143.

[50] *See* Kreimer, *supra* note 39, at 14 ("[S]tate actors who seek to control Internet communications have begun to explore strategies that target neither speakers nor listeners.").

A little-noticed feature of *Sullivan* is that it was also a case about intermediary liability, but in 1964 the Supreme Court did not spot the issue.[51] The *New York Times* was sued for something it did not actually write — an advertisement.[52] Under the common law rules of publisher liability, however, the *Times* was responsible for defamatory content it published.[53] The Supreme Court's decision in *Sullivan* did not question this feature of the common law or even see it as a problem for freedom of speech.[54] In fact, *Sullivan* and later cases assumed that the common law rules of publisher liability and respondeat superior would continue to apply to libel suits.[55]

These assumptions proved ill suited to the digital age. In the 1990s, telecommunications companies quickly recognized that they would be transmitting and storing large amounts of content that they did not produce (and could not reliably edit). Something more than *New York Times Co. v. Sullivan* would be necessary.[56]

The closest the Supreme Court came to recognizing collateral censorship as a First Amendment issue was in a 1959 case, *Smith v. California*.[57] *Smith* struck down a statute that held booksellers criminally liable for stocking books later judicially determined to be obscene, even if the bookstore owner did not know of the content of the books.[58]

---

[51] *See* Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1005 (2008) ("*Sullivan* was a case about the *Times* as intermediary, displaying another entity's supposedly defamatory ad after only minimal screening.").

[52] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 256 (1964).

[53] *Id.* at 262 (quoting jury instructions); *see* RESTATEMENT (SECOND) OF TORTS § 578 (1977) ("Except as to those who only deliver or transmit defamation published by a third person, one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.").

[54] *See Sullivan*, 376 U.S. at 286–88 (discussing whether the *Times* as publisher had the requisite malice, but not whether publishers were liable for statements they did not compose or edit).

[55] *See* Cantrell v. Forest City Publ'g Co., 419 U.S. 245, 253–54 (1974) (approving a jury charge which permitted the imposition of vicarious liability upon a publisher for the knowing falsehoods written by its staff writer).

[56] Tushnet, *supra* note 51, at 1007 ("The [Communications Decency Act] was enacted on the theory that no ISP would accept the risk of standard *Sullivan*-type liability, given the massive amounts of user-generated content that the Internet allows."). The problem was brought to a head by two lower court cases, which came out in opposite directions. *Compare* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 138–42 (S.D.N.Y. 1991) (holding that CompuServe was merely a common law distributor of content on its online fora and could not be expected to supervise or edit its content), *with* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *4 (N.Y. Sup. Ct. May 24, 1995) (holding that Prodigy was a publisher because it held itself out as moderating its bulletin boards and employed software to screen out content). First Amendment lawyer Floyd Abrams argued that even *CompuServe*'s adoption of distributor liability would not be enough to protect telecommunications companies. *See* Floyd Abrams, *First Amendment Postcards from the Edge of Cyberspace*, 11 ST. JOHN'S J. LEGAL COMMENT. 693, 704 (1996) ("[A] far more protective standard is needed than [*CompuServe*'s] 'reason to know' [standard] . . . . It does not now exist as a matter of common law." (punctuation omitted)).

[57] 361 U.S. 147 (1959).

[58] The Court explained that:

Instead of attempting to extend *Smith*, telecommunications companies bargained for intermediary immunity in legislation.[59] The United States now offers intermediaries several different levels of protection depending on the content involved.[60] Section 230 of the Telecommunications Act of 1996,[61] for example, holds users or providers of interactive services harmless for offensive content, but it does not apply to liability based on infringement of intellectual property.[62] Section 512 of the Digital Millennium Copyright Act of 1998[63] (DMCA) offers a safe harbor for Internet service providers, backbone operators, and similar conduits when potentially infringing content flows through them without their knowledge;[64] it also creates an elaborate notice-and-takedown procedure for intermediaries (like YouTube) that host other people's content.[65]

Section 230 immunity and, to a lesser extent, § 512 safe harbors have been among the most important protections of free expression in the United States in the digital age. They have made possible the development of a wide range of telecommunications systems, search engines, platforms, and cloud services without fear of crippling liability.[66] An early version of Google or Facebook might not have survived a series of defamation lawsuits if either had been treated as the publisher of the countless links, blogs, posts, comments, and updates that appear on their facilities. Both the § 230 immunity and the § 512 safe harbors, however, resulted from

---

> [I]f the bookseller is criminally liable without knowledge of the contents, . . . he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature. . . . The bookseller's self-censorship, compelled by the State, would be a censorship affecting the whole public, hardly less virulent for being privately administered.

Id. at 153–54. What the Court calls "self-censorship" is actually collateral censorship by the government using the bookseller; it is made possible by the different incentives of the bookseller and the book author. Balkin, *supra* note 39, at 2302 & n.25 (citing Meyerson, *supra* note 39, at 118 n.259).

Smith, in turn, was analogous to the common law rules of distributor liability, which hold distributors harmless if they are unaware of the defamatory content of what they distribute. *See CompuServe*, 776 F. Supp. at 141–42.

59 Tushnet, *supra* note 51, at 1007–08 & nn.94–95 (arguing that instead of seeking a "super-*Sullivan*," *id.* at 1008 n.95, the communications industry sought a legislative fix, *id.* at 1007 n.94).

60 *See id.* at 1004–05 (noting different intermediary liability regimes for state law torts including defamation and fraud, copyright infringement under the DMCA, other intellectual property violations, and criminal accessory liability for obscenity and child pornography).

61 47 U.S.C. § 230 (2006).

62 *Id.* § 230(c)(1) ("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.").

63 17 U.S.C. § 512 (2012).

64 *See id.* § 512(a) (providing immunity for "[t]ransitory [d]igital [n]etwork [c]ommunications"); *id.* § 512(b) (providing immunity for temporary caching).

65 *See id.* § 512(g) (describing notice-and-takedown procedure for service providers).

66 *See* Balkin, *The Future of Free Expression in a Digital Age*, *supra* note 14, at 436–38 (describing intermediary liability's effects on innovation).

legislative acts rather than Supreme Court decisions. And not all countries have speech-protective rules of intermediary liability.[67]

What a system of intermediary immunities and safe harbors does not protect, however, constitutes a system of intermediary liability and, hence, of potential collateral censorship. Section 512(g) of the DMCA offers companies that host content a safe harbor only if they agree to a notice-and-takedown scheme. If a private party alleges that the intermediary is hosting content that infringes the party's copyrights, the intermediary must promptly remove it or risk liability.[68] Thus, intermediaries still have incentives to take down content that is protected by fair use and the First Amendment.[69] Individuals can get their content restored if they submit a counter-notice, identify themselves, and agree to jurisdiction and service of process, but very few do.[70] As a result, the notice-and-takedown rules limit the speech of those who wish to speak anonymously, those who cannot afford legal representation, and those who live overseas and do not wish to subject themselves to litigation in American courts. Moreover, the content industries have repeatedly pushed for ever-greater intermediary liability, both through interpretations of § 512 of the DMCA[71] and through new statutes that would render its safe harbor provisions largely superfluous.[72]

B. Digital Prior Restraint

1. Old School: Traditional Prior Restraints and Their Effects. — One of the oldest forms of speech regulation, dating back to the early days

---

67 *See, e.g.*, Noah C.N. Hampson, Comment, *The Internet Is Not a Lawless Prairie: Data Protection and Privacy in Italy*, 34 B.C. INT'L & COMP. L. REV. 477 (2011) (describing Italy's prosecution of three Google executives for a YouTube video that violated the privacy rights of an autistic student who was shown being bullied by classmates); Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481 (2009) (describing differences between American DMCA safe harbors and the European Union Council Directive on Electronic Commerce).

68 *See* 17 U.S.C. § 512(g) (describing notice-and-takedown procedure).

69 *See, e.g.*, Mulligan, *supra* note 39, at 181–84 ("The notice-and-takedown system . . . obviates the safeguards for speech in actually bringing a copyright infringement lawsuit." *Id.* at 181.); Tushnet, *supra* note 51, at 1003 ("Because DMCA notice requirements are minimal and ISPs have no incentive to investigate, the notice-and-takedown process can be used to suppress critical speech as well as copyright infringement.").

70 *See* Tushnet, *supra* note 51, at 1003 ("[M]ost users who receive notice do not counternotify, even when they might have valid defenses.").

71 *See, e.g.*, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (litigating the degree of knowledge of infringement necessary to qualify for DMCA safe harbors), *aff'd in part, vacated in part, rev'd in part and remanded*, 676 F.3d 19 (2d Cir. 2012).

72 *See infra* section II.B.2.c, TAN 89–97 (discussing the Combating Online Infringement and Counterfeits Act, the Stop Online Piracy Act, and the PROTECT IP Act of 2011). Moreover, § 230 comes with an additional twist: it holds online service providers harmless when they do block and filter content, thus making it easier for them to cooperate with the government. *See* 47 U.S.C. § 230(c)(2) (2006).

of the printing press, is prior restraint.[73] Although today prior restraint is generally associated with judicial injunctions — the subject of *Pentagon Papers* — its roots lie in older systems of licensing and bureaucratic administration, in which states required licenses to operate a printing press and required preclearance of content before it could be published.[74]

The government's request for an injunction in the *Pentagon Papers* case assumed certain facts about the world and about communications technology that made an injunction worth obtaining. The request for an injunction assumed, for example, that the Pentagon Papers could be successfully published only if newspapers got copies and had the time to typeset them. It assumed that making copies of the original set would take considerable time and effort and that Daniel Ellsberg did not have the then-magical ability to make multiple electronic copies of the Papers and spread them instantaneously around the globe and beyond the reach of American courts.

