Between Truth and Power (New York: Oxford Univ. Press, 2019)

Chapter 4
Open Networks and Closed Circuits

"Sovereign is he who decides on the exception."
– Carl Schmitt, *Political Theology*

Platforms are not the only powerful entities with interests in shaping flows of information, and logics of intermediation are not the only kinds of logics that networked digital information infrastructures enable. Such infrastructures also offer new possibilities for interrupting and blocking information flows, and those capabilities can be deployed to serve a variety of interests. In particular, both nation states and digital content providers have sought to impose interdiction obligations on network intermediaries—and network intermediaries have responded to those efforts in ways that leverage and solidify their own operational authority.

This chapter considers the extent to which efforts to optimize networked digital information infrastructures for interdiction and control have begun to coalesce into more definite patterns. One organizing theme for that inquiry is the idea of the exception in political theory. The idea of the exception originates in the tradition of emergency authority. For millennia, legal theorists have reasoned that in true emergencies, including most notably in wartime, the state has some leeway to suspend operation of the ordinary rules and procedures that characterize the rule of law. For twentieth-century political theorist Carl Schmitt, whose theories became key pillars of the National Socialist regime in 1930s Germany, that tradition pointed to an insight about the nature of sovereignty more generally. Schmitt reasoned that because it is the emergency—the state of exception—that legitimates the exercise of absolute power, true sovereignty consists in the power to say when the exception exists.[1] That conclusion profoundly challenged the liberal tradition in political theory, which conceives sovereignty in terms of consent, ordered liberty, and fidelity to the rule of law.

Nominally, the post-war constitutional order has rejected Schmittian theorizing about sovereign power in favor of renewed commitments to constitutionalism and legal process.[2] And yet matters are not quite so simple. The state of exception may be integrated into the legal and political fabric in less obvious ways. As political theorist Giorgio Agamben argues, some actions are lawlike in form but not in substance; they manifest the bare force of law stripped of the features that give the rule of law legitimacy.[3] For some constitutional theorists, that argument resonates especially well with the narratives about security and control that have emerged in the context of the post-9/11 "war on terror" and aptly describes the new kinds of authoritarian legal structures those narratives are invoked to justify.

In the networked, massively intermediated information environment, the themes of exception and bare force of law also take on a new kind of meaning. Sovereignty consists in the power to say what information will flow and what will not, and the party making that determination need not be a state sovereign at all. As emergent *logics of fiat interdiction* have encountered those of intermediation and legibility, powerful new platform entities have resisted the imposition of formal mandates, seeking arrangements that better serve their own interests. And so a second organizing theme for the discussion in this chapter is that of contest and compromise between competing authorities.

The chapter begins by identifying and exploring the logics that are claimed to justify fiat interdiction of particular kinds of networked information flows. It traces the intertwined development of three themes: threats to public safety, threats to information property, and threats to state authority. In each case, traditional narratives according enforcement imperatives some limited leeway have morphed into expansionist accounts of existential threat that are thought to justify correspondingly broad countermeasures. Those accounts are more than just a series of instrumentalist arguments for drawing legal lines differently. They are efforts to mobilize, cultivate and normalize systemic reflexes equating (some kinds of) uncontrolled information flow with danger and hard-coded control with safety. Next, the chapter traces the processes by which mechanisms for combating existential threats have begun to crystallize, producing effective lacunae within which absolute authority over information flow is both unaccountable and unquestioned.

Processes of contest and compromise between and among state actors, intellectual property owners, and platform intermediaries have unfolded in a variety of different settings and with varying amounts of publicity, transparency, and public participation. In terms of law on the books, those struggles have produced a still-shifting patchwork of regulatory obligations and political stalemates. In some contexts, the struggles among competing authorities to dictate the terms of the exception have produced institutional settlements that involve strong legal mandates. In particular, contests over intellectual property enforcement and state secrecy have produced versatile, expansionist templates for control of information flow. In other contexts, platform-based, algorithmically-mediated "self-regulation" has emerged as the path of least resistance. In tension with the logics of fiat interdiction—but in keeping with the logics of innovative and expressive immunity that Chapter 3 explored—dominant platforms enjoy increasing autonomy to determine for themselves how various enforcement imperatives are met. Meanwhile, logics of fiat interdiction have become progressively normalized within legal and policy discourses.

Logics of Fiat Interdiction

State actors have always sought to control information flows, and all states permit some such controls. For example, even in countries that traditionally have recognized broad protection for freedoms of speech and association, there is broad consensus that neither child pornography nor step-by-step instructions for producing weapons-grade plutonium should circulate freely. Democratic, speech-regarding countries also have long-standing disagreements about other free speech exceptions. For example, U.S.

courts have interpreted the First Amendment as sheltering hate speech, but the post-World War II European constitutional order views hate speech as undermining protection for fundamental human rights and therefore unworthy of protection. In the United States, free speech doctrine sharply limits potential liability for defamation and publication of private facts; European countries with stronger traditions of legal protection for dignitary interests allow both tort theories broader scope. For the most part, however, until the dawn of the internet era, the areas of agreement and disagreement about the scope of free speech protection were well understood and relatively stable.

In mid-1990s, amid dawning realization that decentralized digital networks facilitated the uncontrolled and radically democratic spread of all kinds of information, long-stable areas of consensus about state control of information flows began to destabilize and shift. Traditionally authoritarian states such as China, Iran, and Saudi Arabia responded to networked digital communications infrastructures by mandating backbone-level filtering for certain kinds of undesirable content and by enlisting internet access and search providers to perform additional filtering and surveillance.[4] Other countries began to confront new kinds of disputes about prohibited information flow. In the United States, public fears about uncontrolled flows of dangerous information coalesced around a set of threats that tech pundits dubbed the "Four Horsemen of the Infocalypse": terrorism, drug dealers, pedophiles, and organized crime.[5] The Four Horsemen represented existential threats to the fabric of society and the rule of law: threats in response to which ordinary procedures might be suspended in favor of extraordinary measures. They were quickly joined by two more: large-scale, networked infringement of intellectual property rights that threatened powerful information-economy interests and large-scale, networked leaking and whistleblowing that threatened state secrecy. The articulation of those threats set the stage for a shift in the legal understanding of the relationship between speech and danger—and consequently for the emergence of new logics of interdiction justified by conditions of permanent emergency.

Dangerous Knowledge

Debates about the government's ability to prevent the spread of information that threatens public safety predate the internet era by many decades. The First Amendment doctrines that evolved over the course of the twentieth century, however, allowed the government to label speech "dangerous" and prohibit it on that ground only after showing a sufficiently direct connection to physical harm or the threat of harm. Rising fears about the uncontrolled, viral spread of existential threats have prompted steady erosion of that relatively bright line in favor of a standard that is both much more deferential to executive threat assessments and much more open-ended about the sorts of information that can qualify as threatening. The catalyst for that process of doctrinal erosion has been the idea of *culpable facilitation*. Activities that might seem speech-like are framed instead as taking on more material and culpable qualities by virtue of their connection to other activities seen as posing threats to public safety and security. Over time, the culpable facilitation construct has become both powerful and capacious.

An early dispute about the circumstances under which executable computer code could qualify as dangerous knowledge subject to government control illustrated the potential power of the idea of culpable facilitation as the basis for interdiction.

Executable code changes the behavior of digital networked systems to produce results. For many commentators, that capacity distinguished code from more traditional forms of expression and made the assertion of a regulatory interest only logical. During the Cold War, the State Department had adopted export control regulations covering not only munitions but also certain dual-use technologies, and had classified cryptographic techniques, without reservation, as covered technologies.[6] Within just a few decades, however, the personal computer revolution had put unprecedented processing power within general reach, and the internet had enabled widespread distribution of executable code and, eventually, encryption technologies suitable for widespread adoption to ensure communications privacy and security.[7] To those who worried about code's powerful functional capabilities, extension of the cryptography export controls into the modern era of widely distributed computer power seemed wise. Others, however, underscored code's dual-purpose and communicative aspects and worried about the potential for overbreadth and chill.