The idea that government might successfully suppress sensitive information like the Pentagon Papers through a judicial injunction seems almost quaint today. The Daniel Ellsbergs of the present would likely partner with an organization like WikiLeaks, which has secure servers in many different places overseas.[75] WikiLeaks, in turn, would partner (and has partnered) with established news organizations in different countries around the world to generate publicity for the leaks. When the WikiLeaks cables began publication, the Obama Administration did not try seeking an injunction like the Nixon Administration. Instead, it relied on different methods for controlling WikiLeaks.[76]

Nevertheless, even in a digital world, prior restraint — including ex parte injunctions — can still be an important tool of speech regulation if employed in the right way. Some of the most important features of new-school speech regulation employ digital technologies to achieve effects similar to traditional prior restraints even though they do not use licensing schemes and judicial injunctions. Before discussing these new-school techniques, therefore, it is important to understand how prior restraints

---

[73] *See* FREDRICK SEATON SIEBERT, FREEDOM OF THE PRESS IN ENGLAND, 1476–1776, at 21–30 (1952).

[74] *See* Philip Hamburger, *The Development of the Law of Seditious Libel and the Control of the Press*, 37 STAN. L. REV. 661, 673 (1985) ("[L]icensing . . . offered many advantages. Especially created for the task of controlling written material, licensing provided the Crown with censorship prior to publication and easy conviction of offenders.").

[75] MICAH L. SIFRY, WIKILEAKS AND THE AGE OF TRANSPARENCY 27–28, 37 (2011); Noam Cohen, *What Would Daniel Ellsberg Do with the Pentagon Papers Today?*, N.Y. TIMES, Apr. 19, 2010, at B3.

[76] *See infra* section II.C.2.c, TAN 125–143.

work and why they restrict press freedoms more than do subsequent criminal prosecutions.[77]

Prior restraints (which include licensing schemes) are especially troublesome because they shift the costs of action, the burdens of proof, and the consequences of inertia from the state to the speaker. Prior restraints attempt to make offending content easy to identify, block, and control, and offending speakers easy to prosecute, punish, and deter. We can divide these effects into six categories:

(a) Deliberate Overbreadth of Coverage. — First, prior restraints subject a much greater breadth and variety of content to government scrutiny and surveillance than a system of subsequent prosecution and punishment. The prosecutor or civil plaintiff only considers actions that come to their attention and then must decide whether or not to act; in a system of prior restraint, everything, no matter how innocent, is placed before the government and requires the government's permission before it may be published. The power — and the vice — of prior restraint is that both protected and unprotected content are lumped together.

(b) Shifting the Burden of Inaction/Inertia. — Second, under a system of prior restraint, communication — including communication of content that is completely protected under the First Amendment — cannot occur until permission is granted, which may undermine the communicative force or value of the message. It is up to the speaker to gain the state's permission. If the government does not respond and give permission, the speaker is silenced. In a system of subsequent punishment, there is no delay in expression and it is up to the state to react. If the state does nothing, free expression continues. In this way, the practice of prior restraint magnifies the problem of overbreadth, because significant amounts of protected material may be blocked indefinitely to facilitate the search for unprotected material.

(c) Shifting Decisionmaking to Limited Procedural Protections and Extra-Judicial Procedures. — Third, a system of subsequent punishment entitles the speaker to the full panoply of procedural protections, including trial by jury, as well as constitutional protections for freedom of speech. A system of prior restraint can be administrative or informal, and the question is not whether the content is protected by the First Amendment, but whether the administrator thinks it falls into the relevant statutory categories. Executive or administrative officials make the judgment, and that judgment may be subject only to a more limited judicial review of administrative action. Moreover, in the digital age, decisions may be made by

---

[77] For the canonical discussion of the First Amendment problems of prior restraints, see Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 LAW & CONTEMP. PROBS. 648, 656–60 (1955). *See also* Stephen R. Barnett, *The Puzzle of Prior Restraint*, 29 STAN. L. REV. 539 (1977); Vincent Blasi, *Toward a Theory of Prior Restraint: The Central Linkage*, 66 MINN. L. REV. 11 (1981); John Calvin Jeffries, Jr., *Rethinking Prior Restraint*, 92 YALE L.J. 409 (1983).

software programs, with no human intervention, and there may be no practical method of judicial review.

(d) Shifting from Public Prosecution to Low-Visibility Systems of Control. — Fourth, a system of prior restraint can operate in the background, outside of public scrutiny. It can be administratively routinized and mechanized. This problem is heightened when blocking or filtering of digital content is automatic. A system of subsequent punishment requires an individualized decision to prosecute and, in many cases, a criminal or civil trial; this affords a greater opportunity for public scrutiny and public discussion about whether prosecution is wise.

(e) Shifting the Burden of Error Costs. — Fifth, systems of prior restraint create institutional incentives for over-censorship. As Professor Thomas Emerson once explained, "[t]he function of the censor is to censor. He has a professional interest in finding things to suppress. . . . He is often acutely responsive to interests which demand suppression — interests which he himself represents — and not so well attuned to the more scattered and less aggressive forces which support free expression."[78] This is all the more the case when the power to enjoin is placed in private hands or automated in a filtering program.

(f) Forcing Self-Identification; Increasing the Probability of Location, Apprehension, Suppression, and Punishment. — Sixth, prior restraints are designed to make it more likely that the content that interests government will be suppressed and its publishers identified and punished. In a system of subsequent punishment, the government has to locate the offending content and then decide whether it is worth the time and resources to prosecute. A system of prior restraint shifts the burden of expense from the government to the speaker and lowers the cost of censorship. The burden falls on the speaker to prove why the content should be published.

If the speaker ignores or defies the licensing system in a system of prior restraint, the central question is not whether the content was constitutionally protected, but whether the speaker obtained proper permission beforehand. This is the central feature that makes judicial injunctions operate like prior restraints.[79] Under the collateral bar rule, if a person violates a court order injunction against publication, the publisher ordinarily loses the right to challenge the constitutionality of the court's order as a defense to a contempt charge.[80]

---

[78] Emerson, *supra* note 77, at 659.

[79] Jeffries, *supra* note 77, at 431–32 (arguing that one feature of injunctions that may make them more troubling than subsequent punishment is the continuing vitality of the collateral bar rule).

[80] Richard E. Labunski, *The "Collateral Bar" Rule and the First Amendment: The Constitutionality of Enforcing Unconstitutional Orders*, 37 AM. U. L. REV. 323, 327 (1988) (describing the rule). Courts have grafted exceptions onto the doctrine to mitigate its harshness, arguing that the rule should not apply where the order is "transparently invalid." *See* Walker v. City of Birmingham, 388 U.S. 307, 315 (1967) (invoking the collateral bar rule and arguing that "this is not a case where the injunction was transparently invalid or had only a frivolous pretense to validity"); *In re* Providence Journal Co., 820

Moreover, a criminal prosecutor who suspects that someone has violated the law normally does not take the violation as a personal affront; instead, he or she engages in a professional calculus of whether prosecution is worth the effort given limited resources. On the other hand, if a speaker fails to ask permission in a system of prior restraint, the licensors (or the judge, in the case of an injunction) are more likely to view the act as a threat to their authority, causing them to favor certain and severe punishment in order to establish their power.

2. New School: Prior Restraints Aimed at the Digital Infrastructure. — Digital technology allows both the state and cooperating private parties to achieve many of the same cost- and burden-shifting effects of prior restraint through techniques that do not necessarily involve administrative or bureaucratic review on the one hand, or judicial injunctions on the other.

(a) Filtering. — Filtering systems use technology to achieve many of the same effects as a traditional prior restraint. Filtering systems are often overbroad — particularly when filtering is done at the DNS or IP level.[81] Especially when the goal is to reduce cost and achieve comprehensiveness, however, overbreadth may be a feature, not a bug.

Filtering methods are often kept secret — and may be protected by trade secret law — in order to prevent reverse engineering. Filtering criteria — especially when the state uses filters designed by private parties — may not respect First Amendment categories, and may be inappropriately content-based or viewpoint-based.[82] Filtering systems block speech automatically without an opportunity to contest the filter and without procedural protections for the speaker or an individualized constitutional analysis of the speech that is blocked.[83] Error costs are borne by the speaker, not the filtering system, and the burden is on the speaker to have the block altered

---

F.2d 1342, 1347 (1st Cir. 1986) ("[A] transparently invalid order cannot form the basis for a contempt citation.").

[81] Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 397 (2009) ("Most, if not all, Internet filtering systems will be overbroad (blocking innocent content), underbroad (failing to block proscribed material), or both.").

[82] Where there is no state action, there is no constitutional objection to private parties filtering based on content and viewpoint, and another provision of section 230 even holds intermediaries harmless for blocking content. 47 U.S.C. § 230(c)(2) (2006). Nevertheless, when content- or viewpoint-based filtering results from collateral censorship by the government, there is state action. *See* Balkin, *supra* note 39, at 2299.

[83] This point is especially important in the context of intellectual property. Many new-school speech regulations are directed at potential violations of copyright. Although "[p]reliminary injunctions [against specific publications] are a common judicial response to the imminent infringement of an apparently valid copyright," Dall. Cowboys Cheerleaders, Inc. v. Scoreboard Posters, Inc., 600 F.2d 1184, 1187 (5th Cir. 1979) (collecting cases), it does not follow that administrative or technological schemes of prior restraint — which do not involve any judicial determination of infringement — are beyond the free speech principle.

or removed. Finally, filtering systems operate silently in the background, and their effects may be unnoticed by the general public.[84]

(b) Domain Name Seizures. — States can also control content by asserting control over the domain name system, which connects IP numerical addresses to domain names like www.nytimes.com. In November 2010, for example, the Department of Homeland Security launched Operation In Our Sites, which seizes the domain names of persons or entities suspected of infringing intellectual property rights.[85]

Domain name seizures share at least five features of traditional prior restraints. First, they are overbroad by design; crippling the domain name system blocks all content reachable by a given domain name. Second, they shift the burden of inaction and inertia; access through the domain name system is blocked until the government restores the domain name. Third, seizures generally involve ex parte proceedings with limited procedural protections for affected speakers. Fourth, seizures are low-visibility operations. Fifth, in seizing domain names the government may work with members of private industry who have few incentives against overzealous prosecution.