In the mid-1990s, litigants in a pair of cases challenged the application of federal export control regulations to restrict internet-based distribution of encryption technologies and won rulings acknowledging that human-readable source code is speech and that even machine-readable object code has an important expressive dimension.[8] Following the general rule established in other cases involving expressive conduct, both courts concluded that intermediate First Amendment scrutiny of the challenged regulations was appropriate. Generally speaking, that conclusion seems both inevitable and right given the close nexus between cryptographic code and confidential communication, and it proved sufficient to dispose of the underlying disputes. By any standard, the prohibition was not narrowly drawn. Rather than risk an adverse ruling on either the validity of the prohibition or the particular classification decisions that it had made, the government announced that it would amend the regulations in a way that excluded the source code at issue.[9] After the amendment, the disputes ended and the wider public controversy died away.

From a different perspective, though, that outcome shows the culpable facilitation construct beginning to function as an entering wedge for assertions of government need to control dangerous knowledge that were relatively open-ended. Rather than targeting implementations of code to destroy or penetrate critical systems, the cryptography export rules rested on a broad application of the idea of culpable facilitation: they targeted code that could be used to conceal communication. Identification of the proper standard for review of government regulations stopped several steps short of answering some rather important questions about how to craft and administer more well-balanced rules. The amended export-control regulations exclude over-the-counter, non-customizable implementations designed for installation by users but specify that, "when necessary," unspecified "details" must be made available to help determine whether those criteria are met. That phrasing is a recipe for government leverage without transparency or accountability. According to some reports, it is now routinely used to help ensure that communications providers afford desired levels of accessibility for government investigations.[10]

Consider now a less specialized and more open-ended set of prohibitions that repeats the same pattern of asserted existential threat, culpable facilitation rubric, and

discretionary enforcement. During the 1990s, after years of debate about the appropriate response to an upsurge in terrorist activity around the world, Congress first amended the immigration laws to exclude those who had provided material support to terrorist activities from entering the country and then enacted a new law criminalizing the knowing provision of material support for terrorism. The idea that provision of support might itself be criminally punishable was not new. Criminal prohibitions against aiding and abetting violators have existed for centuries, and a statute first enacted in 1790 forbids those owing a duty of loyalty to the United States—including both members of the military and other government officers and employees—from giving "aid and comfort" to its enemies.[11] The new law, however, appears to have been the first time that a prohibition specifically directed toward the idea of "aid and comfort" had been incorporated into the general criminal code, and the prohibition expanded on that eighteenth-century framing of the idea of culpable facilitation by listing a variety of covered activities, including financial services, training, provision of lethal substances, and transportation.[12] An exception allowed humanitarian assistance to those not directly involved in violent conduct, but two years later, in the aftermath of the 1995 bombing of the Oklahoma City federal building by domestic terrorists, Congress eliminated the humanitarian assistance provision and also extended the material support prohibition to encompass assistance to designated foreign terrorist organizations.

In *Holder v. Humanitarian Law Project*, a majority of the Supreme Court rejected a First Amendment challenge to the amended material support law.[13] The entity challenging the law had provided human rights advocacy training to certain Kurdish and Tamil dissident organizations designated as terrorist organizations by the State Department. Under the previous version of the ban, its activities would have been lawful; now, it feared prosecution. According to mid-twentieth century jurisprudence about speech and danger, which allowed punishment of speech only when sufficiently linked to direct threats of violence, *Humanitarian Law Project* should have presented an easy case for invalidation.[14] But both the world and narratives about the threats it presented had begun to change rapidly.

The statute challenged in *Humanitarian Law Project* did not single out computer code or computer-based training as especially dangerous, but it nonetheless reflected a contemporary sensibility about the materiality of certain kinds of expressive conduct. As the lawsuit wound its way through the courts, Congress amended the definition of "material support or resources" to include "expert advice or assistance," and then amended the definition of "expert advice or assistance" to include "advice or assistance derived from scientific, technical or other specialized knowledge."[15] Expert speech, Congress seemed to be saying, has a kind of power that ordinary speech does not, and it can be restricted on that basis—which, both Congress and the courts seemed to think, is a different proposition than making invidious distinctions among kinds of speech or kinds of speakers. In a world in which the line between speech and computer-mediated action had become vanishingly thin, the idea that expert legal training produced material consequences could begin to seem entirely credible.

The statute also did not single out networked, digital communication as especially problematic, but the majority opinion by Chief Justice Roberts nonetheless reflects a contemporary sensibility about the threats posed by uncontrolled online spread of

potentially damaging information. The Court held oral argument in February 2010. In April 2010, the news broke that WikiLeaks.org, a self-described open government organization founded in 2006, had published a video of a 2007 attack by a U.S. military helicopter in Baghdad that killed a number of civilians, including children, and two Reuters employees. The video, which WikiLeaks titled "Collateral Murder," received extensive coverage by U.S. newspapers of record, which noted the organization's history of leaking hidden information about government and corporate operations.[16] WikiLeaks attracted its share of defenders, but its critics saw a textbook case of advocacy run amok and threatening to disrupt the orderly flows of policing and nation-building. A *New York Times* article on WikiLeaks published only a few weeks beforehand had quoted a Pentagon report as concluding that information of the sort routinely published by WikiLeaks "could be used by foreign intelligence services, terrorist groups and others to identify vulnerabilities, plan attacks and build new devices."[17]

The Court decided *Humanitarian Law Project* two months after WikiLeaks published the "Collateral Murder" video and two days after the *New York Times* reported as front-page news that U.S. Army Specialist Bradley Manning had been arrested on suspicion of having leaked the video and other information to WikiLeaks.[18] At oral argument and in its briefs, the government had asserted that expert training in human rights advocacy could work to legitimize dangerous organizations.[19] By traditional First Amendment standards, the argument was laughable; rhetorical battles over legitimacy are exactly the sorts of contests that belong in the realm of persuasion. The majority accepted it uncritically, and also noted that terrorist organizations could rely on such training to "threaten, manipulate, and disrupt" the international legal system.[20] Additionally, it cautioned about the risks of "straining the United States' relationships with its allies and undermining cooperative efforts between nations to prevent terrorist attacks."[21]

The exercise of situating the justices within a larger cultural context is inevitably speculative; even so, the justices live in the same world that the rest of us do. Read in context, the *Humanitarian Law Project* decision is a product of its time, and not only because the majority's observations about materiality, risk, and danger expressed the deference to asserted national-security imperatives that had become the norm in the post-9/11 environment.[22] Those observations also dovetail neatly with the fears about the uncontrollable viral spread of damning and damaging information that were suddenly coming to loom so large in the public view.

Both the *Humanitarian Law Project* litigation and the saga of the cryptography export rules supply object lessons in the expansionist trajectory of the logic of culpable facilitation in times of perceived exceptional threat. As domains of expertise far removed from violence and lawlessness were recast as inextricably entwined with threats to the body politic, government practices that the courts of an earlier era would have recognized instantly as overbroad and politically suspect came to seem both apolitical and existentially justified. In the case of the material assistance statute, that double shift in meaning has vastly expanded the universe of activities potentially meriting prosecution, sweeping in everything from human rights training to religious instruction to remittances sent by would-be migrants via private payment networks.[23] In the case of the export control regulations, the continuing provisional assertion of authority to verify the eligibility of cryptographic products for general distribution has enabled the government

both to assert an ongoing interest in the capabilities of networked communications products and services and to further that interest in ad hoc and unaccountable ways.

Other People's Property

A second strand of the contemporary discourse about speech and existential threats concerns the copyright pirate, and the appearance of this "fifth horseman" is in itself a development worth remarking. Initially, legislative anxieties about online immorality—in particular, pornography and drug dealing—promised to play a far more significant role in policymaking for the internet. Ultimately, however, the influence of powerful new information-economy actors and the economic logics of digital property and *digital contraband* proved both more durable and more difficult to cabin.