In one unfortunate incident, agents of the Immigration and Customs Enforcement (ICE) seized the domain name of a hip-hop website operated by Dajaz1 on suspicion of facilitating copyright infringement. The affidavit justifying the seizure was based on inaccurate information; in particular, the allegedly infringing links that justified the seizure order had actually been given to Dajaz1 by the artists themselves.[86] Nevertheless, the ICE and the Deparment of Justice, working with the Recording Industry Association of America (RIAA), kept the site down for a year, in part by obtaining a series of secret, ex parte extensions to the initial order.[87] Ultimately the seized domain was restored after the government decided that there was lack of probable cause to proceed with a prosecution.[88]

---

[84] The government may also make circumvention of filtering technology illegal. *Cf.* 17 U.S.C. § 1201 (2012) (outlawing distribution of technologies that circumvent access control devices).

[85] NAT'L INTELLECTUAL PROP. RIGHTS COORDINATION CTR., OPERATION IN OUR SITES, http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf (last visited May 10, 2014), *archived at* http://perma.cc/6KMD-5BTW.

[86] Dara Kerr, *Homeland Security's Domain Seizures Worries Congress*, CNET (Sept. 3, 2012, 8:41 PM), http://news.cnet.com/8301-1023_3-57505318-93/homeland-securitys-domain-seizures-worries-congress/, *archived at* http://perma.cc/9U3Q-CSBT.

[87] *See In the Matter of the Seizure of the Internet Domain Name "DAJAZ1.COM,"* ELEC. FRONTIER FOUND., https://www.eff.org/cases/matter-seizure-internet-domain-name-dajaz1com (last visited May 10, 2014), *archived at* http://perma.cc/X42D-5NL2 (sealed court records released to the public in May 2012); Kerr, *supra* note 86.

[88] *See* Kerr, *supra* note 86; Timothy B. Lee, *Waiting on the RIAA, Feds Held Seized Dajaz1 Domain for Months*, ARS TECHNICA (May 4, 2012, 11:41 AM), http://arstechnica.com/tech-policy/2012/05/waiting-on-the-riaa-feds-held-seized-dajaz1-domain-for-months/, *archived at* http://perma.cc/URT7-V56S; *see also* Bambauer, *supra* note 8, at 865–67 (describing Operation Protect Our Children, in which the Departments of Justice and Homeland Security used ex parte orders to take

This episode contains three of the signature aspects of new-school speech regulation: (1) cooperation between government and private industry, (2) attacks on Internet infrastructure to control speech, and (3) new enforcement techniques that route around traditional procedural guarantees and civil liberties protections.

(c) Injunctions Designed to Induce Filtering and/or Collateral Censorship. — States, often urged on by the content industries, have also devised elaborate new schemes that use injunctions in novel ways. Their central innovation is a shift from restraints that target speakers to restraints that target owners of private infrastructure; the goal is to get owners of private infrastructure to do the work of surveillance, blocking, and filtering.

Three excellent examples are recent pieces of legislation proposed (and thankfully rejected) in the United States Congress: The Combating Online Infringement and Counterfeits Act (COICA),[89] the Stop Online Piracy Act (SOPA),[90] and the PROTECT IP Act of 2011 (PIPA).[91] These bills had the ostensible purpose of regulating, blocking, and punishing foreign websites that did nothing other than provide materials that infringed intellectual property rights. Yet their actual provisions reached so broadly that they would have swept in a great deal of protected expression in the process. The two bills eventually generated enormous controversy. They were widely opposed by Internet activists, technology companies, and members of the general public because of their perceived threats to freedom of expression and Internet freedom generally.[92] Indeed, the protests against SOPA and PIPA are among the most prominent recent examples of popular constitutionalism in the defense of free speech rights.[93]

---

control over domain names believed to host child pornography, sweeping up sites that were innocent of any crime).

89 Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. (2010), *archived at* http://perma.cc/EQ5S-2B28.

90 Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011), *archived at* http://perma.cc/88NK-M47F.

91 Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (as amended, May 26, 2011) [hereinafter PIPA], *archived at* http://perma.cc/LK8N-9PB4.

92 On the history of the protests against SOPA and PIPA, see generally EDWARD LEE, THE FIGHT FOR THE FUTURE (2013), *archived at* http://perma.cc/6CNV-F7E3. During a high point in the protests, on January 18, 2012, Wikipedia went black to protest the two bills; Google used an anti-SOPA logo with a link for more information, and Mozilla directed the Mozilla.org and Mozilla.com English webpages to an "action page." Vlad Savov, *The SOPA Blackout: Wikipedia, Reddit, Mozilla, Google, and Many Others Protest Proposed Law*, THE VERGE (Jan. 18, 2012, 12:10 AM), http://www.theverge.com/2012/1/18/2715300/sopa-blackout-wikipedia-reddit-mozilla-google-protest, *archived at* http://perma.cc/GVK3-9DFM; *see also* Yochai Benkler et al., *Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate* (Berkman Ctr. for Internet & Soc'y, Research Publ'n No. 2013-16, 2013), *archived at* http://perma.cc/5SB4-YYJK (showing the evolution of the controversy online).

93 Precisely because the courts never passed on the constitutionality of the two bills, the episode belongs in the same category as a number of other political controversies that shaped concepts of freedom of expression in the United States. *See generally* MICHAEL KENT CURTIS, FREE SPEECH, "THE

Although these bills were not enacted into law, they are instructive for two reasons. First, Congress, which is subject to continuing lobbying from the content industries, may well attempt similar legislation in the future. Second, these bills show how a determined government — often working hand in hand with private industry — can leverage many different aspects of the digital infrastructure to create ingenious new methods of control. Thus, studying the techniques used in SOPA, PIPA, and COICA offers us a window on the likely free speech controversies of the future.

Section 102 of SOPA, for example, gave the U.S. attorney general the ability to obtain injunctions against "foreign infringing sites."[94] This term was broadly defined to include sites whose *domain name* is registered outside the U.S. — even if it is an American company using a foreign registrar.[95] More important, a site was treated as "infringing" if any portion of the site "facilitat[es]" copyright infringement.[96] The latter term is vague and subject to varying interpretations. It might apply, for example, to platforms similar to Facebook or YouTube whose customers often upload or link to infringing content. If these sites have not installed filters to block all such content or prevent it from being uploaded, the argument would go, they might be "facilitating infringement" within the meaning of the statute, even though they have no knowledge of specific infringing activity and they would not be secondarily liable under existing copyright law.

Section 102 thus threatened to do an end run around the safe harbor rules of the DMCA. These provisions protect intermediaries from liability for copyright infringement unless the intermediaries have actual knowledge of infringing activity on their services, or in the words of the House Report on the DMCA, "turned a blind eye to 'red flags' of obvious infringement."[97]

The DMCA's standard of actual knowledge ameliorates problems of collateral censorship. Conversely, section 102 would have given intermediaries who fell within the statutory definition incentives to engage in collateral censorship — for example, through installing content filters — that would benefit the content industry. Thus, the goal of an injunction against a party doing business in the United States is not to shut down its operations but to induce it to engage in filtering and blocking the content and

---

PEOPLE'S DARLING PRIVILEGE" (2000) (reviewing significant freedom of speech controversies in American history).

94 H.R. 3261 § 102.

95 *Id.* § 101(4) & (8). *See* Marvin Ammori, *SOPA/PIPA Copyright Bills Also Target American Sites*, AMMORI.ORG (Dec. 31, 2011), http://ammori.org/2011/12/31/sopapipa-copyright-bills-also-target-domestic-sites/, *archived at* http://perma.cc/5UBX-7UXB (giving examples of Google.ca and Amazon.co.uk).

96 H.R. 3261 § 102(a).

97 H.R. REP. NO. 105-551, pt. 2, at 57 (1998); *see also* 17 U.S.C. § 512(c)(1)(A)(ii) (2012) (providing that to benefit from the safe harbor, an ISP must "not [be] aware of facts or circumstances from which infringing activity is apparent").

speech of others. The goal of the injunction, in other words, is collateral censorship.

(d) Prior Restraints Directed Against the Digital Infrastructure. — In many cases, however, a site accused of being a "foreign infringing site" would be outside the United States and would not submit to the jurisdiction of American courts. In these cases, the U.S. attorney general could get an injunction without an adversary hearing.[98] Of course, an injunction directed against such an overseas site might do little to stop the site itself. Nevertheless, once the attorney general was armed with an ex parte injunction, the real power of the statute would be revealed. Instead of going after the original site, the attorney general could then issue commands to many different parts of the digital infrastructure within the United States. The government could order search engines not to link to the site, it could order online advertisers not to advertise on the site, and it could order payment processors (for example, credit card companies) not to transact business between U.S. customers and the site.[99]

Perhaps most important, the attorney general could order all Internet "service provider[s]"[100] — which include broadband companies, university networks, libraries, private networks, phone companies, and cable companies — to take "technically feasible and reasonable measures designed to prevent access" to the site.[101] This would include not only blocking and filtering, but also preventing the site's domain name (for example, nytimes.com) from resolving to the domain's assigned Internet Protocol address (for example, 170.149.172.130, the IP address currently assigned to nytimes.com[102]). In other words, the government could issue orders to interfere with the practical functioning of the domain name system, which translates familiar domain names into numerical Internet addresses that allow communication between networks. The integrity of this system is crucial not only to effective worldwide communication but also to cybersecurity.[103]

All of these businesses would face potential government lawsuits if they objected to the orders, but would receive legal immunity if they cooperated.[104] SOPA thus created incentives for key elements of the Internet

---

98 *See* H.R. 3261 § 102(b)(2).