In 1996, fears about proliferation of online pornography and pedophilia became the focus of a short-lived and controversial legislative campaign to clean up the internet. Among other things, the proposed legislation provided an early illustration of the power of "alternative facts" to fuel outrage. In addition to horror stories and alarmist rhetoric, the bill's main sponsor in the Senate relied on an academic study that purported to measure the quantity and evaluate the nature of pornographic content available online, but that had serious methodological deficiencies. Its author had avoided traditional processes of peer review by seeking and winning publication in a student-edited law journal. Although his sensationalized claims were quickly discredited, that seemed to make little difference to the bill's supporters and did not slow its momentum.[24] As eventually enacted, the Communications Decency Act's prohibitions were broad and vague, establishing criminal penalties for the knowing preparation or solicitation and transmission of "indecent" content.[25]

As its opponents had foreseen, the CDA's core prohibitions could not withstand judicial scrutiny. Anxiety about sexually explicit speech is a traditional theme within First Amendment discourse, and precisely for that reason, claims that the internet was simply an out-of-control smut factory encountered well-established case law mandating very skeptical review. The federal courts swiftly invalidated both the initial legislation and the first revision that Congress attempted.[26] The effort to ban online smut became another chapter in a history of moral panic, legislative overreach and judicial correction that extends over many decades (As we saw in Chapter 3, that history creates its own risks, powerfully shaping civil libertarian thinking about current problems bedeviling platform-based speech environments.) In subsequent years, traditional First Amendment narratives have remained robust enough to quell periodic alarm about online smut and crime, and law enforcement officials have used traditional enforcement tactics to combat trafficking in unsavory materials.[27]

At the same time, however, alarm about the uncontrolled online spread of a different kind of information began to command the attention of law- and policymakers. Over the course of the twentieth century, the publishing, music, television, and motion picture industries had coalesced into a politically savvy interest group accustomed to exerting powerful influence over the shape of copyright legislation. By the 1990s, the software industry also had emerged as a force to be reckoned with in legislative debates. Both old and new copyright industries and their respective trade associations began a

systematic campaign to frame online copyright infringement as an existential threat to society in its own right.

In Congress and in the media, entertainment and software industry representatives worked to position online copyright infringement, and particularly peer-to-peer file-sharing, as morally objectionable and socially insidious. In a blizzard of press releases and media interviews, and in a variety of more formal interventions ranging from conference remarks to congressional testimony, they equated online copyright infringement with theft, piracy, communism, plague, pandemic, and terrorism.[28] They attempted to link peer-to-peer technologies with the rapid spread of pornography and with increased risk of exposure to viruses and spyware.[29] And they urged enactment of new laws designed to prevent unauthorized flows of digital content and to keep authorized flows secure.

During the 1990s, the convergence of economic power, legislative access, and moral panic rapidly produced a series of enactments expanding the duration of copyrights and prohibiting unauthorized access to and appropriation of valuable digital resources. New statutes included the Copyright Term Extension Act, which added 20 years to the terms of both new and already-subsisting copyrights; the Uruguay Round Agreements Act, which restored copyright protection to many foreign works then residing in the public domain; the Digital Millennium Copyright Act (DMCA) of 1998, which authorized new interdiction-based strategies for countering online copyright infringement; and the Economic Espionage Act, which criminalized the misappropriation of valuable trade secrets. Additionally, a series of amendments to the Computer Fraud and Abuse Act extended statutory prohibitions on unauthorized access to computing resources to encompass many more types of computer systems and a much wider range of conduct.[30]

Rejecting a steady stream of constitutional challenges to the new legislation, the federal courts concluded that, in general, new protections for proprietary information resources did not trigger the First Amendment at all. So, for example, in *Eldred v. Ashcroft* and *Golan v. Holder*, the Court held that laws retrospectively extending copyright terms and resurrecting lapsed foreign copyrights from the public domain required no special free speech scrutiny. That was so because, as Justice Ginsburg explained for the majority in *Eldred*, there is no "right to make other people's speeches."[31] Reasoning that copyright itself performs a constitutional function by incentivizing production and distribution of speech, the Court indicated that Congress has nearly unlimited leeway to expand the footprint of the copyright regime as long as it leaves certain traditional limits on copyright scope undisturbed. In cases challenging the DMCA's interdiction-related provisions, lower courts invoked the rhetoric of pandemic alongside that of piracy, framing online infringement as a threat to both the rule of law and the survival of the body politic.[32]

More generally, alarmist rhetoric about online infringement of intellectual property rights worked to alter the tenor of public discussions about ownership of and access to digital resources. Terms such as "piracy" and "theft," formerly rare in intellectual property discourse, have become commonplace. Public service advertisements funded by copyright industry organizations portray those downloading

music and movies as selfish, immoral, and criminal.[33] As the new narratives about digital contraband have become ordinary and familiar, they have worked to legitimate exceptional enforcement measures.

State Secrets and State Secrecy

A final important strand of the contemporary discourse about information contraband involves ever-expanding logics of *operational secrecy* surrounding government activities. Governments have always kept secrets, but the kind of secrecy that the logic of the exception justifies is different. With increasing frequency, the government has sought not only to punish unauthorized disclosures of particular information but also and more generally to develop institutional structures for "deep secrecy"—structures that free some government actors from the obligation to provide any account of their actions at all.[34]

Unlike rules prescribing export controls for munitions or targeting online copyright infringement, the state secrets doctrine is centuries old. Framed broadly in terms of the overlapping imperatives of national and domestic security, the doctrine has long been understood to shield certain kinds of information about executive branch operations from disclosure.[35] In the contemporary legal system, the state secrets doctrine underlies a variety of rules and practices, including the rules for classifying certain types of information as confidential, statutes that specify penalties for unauthorized disclosure, and procedures for in camera review of secret executive branch actions by special legislative oversight committees and courts. Those rules, statutes, and procedures exist in tension with others purporting to guarantee openness and transparency, including freedom of information laws and whistleblower protection statutes. Leaks and leaking in violation of state secrecy rules also are well-established practices with their own complex institutional sociologies.[36]

In the networked information era, however, anxieties about the dangers of uncontrolled information flow have elicited free-floating and seemingly unconstrained logics of operational secrecy that attach to a wide variety of government functions with asserted connections to national security. That shift has engendered intense debates about government accountability, lending momentum to an ongoing legal campaign to shed light on the far-flung operations of the modern surveillance state and also to diverse and creative efforts to create new institutionalized structures for facilitating leaking. In response, the government pursuit of operational secrecy has grown ever more determined.

By the turn of the twenty-first century, a diverse collection of scholars, tech industry observers, and legal advocates had become worried about vast, secret expansions in government surveillance activities and capabilities. Following the 9/11 attacks on the World Trade Center and the Pentagon, investigations into intelligence failures leading up to the attacks focused public attention on a set of special surveillance procedures authorized by the Foreign Intelligence Surveillance Act (FISA) and on a secret court constituted under the FISA to oversee surveillance requests.[37] Soon, however, the evidence began to suggest that surveillance programs authorized in the aftermath of 9/11 extended more broadly than even that statute permitted. In 2004, U.S. Treasury agents investigating Al-Haramain, a Muslim charity headquartered in Oregon, for alleged links

to terrorist activities abroad inadvertently disclosed to Al-Haramain's attorneys a document indicating that the government had undertaken lengthy warrantless surveillance of the charity's telephone calls.[38] In 2005, the *New York Times* published an investigative report revealing that, following the 9/11 attacks, the administration had authorized a program of warrantless mass communications surveillance, and in 2006, a technician who had recently retired from AT&T's San Francisco Bay Area operations center disclosed the existence of a long-term, secret government data-collection operation housed directly within the center itself.[39]

Litigation arising from these indirect and partial disclosures, however, led nowhere. After the Electronic Frontier Foundation filed a class action lawsuit against AT&T on behalf of customers who objected to the company's apparent facilitation of routine government monitoring, Congress hastily amended the FISA statute, authorizing the government to make warrantless demands for interception of communications with parties located abroad and granting retroactive immunity from civil liability to communications intermediaries that assisted with such interception. Because it now lacked authority to grant the relief plaintiffs had requested, the court dismissed the lawsuit.[40] A group of human rights advocates who believed that their calls with vulnerable clients and witnesses were being monitored filed a different lawsuit asserting that warrantless government surveillance under the amended statute chilled the exercise of their constitutional rights and those of their clients. Reasoning that plaintiffs could not prove that they or their clients had been targeted or that any of their communications had been collected and read, the court ruled that they had not alleged any actual injury and lacked standing to sue.[41] While that lawsuit worked its way through the appeals process, the massive scale of government communications surveillance was becoming something of an open secret. In 2012, *Wired* magazine published a detailed piece of investigative reporting by journalist James Bamford that described a new data center being built by the government in the middle of the Nevada desert and drew the obvious conclusions about the center's purpose.[42] Even so, a majority of the Supreme Court upheld dismissal of the constitutional claims, characterizing plantiffs' arguments as based on speculations and assumptions..[43]