99 *Id.* § 102(c).

100 *Id.* § 102(c)(2)(A); *id.* § 101(22) (cross-referencing 17 U.S.C. § 512(k)(1) (2012)).

101 *Id.* § 102(c)(2)(A).

102 *See IP-Tracker.org, IP Locator also known as IP Lookup Tool*, http://www.ip tracker.org/locator/iplookup.php?ip=nytimes.com, *archived at* http://perma.cc/6WWM-5VUM (last visited May 10, 2014) (identifying the IP address of nytimes.com).

103 *See* Mark Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 34–35 (2011) (discussing the effects of the DNS provisions of SOPA and PIPA); Vint Cerf et al., An Open Letter from Internet Engineers to the United States Congress (Dec. 15, 2011), *archived at* http://perma.cc/32MP-LUAZ (arguing that SOPA and PIPA would create serious security risks).

104 H.R. 3261 § 102(c)(5).

infrastructure to assist the government in blocking U.S. citizens' access to foreign sites — regardless of the proportion of the foreign site that contained infringing materials (it could be only one page out of a thousand), and regardless of whether the materials were actually proven to be infringing — all based on ex parte injunctions. This technique is potentially more powerful than the traditional prior restraint to the extent that it gives the government control not over the original publisher but over key aspects of the digital infrastructure.

(e) "Private Prior Restraint" Directed Against the Digital Infrastructure. — In addition to government orders against third parties, section 103 of SOPA envisioned a new system of digital control that we might call "private prior restraint." It deputized private parties to control other private parties who in turn operate the digital infrastructure. If a private party notified an online advertiser or a payment processor that it was doing business with a website "dedicated to [the] theft of U.S. property,"[105] advertisers and payment processors would have five days to stop dealing with the site or face potential legal sanctions.[106] The complaining private party did not actually have to prove anything in court to set this machinery in motion; it merely had to make the allegation that it was harmed by activities on the site "or portion thereof,"[107] which might include one page on a web platform consisting of thousands of pages.

The term "dedicated to the theft of U.S. property" was also defined very broadly. It included any business that either "facilitates"[108] infringement or "avoid[s] confirming a high probability"[109] of infringing activity on its site, regardless of whether the business has knowledge of specific infringing activities and whether it would be secondarily liable under existing law.[110] This provision would have made vulnerable most businesses that rely on user-created content — which is to say, a significant chunk of the digital infrastructure of free expression. Third parties could continually threaten to deter payment processors and advertisers from dealing with these companies.

The point of the system of private prior restraint is to induce businesses that rely on advertising and payment systems to install filters and to continually police and remove any suspicious content on any portion of their platforms or websites. In other words, the goal of the system is to induce companies to engage in collateral censorship, with the predictable conse-

---

105 *Id.* § 103(a)(1) (internal quotation mark omitted).

106 *Id.* § 103(b); *id.* § 103(d)(4). If the accused site issues a counter-notice, *id.* § 103(b)(5), or if the payment provider or advertiser fails to stop doing business with the site within five days, *id.* § 103(c), the accuser can also sue for an injunction against the domain name registrar to prevent resolution of the domain name. *Id.* § 103(c).

107 *Id.* § 103(a)(2).

108 *Id.* § 103(a)(1)(B)(i).

109 *Id.* § 103(a)(1)(B)(ii).

110 *See supra* TAN 65–66 (discussing the standard of intent under the DMCA).

quences of overfiltering and overblocking. Those companies that refuse would have to scramble to find payment systems and advertisers who would continue to deal with them. To the extent that no one will deal with them, their operations are thereby curtailed. This feature leads to the next set of techniques, digital blacklists.

C. Public/Private Cooperation and Co-optation — From McCarthyism to Digital Blacklists

1. Old School: Public/Private Cooperation and Co-optation. — In old-school speech regulation, the state does not act alone. Private parties may push the state to regulate speech, and even offer their assistance. Conversely, the state may enlist the assistance of private parties, either through sticks, carrots, or a combination of the two. A related strategy is media co-optation. The desire for good relationships between the press and government officials and continued access to government sources may lead media organizations to pull their punches in coverage, skew coverage, self-censor, or delay publication of embarrassing materials.

Private parties may also assist the state by engaging in private surveillance and identifying suspicious people to the authorities, or by shunning or blacklisting dissidents or persons suspected of engaging in activity the state wants to restrict. The system of blacklists that we now associate with the McCarthy period is an example of public/private cooperation and co-optation. The government made clear that it wanted to root out communists in industries, education, the arts, and the professions. Private parties took this as a signal to refuse to do business with people who were suspected of having subversive sympathies or who refused to cooperate with the government's search for subversives.

2. New School: Data Sharing, Immunities, and Digital Blacklists. — Public/private cooperation and co-optation are hallmarks of new-school speech regulation.[111] In some cases, as in the recent revelations regarding government surveillance, the government serves owners of private infrastructure with gag orders that forbid them from discussing these arrangements.[112] In other cases the government offers a combination of carrots and sticks, the most important being legal immunity for assisting the government in identifying or shutting down Internet sites and speakers that the government disfavors or seeks to regulate.

(a) Access to Data. — Many private entities collect and sell personal data to governments to facilitate surveillance and analysis; this practice allows federal and state governments to route around the requirements of the

---

111 *See generally* Yochai Benkler, *WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons*, DAEDALUS, Fall 2011, at 154; Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003).

112 *See infra* Part III, TAN 144–195.

Fourth Amendment.[113] Whether willingly or not, private companies — including telecommunications companies, search engines, and social media companies — can give the state access to their data either directly or through intermediaries.[114] At government request (or compulsion), private companies can also build special access facilities or "backdoors" that enable government penetration of their communications and data storage systems.[115] In return, the state can offer private companies immunity for cooperation, for technological access, and for policing and blocking speech that the government finds harmful or dangerous. The FISA Amendments Act of 2008,[116] for example, offered telecommunications companies retroactive immunity for working with the government to share data.[117] Failure to cooperate, in turn, may subject private companies either to legal liability or to regulatory pressure.

(b) Immunity for Collateral Censorship. — States can give intermediaries immunity if they engage in collateral censorship. If an intermediary searches for and blocks offending content, or refuses to do business with the relevant speaker, it is held legally harmless. But if it fails to search, block, or stop doing business, it may be held contributorily or vicariously liable for the offending content.

Section 103 of SOPA offers an example of these techniques. Once informed by another private party that they were doing business with a targeted site, payment providers and advertisers would be held harmless if they stopped doing business with the site, even if the allegations were never proved in court.[118] An earlier version of this legislation, COICA, was even more forthright in encouraging the cooperation of private parties.[119] COICA required the attorney general to create a public blacklist of sites that, "upon information and reasonable belief, the Department of Justice determines are dedicated to infringing activities but for which the Attorney General has not filed an action under this section."[120] Once a site is placed on the attorney general's list, ISPs, payment system providers, do-

---

113 *See* ROBERT O'HARROW, JR., NO PLACE TO HIDE 2–4 (2005) (describing various data aggregator services available to law enforcement officials).

114 *See* Joshua Brustein, *Tech Giants, Like Telecoms, Have Been Sharing with the NSA*, BUSINESSWEEK (June 6, 2013), http://www.businessweek.com/articles/2013-06-06/tech-giants-like-telecoms-have-been-sharing-with-the-nsa, *archived at* http://perma.cc/FWF6-JLYS.

115 Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1.

116 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. §§ 1812, 1881, 1881a–1881g, 1885, 1885a–1885c (2006 & Supp. V 2011)).

117 *See id.* § 201, 122 Stat. 2436, 2468–70 (adding § 802, now codified at 50 U.S.C. § 1885a, to FISA).

118 Stop Online Piracy Act, H.R. 3261, 112th Cong. § 103 (2011).

119 *See* Benkler, *supra* note 111, at 160–61.

120 Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. § 2324(j)(1) (2010) (as referred to S. Comm. on the Judiciary, Sept. 20, 2010).

main name service providers, and advertising providers are immunized if they stop doing business with or deny service to the site.[121] The burden is then on the site to prove that it does not belong on the attorney general's list.[122] This ingenious system of private prior restraint achieves all of the cost- and burden-shifting effects of traditional prior restraint without the need for an official government licensing system or a judicial injunction. A subsequent version of COICA replaced the Justice Department blacklist with statutory authorization for private blacklists: "No domain name registry, domain name registrar, financial transaction provider, or service that provides advertisements to Internet sites shall be liable to any person on account of any action described in this subsection voluntarily taken if the entity reasonably believes the Internet site is dedicated to infringing activities . . . ."[123]

Section 5 of the PROTECT-IP Act similarly absolved payment system providers and advertisers from liability for voluntarily refusing to do business with "an Internet site if the entity acting in good faith and based on credible evidence has a reasonable belief that the Internet site is an Internet site dedicated to infringing activities."[124] The point of immunity provisions like these is to encourage the creation of industry blacklists; even if the blacklist contains incorrect information, there is no legal liability for creating and acting on it.

(c) Soft Power. — Government actors can also encourage speech regulation informally.[125] We might understand these techniques as extralegal methods of collateral censorship. The most prominent recent example involves the U.S. government's attempts to shut down WikiLeaks without giving any direct orders or making any direct threats to private companies.[126] On November 28, 2010, WikiLeaks and its mass-media partners — which included well-known organizations like the *Guardian*, the *New York Times*, and *Der Spiegel* — began to release documents from a cache of approximately 250,000 classified cables sent between U.S. embassies around the world and the State Department.[127] Reaction by government

---

121 *See id.* § 2324(j)(2).

122 *See id.* § 2324(j)(3).

123 Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. § 2(e)(5)(B) (as reported by the S. Comm. on the Judiciary, Nov. 18, 2010).

124 Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. § 5(a) (as reported by the S. Comm. on the Judiciary, May 26, 2011).

125 *See* Derek E. Bambauer, *The New American Way of Censorship*, ARIZ. ATT'Y, Mar. 2013, at 32, 34, 36–37 (describing multiple tools of "soft censorship" that achieve their goals indirectly or through influence over other actors). Bambauer defines "soft censorship" somewhat more broadly than what I am calling "soft power": it includes "employing unrelated laws as a pretext to block material, paying for filtered access, or persuading intermediaries to restrict content." Bambauer, *supra* note 8, at 867.

126 *See* Bambauer, *supra* note 8, at 891–93 (describing the multipronged campaign to apply pressure to WikiLeaks); Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 330–51 (2011) (same).

127 Benkler, *supra* note 126, at 326.

officials and politicians was swift, and directed primarily at WikiLeaks rather than at its traditional media partners. Although the *New York Times* was a copublisher of the cables, Vice President Joseph Biden argued that WikiLeaks's founder, Julian Assange, was "closer to being a hi-tech terrorist than the Pentagon Papers";[128] Secretary of State Hillary Clinton called the release of the diplomatic cables "an attack on the international community."[129]

On November 27, 2010, the day before the publication of the cables began, State Department Legal Adviser Harold Koh wrote a cleverly drafted letter to WikiLeaks that was circulated to the public.[130] It did not directly claim that WikiLeaks had broken the law or would break the law by publishing the cables, or that WikiLeaks's and its partners' operations were constitutionally unprotected.[131] Instead, the letter asserted that the materials "were provided in violation of U.S. law," without specifying who had broken the law.[132] The letter argued that "[a]s long as WikiLeaks holds such material, the violation of the law is ongoing," and noted "that WikiLeaks also has provided approximately 250,000 documents to [the *New York Times*, the *Guardian*, and *Der Speigel*] for publication, furthering the illegal dissemination of classified documents."[133] Thus, while not directly asserting that WikiLeaks had itself broken the law (which would also implicate the *Times*), the State Department "correctly asserted that the law had been broken (by someone), insinuating that WikiLeaks was the offending party."[134]

On December 1, Senator Joseph Lieberman, Chairman of the Senate Homeland Security Committee, called for companies to stop doing business with WikiLeaks.[135] His office privately contacted Amazon.com — which hosted WikiLeaks on its servers — to ask about its associations with WikiLeaks.[136]

---

128 *Julian Assange Like a Hi-Tech Terrorist, Says Joe Biden*, THE GUARDIAN (Dec. 19, 2010, 1:20 PM), http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden, *archived at* http://perma.cc/56HV-MKF7.

129 Glenn Kessler, *Clinton, in Kazakhstan for Summit, Will Face Leaders Unhappy over WikiLeaks Cables*, WASH. POST (Nov. 30, 2010, 8:44 AM), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/30/AR2010113001095.html, *archived at* http://perma.cc/4VUE-6KJ7.

130 Letter from Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, to Jennifer Robinson, Attorney for Julian Assange (Nov. 27, 2010), *archived at* http://perma.cc/653P-2LZF.

131 *See id.*

132 *Id.*

133 *Id.*

134 Benkler, *supra* note 111, at 156.

135 Charles Arthur, *WikiLeaks Under Attack: The Definitive Timeline*, THE GUARDIAN (Jan. 8, 2010, 11:39 AM), http://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline, *archived at* http://perma.cc/E6B2-XHSY.

136 Rachel Slajda, *How Lieberman Got Amazon to Drop Wikileaks*, TALKING POINTS MEMO (Dec. 1, 2010, 9:56 PM), http://talkingpointsmemo.com/muckraker/how-lieberman-got-amazon-to-drop-wikileaks, *archived at* http://perma.cc/YV55-JCQS.

Following the State Department's public letter and Senator Lieberman's public call, various parts of the digital infrastructure began denying service to WikiLeaks. Amazon promptly removed WikiLeaks from its servers.[137] EveryDNS, the domain registrar that served the WikiLeaks domain, stopped pointing WikiLeaks.org to WikiLeaks's servers.[138] Relying on the State Department's letter, PayPal discontinued handling payments for WikiLeaks.[139] Visa, MasterCard, and Bank of America soon joined in.[140] Later that month, Apple, which controls the applications that can be loaded on iPads and iPhones, removed a third-party application from its App Store which "allow[ed] iPhone users to access and search WikiLeaks embassy cables."[141] Although WikiLeaks was able to find a substitute for server hosting and storage and a Swiss domain name, the loss of payment services damaged its ability to continue operations.[142]

The WikiLeaks episode shows how the government can leverage private control of the infrastructure of free expression without making any threats, overt or veiled, simply by encouraging the private actors who control the digital infrastructure to shut down offending speakers.[143] WikiLeaks's position was hardly different from that of the *New York Times* in *Pentagon Papers*: it received a large volume of materials from a source and published them to the world. Yet it was surprisingly easy for American officials to use the soft power of public statements and a few well-placed inquiries to persuade the private enterprises that control the digital infrastructure of expression to stop doing business with WikiLeaks. In part that is because most businesses dislike bad publicity and prefer to be thought of as good corporate citizens. They prefer a quiet life in which they can make profits and serve the vast majority of their customers without undue government interference. In part it is because WikiLeaks, unlike its traditional media partners, was largely an unknown entity whose reputation was easily besmirched and was easily portrayed as a criminal or terrorist organization. Notably, the Obama Administration and Senator Lieberman did not try the same strategy against the *New York Times*, much less *Der Spiegel* or the *Guardian*. Had they publicly encouraged Visa, MasterCard, and Amazon to stop doing business with the *New York Times*, this would have seemed like a gross interference with freedom of the press and a new form of digital McCarthyism.

---

137 Benkler, *supra* note 126, at 339–40.

138 *Id.* at 340.

139 *Id.* at 341.

140 *Id.* at 341–42.

141 Benkler, *supra* note 111, at 157.

142 *Id.* at 157–58.

143 *See* Bambauer, *supra* note 8, at 894–99 (describing multiple techniques by which governments convince, persuade, or cajole infrastructure companies to restrict speech).

III. PRIOR RESTRAINT IN AID OF DIGITAL SURVEILLANCE: NATIONAL SECURITY LETTERS

A full discussion of the ways that surveillance affects freedom of expression and association is beyond the scope of this Essay.[144] Here I am interested in a more specific question: how the ever-increasing demand for digital surveillance leads governments to target the infrastructure of free expression.

The digital age leads not only to the democratization of communication and content production, but also to pervasive digital surveillance, and to the expansion of state capacities for surveillance that I have elsewhere called the National Surveillance State.[145] But in order to engage in surveillance, the government needs access to the facilities through which most people are speaking; hence the government needs access to the infrastructure of free expression, which is largely held in private hands. Thus, a consequence of the governance demands of the National Surveillance State is the need to coerce or co-opt the private owners of the infrastructure of free expression to assist the government's surveillance operations. Such cooperation is not new. In the predigital era, telecommunications companies sometimes assisted the government's surveillance efforts.[146] But because the demands for and the possibilities of surveillance have grown exponentially, and because so much speech in the digital era operates through privately owned digital networks, services, and platforms, digital surveillance requires considerable amounts of public/private cooperation.

The need for cooperation, in turn, requires that private companies not reveal the nature and extent of their cooperation. Often owners of private infrastructure cannot reveal the extent of government surveillance without tipping off potential targets and making surveillance futile. Hence government digital surveillance programs inevitably lead to prior restraints on owners of private infrastructure or techniques that operate in much the same way as prior restraints. The flip side of pervasive digital surveillance is pervasive practices of prior restraint.

---

144 *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

145 *See* Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006).

146 For example, through Project SHAMROCK, telegraph companies provided the NSA with "copies of most international telegrams leaving the United States between August 1945 and May 1975." S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK III: SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 765 (1976); *see also* L. Britt Snider, *Unlucky SHAMROCK: Recollections from the Church Committee's Investigation of NSA*, STUD. INTELLIGENCE, Winter 1999–2000, at 43, *archived at* http://perma.cc/VTN9-JVVJ.

A good example of how digital surveillance necessitates wide ranging use of prior restraint is the government's practice of issuing national security letters (NSLs). The use of NSLs greatly increased with the USA Patriot Act in 2001, which allowed many different government authorities to use them in any investigation related to terrorism or foreign intelligence.

NSLs have two central features. First, they can be issued by executive officials without a judicial warrant or a hearing.[147] Second, NSLs normally come with a gag order.[148] The recipient may not reveal the contents of the NSL or the fact that it exists, and recipients are subject to the gag order until the government releases them, which it may never do.[149] Before the 2006 reauthorization of the Patriot Act, it was not possible to challenge an NSL in court and request the lifting of a gag order.[150] In the Patriot Act reauthorization, Congress added limited judicial review of NSLs.[151] Although these changes offer the theoretical possibility of a remedy, they

---

147 *See* 18 U.S.C. § 2709(b) (2012) (authorizing the Director of the FBI and other officials to request specified information about a subscriber from an electronic communication service provider); *id.* § 2709(a) (imposing duty on electronic communication service providers to comply with national security letters).

148 A recipient may not disclose the fact or the contents of the NSL or the accompanying gag order to anyone (except an attorney representing the recipient) if a senior FBI official certifies that "otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." *Id.* § 2709(c)(1). The government has estimated that approximately 97 percent of NSLs come with a gag order. *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013).

149 18 U.S.C. § 2709(c)(1). The government also uses gag orders when it requires telecommunications companies to provide bulk telephone metadata under section 215 of the Patriot Act. *See* 50 U.S.C. § 1861(c)(2)(E) (2006 & Supp. V 2011); *id.* § 1861(d)(1). Section 215 orders are obtained from the Foreign Intelligence Surveillance Court or a designated U.S. Magistrate in ex parte proceedings. *Id.* § 1861(b)(1). Section 215 nondisclosure orders may only be challenged a year after they are issued. *See id.* § 1861(f)(2)(A)(i).

Nondisclosure orders are also issued under section 702 of the Foreign Intelligence Surveillance Act. *See* 50 U.S.C. § 1881a(h)(1)(A) (2006 & Supp. V 2011) (authorizing order by attorney general); *id.* § 1881b(c)(5)(b) (authorizing court nondisclosure order in cases involving United States persons overseas). A telecommunications company may challenge an order under § 1881a as soon as it is received. *Id.* § 1881a(h)(4)(A).

The following discussion focuses on NSLs because they present the most troublesome situation for freedom of expression. Unlike section 215 and section 702 orders, NSL nondisclosure orders are imposed without any prior judicial hearing. Nevertheless, many of the same difficulties apply to section 215 and section 702 nondisclosure orders because they are issued ex parte, without notice, and in the case of section 215 orders, without a prompt opportunity for judicial reconsideration in an adversarial hearing.

150 *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 115, 116(a), 120 Stat. 192, 211–14 (2006), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 4(b), 120 Stat. 278, 280 (2006) (codified at 18 U.S.C. § 3511 (2012)); John Doe, Inc. v. Mukasey, 549 F.3d 861, 867–68 (2d Cir. 2008) (describing the addition of § 3511).

151 18 U.S.C. § 3511(b) (2012).

were deliberately designed to make it very difficult to lift gag orders without the government's consent.[152]

NSLs are powerful examples of the merger of the infrastructure of surveillance with the infrastructure of free expression. The government, which does not own the infrastructure of free expression, needs to coerce or co-opt private owners to assist in its surveillance. It must also ensure that private businesses do not disclose the government's activities or even the fact that they have received an order that compels their participation. In the words of an anonymous recipient of an NSL, the state conscripts recipients into being "secret informer[s] for the government."[153]

Gag rules not only prevent owners of private infrastructure from tipping off targets of surveillance; they also help ensure that the public is not aware of the scope and extent of government surveillance. This feature allows NSLs to serve as a pervasive background feature of digital communications without raising public alarm. In fact, one of the most important effects of the Patriot Act expansion was that it allowed NSLs to become routine features of government investigation. As digital surveillance becomes bureaucratically normal and proliferates, it becomes increasingly difficult to offer individualized determinations and significant procedural protections.

Aiming surveillance at owners of infrastructure rather than identified persons of interest meshes with the bureaucratic, routinized character of surveillance in the National Surveillance State. The recipients of many, if not most, national security letters are large businesses. They may have little reason to challenge NSLs and gag orders, first, because they want smooth relations with the government, and second, because they probably do not want their customers to know the degree of their cooperation (com-

---

[152] 18 U.S.C. § 3511(b)(2) creates a heavy presumption in favor of retaining a gag order, and makes it very easy for the government to require courts to keep the order in place. It permits a court to "modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." However, if a high-ranking government official (for example, an agency head, the deputy attorney general, or the director of the Federal Bureau of Investigation) "certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive unless the court finds that the certification was made in bad faith." *Id.*

Similarly, 18 U.S.C. § 3511(b)(3) greatly limits the ability of gag order recipients to get old orders modified or removed. If the court denies a petition to remove a gag order, the recipient must wait a year before he or she can once again ask that it be modified or lifted. The effect is to keep gag orders in place indefinitely, or as long as the government wants.

[153] *See* Anonymous, *My National Security Letter Gag Order*, WASH. POST (Mar. 23, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html, *archived at* http://perma.cc/JA9J-UY4Y.

pelled or not) with government surveillance.[154] Indeed, one effect of the Snowden revelations was to expose the possibility that large companies like Verizon, Google, Facebook, and others were actively assisting the government's surveillance efforts in a variety of different contexts. This was bad publicity for most of these companies — especially those with large customer bases outside the United States.

NSL gag orders have all of the features of a classic administrative prior restraint. In some ways their effects are even more characteristic of a prior restraint than the judicial injunctions in *Near v. Minnesota* and *Pentagon Papers*.

First, the secrecy of NSLs encourages overbreadth of coverage, both for the scope of the surveillance and for the length of the gag order. The executive branch is the judge of the scope and the necessity of the NSL and the length of the gag order.

Second, NSL gag orders powerfully shift the burden of action and inertia. The NSL's existence may not be revealed until the government permits it. The government has few incentives to remove the gag order, even and especially if the NSL turns out to be completely unnecessary, illegal, or in violation of the government's own internal investigative rules. The government has few reasons to air its dirty laundry in public. Even after the 2006 amendments, there is only a very limited judicial remedy to remove an NSL gag order.[155] Moreover, NSL recipients who fail to persuade a court to lift the gag order must wait a full year before they can try again.[156]

Third, the NSLs are issued by executive officials with no judicial or constitutional protections for the recipients before the gag order is issued. Executive officials decide whether to issue the NSL based on investigative priorities, not First Amendment concerns, and they are subject only to very limited judicial review. The only limit on NSLs is that they cannot be issued *exclusively* for the purpose of investigating conduct protected by the First Amendment; the law merely requires the government to assert an additional purpose for the investigation.[157]

Fourth, the use of gag orders ensures that the vast system of NSLs currently in operation is invisible to the public. Tens of thousands of NSLs are issued secretly every year,[158] and those who know the most about the

---

154 *See id.* ("[T]he inspector general's report suggests that large telecom companies have been all too willing to share sensitive data with the agency — in at least one case, a telecom company gave the FBI even more information than it asked for.").

155 *See supra* note 152.

156 18 U.S.C. § 3511(b)(3).

157 *See* 18 U.S.C. § 2709(b)(1) (2012) (allowing the FBI Director to request information "provided that such an investigation of a United States person is not conducted *solely* on the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States") (emphasis added).

158 *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 120–21 (2007), *archived at*

practice and its consequences are forbidden to speak about it. A 2007 op-ed by an anonymous recipient[159] of an NSL starkly presented the effects of enforced secrecy:

> Living under the gag order has been stressful and surreal. Under the threat of criminal prosecution, I must hide all aspects of my involvement in the case — including the mere fact that I received an NSL — from my colleagues, my family and my friends. When I meet with my attorneys I cannot tell my girlfriend where I am going or where I have been. I hide any papers related to the case in a place where she will not look. When clients and friends ask me whether I am the one challenging the constitutionality of the NSL statute, I have no choice but to look them in the eye and lie.[160]

Fifth, the gag order creates incentives for overcensorship and abuse. As noted previously, the government has few incentives to remove a gag order, especially if the NSL was unnecessary, abusive, illegal, or in violation of its own internal rules. The inspector general's report suggests that there have been multiple cases of abuse,[161] which the system of secrecy does nothing to discourage.

Sixth, the recipient of an NSL has been singled out and identified by the government. If the recipient discloses the existence of the NSL, much less its contents, the recipient is very likely to be prosecuted because the government's authority has been directly challenged. The government can hardly countenance widespread civil disobedience with respect to its surveillance activities. If an infrastructure company began to disclose that it regularly received NSLs, others might be emboldened and undermine a valuable source of information. The government therefore has every reason to make an example of anyone who would seek to undermine the system of secret NSLs.

To date only a few district courts and one circuit court have addressed the First Amendment issues raised by the gag orders.[162] In 2008, in *John*

---

http://perma.cc/MG9F-KMQZ [hereinafter INSPECTOR GENERAL'S REPORT ON NSLS] (noting that in 2005, more than 47,000 NSL requests were issued).

159 The anonymous recipient was later identified as Nicholas Merrill. *See* Ellen Nakashima, *Plaintiff Who Challenged FBI's National Security Letters Reveals Concerns*, WASH. POST (Aug. 10, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/09/AR2010080906252
.html, *archived at* http://perma.cc/9WX-LS26.

160 *My National Security Letter Gag Order*, *supra* note 153.

161 *See* INSPECTOR GENERAL'S REPORT ON NSLS, *supra* note 158, at 122–24*; see also* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, at 5 (2008), *archived at* http://perma.cc/A6GX-WM5D (finding that "the FBI had issued national security letters (NSL) for information about [redacted] after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation").

162 *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064 (N.D. Cal. 2013); Doe v. Gonzales (*Doe II*), 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *aff'd in part, rev'd in part, and remanded sub. nom.* John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008); Doe v. Gonzales (*Doe CT*), 386 F. Supp. 2d 66 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415 (2d Cir. 2006); Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated and remanded sub. nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

Doe, Inc. v. Mukasey,[163] the Second Circuit found several constitutional problems with the NSL system but ultimately refused to invalidate the entire system. Instead, it offered a series of potential saving constructions — some of which had only a tenuous relationship to the actual text of the statute — and remanded the case for further proceedings.[164]

NSLs exemplify the difficulties that judges face in dealing with new-school speech regulation. The Second Circuit noted that "the nondisclosure requirement is in some sense a prior restraint,"[165] and that it prevents public discussion of an important public question — the extent and abuse of secret government surveillance.[166] Nevertheless, the court was unwilling to apply Justice Stewart's *Pentagon Papers* test, which would ask whether disclosure of the NSL would "surely result in direct, immediate, and irreparable damage to our Nation or its people."[167] The government could not possibly prevail on that standard with respect to the tens of thousands of NSLs it delivers to companies every year. Even if the government attempted to meet the standard, the proof requirements alone would monopolize a significant share of the docket of the federal courts.

Nor did the Second Circuit apply the potentially less stringent standard of *Nebraska Press Ass'n v. Stuart*,[168] which struck down a pretrial gag order as a prior restraint. *Nebraska Press* would require at the very least that federal courts consider, on a case-by-case basis, any "alternative measures"[169] short of a prior restraint *before* a gag order could be issued, which the NSL nondisclosure rules would also not meet.

Instead, the Second Circuit asked whether the NSL gag order rules met the constitutional requirements of *Freedman v. Maryland*.[170] *Freedman* concerned constitutional limits on state censorship boards that block showing movies until they can be screened for obscenity. *Freedman* held that state boards must make a decision whether or not to ban as soon as possible, that they must promptly go to court to obtain an injunction supporting the ban, where they have the burden of proof to demonstrate that the mov-

---

163 549 F.3d 861. The panel was particularly distinguished: Judge Jon O. Newman wrote the opinion, joined by Judge Guido Calabresi and then-Judge (now Justice) Sonia Sotomayor.

164 *See id.* at 883–85.

165 *Id.* at 876.

166 *Id.* at 878 ("John Doe, Inc., has been restrained from publicly expressing a category of information, albeit a narrow one, and that information is relevant to intended criticism of a governmental activity.").

167 *Pentagon Papers*, 403 U.S. 713, 730 (1971) (Stewart, J., concurring). Justice Brennan's test, based on *Near v. Minnesota*, is similar. *See id.* at 726–27 (Brennan, J., concurring) (suppression permitted only under an "extremely narrow class of cases" involving the most extreme circumstances: "only governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order").

168 427 U.S. 539 (1976).

169 *Id.* at 565.

170 380 U.S. 51 (1965).

ie is unprotected, and that any restraint pending judicial review must be for a brief and specified period. Finally, there must be prompt judicial resolution.[171]

Invoking *Freedman* meant that the Second Circuit was deliberately lowering the bar for judicial scrutiny.[172] *Freedman* concerned licensing schemes for material that is either low-value speech or completely unprotected by the First Amendment.[173] As Justice Brennan explained in *Pentagon Papers*, it should not apply where "the material sought to be suppressed is within the protection of the First Amendment [and] the only question is whether, notwithstanding that fact, its publication may be enjoined for a time because of the presence of an overwhelming national interest."[174]

Ultimately, the Second Circuit did not even require that NSL gag orders meet the *Freedman* standard. The government would have failed that test as well because the government could not possibly have gone immediately before a judge with respect to each of the thousands of NSL gag orders it has issued; and it could not have promptly obtained a determination on the merits that secured full constitutional procedural protections for the Internet service provider.

The government's defense laid bare the reality of digital prior restraints in the National Surveillance State. First, the government explained that it "would be unduly burdened if it had to initiate a lawsuit to enforce the nondisclosure requirement in the more than 40,000 NSL requests that were issued in 2005 alone."[175] In other words, the government pointed out that a central feature of post–Patriot Act National Security Letters is that they are a scheme of routinized, administrative, and bureaucratic surveillance. They are not easily susceptible to individualized judicial review associated with old-school (predigital) methods of surveillance and speech regulation. *Freedman* was designed to deal with the relatively small number of movies produced yearly, and not with a bureaucratic system that generates tens of thousands of surveillance requests in a year. Applying even the *Freedman* standards would mean that the system of surveillance plus gag orders would have to be shut down or drastically curtailed.

Second, the government argued that it should not have to bear the burden of obtaining judicial review for each gag order because "there is no reason to believe that most recipients of NSLs wish to disclose that fact to

---

171 *See id.* at 58–60; *accord* Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 560 (1975).

172 In fact, given the nature and extent of the government's demands for surveillance, the members of the Second Circuit panel could not agree on whether strict scrutiny applied; instead, the panel argued that the result would be the same regardless of the level of scrutiny. John Doe, Inc. v. Mukasey, 549 F.3d 861, 878 (2d Cir. 2008).

173 *Pentagon Papers*, 403 U.S. 713, 726 n.* (1971) (Brennan, J., concurring).

174 *Id.*

175 *Mukasey*, 549 F.3d at 879.

anyone."[176] The reason, as noted earlier, is that the vast majority of NSLs are issued to a relatively small number of large owners of private infrastructure with customers around the world who have no desire to call attention to the degree of their cooperation with American digital surveillance practices.[177] Statements by the U.S. government that only foreigners are being targeted would be cold comfort to their overseas customers. Perhaps a few entrepreneuers with strong ideological objections to government surveillance — like Nicholas Merrill, who produced the *Doe* litigation — would have reason to raise a fuss, but they could be dealt with individually.

Accordingly, the Second Circuit upheld the system of NSL gag orders to the extent that the government would agree to abide informally by a "reciprocal notice procedure,"[178] which, however prudent, had no basis in the text of the statute.[179] The Second Circuit proposed that "[t]he Government could inform each NSL recipient that it should give the Government prompt notice, perhaps within ten days, in the event that the recipient wishes to contest the nondisclosure requirement."[180] Once it received the notice, "the Government could be accorded a limited time, perhaps 30 days, to initiate a judicial review proceeding to maintain the nondisclosure requirement, and the proceeding would have to be concluded within a prescribed time, perhaps 60 days."[181] The effect would be to "nearly eliminate the Government's burden to initiate litigation (with a corresponding minimal burden on NSL recipients to defend numerous lawsuits)."[182] Even if the Second Circuit's reciprocal notice proposal were consistent

---

176 *Id.* (quoting Brief for the Defendants-Appellants at 33, *Mukasey*, 549 F.3d 861 (No. 07-4943-cv), 2008 WL 6082598) (internal quotation marks omitted).

177 *See id.* at 880 ("The typical NSL recipient, . . . who runs a business that is in no sense dependent on revealing the receipt of an NSL, has little if any incentive to initiate a court challenge in order to speak publicly about such receipt.").

178 *Id.* at 879 (internal quotation marks omitted).

179 *Id.* at 883 (noting that although it would be "beyond the authority of a court to 'interpret' or 'revise' the NSL statutes to create the constitutionally required obligation of the Government to initiate judicial review of a nondisclosure requirement[,] . . . the Government might be able to assume such an obligation without additional legislation").

180 *Id.* at 879.

181 *Id.*

182 *Id.* In addition, the Second Circuit construed subsections 3511(b)(2) and (b)(3) to place the burden on the government to show a good reason that disclosure of the receipt of an NSL will risk a harm related to national security. *Id.* at 883. It also held that subsections 2709(c) and 3511(b) were "unconstitutional to the extent that they impose a nondisclosure requirement without placing on the Government the burden of initiating judicial review," *id.*, and that subsections 3511(b)(2) and (b)(3) "are unconstitutional to the extent that . . . a governmental official's certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is treated as conclusive." *Id.*

with *Freedman*, however, the government has not yet issued internal rules that would require it to abide by that proposal.[183]

Although the Second Circuit recognized that "the nondisclosure requirement is in some sense a prior restraint,"[184] it did not view it as a "typical"[185] prior restraint: "it is not a restraint imposed on those who customarily wish to exercise rights of free expression, such as speakers in public fora, distributors of literature, or exhibitors of movies."[186] It viewed the paradigm case as *Pentagon Papers* — in which the government tried to prevent the *New York Times* from publishing information about government operations that the *Times* believed the public had the right to know.[187]

This explanation overlooks three important features of new-school speech regulation. First, in the digital age, the government may be less likely to target individual speakers or members of the institutional press like the *New York Times*. That is because targeting individual speakers

---

[183] *See In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1070–72 (N.D. Cal. 2013) (noting that although the government stated that it would comply with the reciprocal notice procedure, it had not issued rules to that effect, and holding the NSL provisions unconstitutional on the ground that, on their face, they do not comply with *Freedman* and are not amenable to saving constructions). In its brief before the Ninth Circuit in *In re National Security Letter*, the government asserted that "[s]ince 2009, the FBI has complied with the *Doe* injunction and has implemented *Doe*'s 'reciprocal notice' procedures nationwide." Government's Opening Brief, *In re* Nat'l Sec. Letter, Nos. 13-15957 & 13-16731 (9th Cir. Jan. 17, 2014), *archived at* http://perma.cc/ZYM6-6XDV.

In addition to the Second Circuit's proposal, The President's Review Group on Intelligence and Communications Technologies has recommended that NSLs be issued only after a judicial finding, except in cases of emergency. RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 26–27, 93–94, 122–23 (2013), *archived at* http://perma.cc/R65B-VCUL. These recommendations, if followed, would likely reduce the number of NSLs issued, but the proceedings would still be ex parte. In order to comply with even the *Freedman* standards there would still have to be prompt judicial resolution that was not ex parte. Moreover, under the Review Group's recommendations, the burden is still on the recipient to contest the order after it has been issued. *See id.* at 27 ("[N]ondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality."). However, the recommendations would require the government to obtain reapproval of a gag order every 180 days. *Id.*

> The Review Group has also recommended legislation that would allow recipients of gag orders to publicly disclose on a periodic basis general information about the number of . . . orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Id. at 123. This ameliorates, but does not entirely solve, the prior restraint problem.

[184] *Mukasey*, 549 F.3d at 876.

[185] *Id.*

[186] *Id.* The court added that the nondisclosure provision was also a not a "typical content-based restriction[]" even though "the nondisclosure requirement is triggered by the content of a category of information . . . the fact of receipt of an NSL and some related details." *Id.*

[187] *See id.* at 882 (citing *Pentagon Papers*, 403 U.S. 713 (1971)).

may be difficult, inefficient, and unavailing. Speakers may be anonymous or overseas, or they may be able to publish so quickly that a prior restraint is futile. Instead, the government is now far more likely to target the owners of private infrastructure because it needs their cooperation to engage in surveillance. As we saw in the case of SOPA, the government seeks to co-opt private infrastructure to do the government's work. In the digital age, this may be the major function of prior restraint.

Second, some secret NSL orders may be directed at the institutional press, because they seek contact information between reporters and their sources. Instead of trying to enjoin the *New York Times*, the government may issue an NSL that seeks to find out who the *Times* is talking to, for how long, and on what occasions. Recently, the Justice Department obtained two months of contact records of phone numbers belonging to the Associated Press, presumably to further a leak investigation.[188] Revelation of the Justice Department's actions resulted in a public outcry and a significant debate over government investigative practices, leading the Justice Department to reform its internal procedures for making such requests.[189] The information only came out because the Justice Department used a grand jury subpoena; according to its internal rules, such a request must be made public within 90 days.[190] If the government had employed a national security letter, however, the request for phone records would likely still be secret.[191]

Third, and perhaps most important, owners of private infrastructure are "the press" in the twenty-first century. The "press" in the Press Clause refers both to journalistic institutions and to technologies used to disseminate information.[192] During the colonial period many owners of presses printed not only their own speech but also the speech of their customers.[193] When

---

[188] *See* Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, ASSOCIATED PRESS (May 13, 2013, 10:53 PM), http://bigstory.ap.org/article/govt-obtains-wide-ap-phone-records-probe, *archived at* http://perma.cc/Y65X-YEZ8.

[189] Scott Neuman, *Justice Tightens Guidelines for Obtaining Records from Media*, NPR (July 12, 2013, 4:59 PM), http://www.npr.org/blogs/thetwo-way/2013/07/12/201566829/justice-tightens-guidelines-for-obtaining-records-from-media, *archived at* http://perma.cc/5CZF-J9KS.

[190] *See* 28 C.F.R. § 50.10(g)(3) (2013) (Justice Department Guidelines) ("When the telephone toll records of a member of the news media have been subpoenaed without . . . notice . . . notification shall occur within 45 days of any return made pursuant to the subpoena, except that the responsible Assistant Attorney General may authorize delay of notification for no more than an additional 45 days.").

[191] *See* Philip Bump, *The Justice Department Secretly Seized AP Phone Records — on a Terror Leak?*, THE WIRE (May 13, 2013, 5:00 PM), http://www.theatlanticwire.com/politics/2013/05/justice-department-ap-phone-records/65184/, *archived at* http://perma.cc/AWT-92K3.

[192] *See* sources cited *supra* note 18.

[193] MERRILL JENSEN, THE NEW NATION: A HISTORY OF THE UNITED STATES DURING THE CONFEDERATION, 1781–89, at 430 (1950) ("[M]ost newspaper publishers believed that it was a part of their public duty to print materials on all sides of a question, even when they were counter to a particular publisher's own views."); David A. Anderson, *The Origins of the Press Clause*, 30 UCLA L. REV. 455, 466 (1983) (noting that many colonial newspapers, in addition to printing partisan material, "also served as forums for public debate").

the government aims at ISPs, broadband providers, and similar providers of digital infrastructure, it is aiming at the modern-day equivalent of "the press" in the technological sense.[194]

If one inspected only the black-letter law of the First Amendment, one would learn that prior restraints are extraordinary, legally disfavored, and must last the shortest possible time.[195] In the National Surveillance State, by contrast, prior restraints on infrastructure companies are widespread, enjoy favored legal treatment, and potentially last forever. The prior restraint requested by the government in *Pentagon Papers* seemed extraordinary and riveted national attention. The prior restraints characteristic of the National Surveillance State are perfectly ordinary and have gained very little attention; they are as ubiquitous as they are invisible.

IV. CONCLUSION: THE GOALS OF NEW-SCHOOL SPEECH REGULATION

A. Old-School Goals: Chilling Effects and Ex Post Punishment

The goals and practices of old-school speech regulation have been shaped by the possibilities of enforcement in the predigital era or using predigital technologies. Old-school regulation tries to control bodies, spaces, and predigital technologies of mass distribution. Before publication moved to digital networks, it was relatively difficult for the state to block prohibited activity before it happened; therefore much old-school speech regulation is ex post — criminal prosecutions, civil fines, or seizure and destruction of books and other materials. For example, *New York Times Co. v. Sullivan* involved defamation law, which is ex post regulation.

In the old-school model, ex ante prevention of speech is certainly not impossible, but the opportunities are more circumscribed than in new-school speech regulation. These are, roughly speaking, situations in which effective prior restraints are possible in a predigital world. First, the state can block disfavored activities before they happen when the state can plausibly and effectively impose a licensing scheme on publishing or broadcasting technologies, or control access to government property. Second, the state can prevent disfavored speech when it is able to learn that speech is about to occur *and* it can act in time to stop it through a judicial injunction. *Pentagon Papers* involved the latter situation.

---

194 Lee, *supra* note 18.

195 *See* Neb. Press Ass'n v. Stuart, 427 U.S. 539, 562 (1976) ("[A] prior restraint on publication [is] one of the most extraordinary remedies known to our jurisprudence."); *Pentagon Papers*, 403 U.S. 713, 714 (1971) (per curiam) ("Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) (internal quotation marks omitted))); Freedman v. Maryland, 380 U.S. 51, 59 (1965) ("Any restraint imposed in advance of a final judicial determination on the merits must similarly be limited to preservation of the status quo for the shortest fixed period compatible with sound judicial resolution.").

Beyond these two situations, the state usually cannot stop speech before it occurs, and therefore old-school speech regulation often relies on deterrence. The state hopes to prevent undesirable expression by giving people reason to fear the consequences of acting. To this end, the state may pass regulations that are overbroad and vague in order to discourage expressive conduct that the state wishes to prevent. Although the state may not want to capture protected expression, it wants to make sure that all unprotected activity is deterred. From the perspective of regulation (as opposed to civil liberties protection), uncertainty about whether one's conduct is illegal may be a virtue, not a vice.

Modern First Amendment doctrine's focus on chilling effects is simply the flip side of what old-school speech regulation seeks to achieve. Old-school speech regulation *wants* to induce a chilling effect on speech that the state hopes to control. It is also helpful if the state's threats of retribution or punishment for disfavored speech are either highly visible or widely recognized by the public. Similarly, it may also be helpful if surveillance of expressive activity is public or if the possibility of surveillance is highly salient to the public. Even if the public never sees a policeman taking names at a demonstration or sees a person arrested for illegal speech, it is enough that the citizens know that such practices are real. The point of old-school speech regulation is to dissuade and discourage, and thus to produce fear, apprehension, pessimism, or docility.

B. New-School Goals: Pervasiveness, Low Salience, and Ex Ante Prevention — From Chilling Effects to Chilling Out

In a digital world, the state's practices and techniques have a different emphasis. New-school speech regulation offers additional possibilities — and more effective possibilities — for ex ante prevention than old-school speech regulation did. Because the infrastructure of free expression merges with the technologies of regulation and surveillance, the state is better able to discover when disfavored speech is occurring. It may also be easier to block speech, either directly or by inducing private parties to engage in surveillance and collateral censorship. The state can give incentives for private parties to search for disfavored content, slow it down, filter it, or block it entirely.

To be sure, old-school speech regulation does not go away. Even in new-school speech regulation, the government may want to chill activity to protect property rights and surveillance capability. The boundaries of copyright law and the defense of fair use are often quite vague, and hence their combination may chill protected expression. As noted previously, gag orders that accompany national security letters are designed to produce an *in terrorem* effect so that no business will attempt disclosure.

Nevertheless, because digital networks make both surveillance and prevention easier, new-school speech regulation makes greater use of ex ante strategies, including blocking and filtering. Thus, roughly speaking, while

old-school speech regulation emphasizes deterrence and chilling effects, new-school speech regulation emphasizes prevention and low salience (or invisibility).

As surveillance and blocking of harmful content become increasingly effective and pervasive, the old-school approach of generating chilling effects becomes more complicated. Strategies of governance change as we move from a world in which only (or primarily) suspicious people are targeted for surveillance to a world in which government and private business collect data on as many people as possible to facilitate analysis, prevention, and countermeasures.

The state and private infrastructure owners may prefer that surveillance be largely invisible to the general public. The scope and extent of data collection and analysis should be secret or, at the very least, of very low salience in order to make people feel that, although they are secure, they are not constantly being observed. When surveillance is not salient to people, they may be more willing to reveal information that the government or owners of private infrastructure can then collect and analyze. That is especially important because data collected about perfectly innocent people may help the state identify, understand, apprehend, or block the actions of those the state suspects. To the extent that the public is aware of pervasive surveillance, both the government and private business may want the public not to see it as a threat that is designed to induce obedience and docility; instead, government and private business may want to depict data collection operations as normal, unobtrusive, and inoffensive. In the National Surveillance State, the experience of surveillance, once reserved for "suspicious" persons, is democratized, universalized, and made banal. In a world of pervasive surveillance, the state and owners of private infrastructure may not want to achieve chilling effects with respect to most people; instead, they may want most people just to chill out.

In sum, the goal of new-school speech regulation is normalcy and invisibility — or at least low salience — employing actions that prevent rather than merely punish, and that can occur automatically and at a distance. The irony of the democratization of speech in the digital age is precisely that it has led to these practices of control and surveillance. To vary another famous saying, on the Internet, nobody knows you are a dog — except for the government and the owners of private infrastructure.

New York Times Co. v. Sullivan and *Pentagon Papers* are twentieth-century responses to twentieth-century techniques of speech regulation. Yet techniques of speech regulation have not stood still; nor have the technologies that facilitate them. Just as defenders of free expression during the post–New Deal period had to devise ways of constructing constitutional guarantees that would respond to old-school techniques, it falls to current generations to reimagine the free speech principle in a world of new-school speech regulation. The commitment to freedom of speech may be enduring, but the techniques of speech regulation are protean and ever-changing. So too must be our responses.