Then, in June 2013, the world learned that former National Security Agency contractor Edward Snowden had copied and disclosed to reporters for *The Guardian* and the *Washington Post* voluminous files documenting the NSA's extralegal surveillance of communications worldwide. The documents revealed that the major U.S. telecommunications and internet access providers were operating under ongoing demands for bulk production of accountholder information and session metadata. They provided irrefutable, documentary proof of both the vast scope of the government's surveillance operations and the lawlessness of many of the component programs.[44]

The Snowden revelations led to new legislation ostensibly designed to rein in government excesses. After learning about the government's post-9/11 warrantless wiretapping, Congress had created a Privacy and Civil Liberties Oversight Board (PCLOB) but had given it very little authority; after Snowden, it gave the PCLOB independent status and charged it with evaluating the legality of the programs that Snowden had exposed and recommending additional reforms and best practices.[45] Additionally, it added language to the FISA statute restricting the scope of permissible

queries to telecommunications providers, thereby limiting the government's ability to submit new requests for bulk metadata production. It also created a small corps of advocate-advisors authorized to participate in FISA court proceedings on the public's behalf.[46]

From one perspective, the legislative response to the Snowden revelations continued a pattern of secretive government overreach and eventual legislative correction begun much earlier in the modern era. The Snowden episode was not the first revelation about massive unsanctioned government surveillance programs. In the 1970s, disclosures about the COINTELPRO operation—a surveillance and disinformation program devised by the Pentagon to discredit the American Communist Party, leaders of the civil rights movement, and members of a variety of other protest and social justice movements—had prompted a detailed congressional investigation and the enactment of the country's first modern electronic surveillance laws.[47]

From another perspective, however, the official response to the Snowden revelations both confirmed the inadequacy of post-COINTELPRO reforms and was far more anemic than the response to COINTELPRO had been. Unlike the Church Commission, constituted by the Senate to investigate COINTELPRO, the PCLOB lacked authority to compel the production of documents and witnesses, and its recommendations were purely advisory.[48] After it concluded that the bulk metadata program was unlawful and recommended that the program be discontinued and its stored data destroyed, the government took almost two years to comply.[49] Powerful legislators resisted enacting all of the reforms that the PCLOB recommended to provide more comprehensive public accountability, and public opinion remains starkly polarized about how much surveillance authority the government should have.[50] Last and importantly, as in the case of COINTELPRO, the enacted reforms both sanctioned many of the surveillance techniques formerly employed without express authority and institutionalized new processes for secret authorization.[51]

Litigation over government surveillance and related counterterrorism activities in the wake of the Snowden leaks and their legislative aftermath increasingly resembles trench warfare. Courts have become more willing to concede that the government conducted dragnet communications surveillance. However, they have then cited other justifications either for dismissal or for allowing only limited "jurisdictional discovery" that feature logics of fiat interdiction at their core, including both the need to defer to the executive branch in national security matters and the imperative of protecting state secrets.[52] Additionally, the government's litigation strategy has relied on the prevalence of sunset clauses and reauthorization requirements in national security surveillance statutes. Government officials have argued that courts should avoid ruling on the constitutionality of grants of surveillance authority that have since been amended, an argument that, if accepted, would effectively convert such provisions into strategies for evading judicial review.[53]

Litigation over government surveillance practices also has shown the government increasingly willing to experiment with new tactics involving refusal to follow ordinarily-applicable procedural and evidentiary rules. Recall Al-Haramain, the Muslim charity whose attorneys accidentally received a confidential document in discovery. The

attorneys promptly returned the document, but later sought to introduce testimony about it in litigation challenging the charity's designation as terrorist-affiliated. The government argued that the state secrets doctrine barred the testimony. The courts ultimately agreed with that interpretation of the doctrine but noted that the FISA statute authorizes courts (though not parties or their attorneys) in subsequent litigation to inspect documents relating to secret government surveillance. The district court therefore ordered the document produced for inspection subject to appropriate protective constraints.[54] Over a period of many months and multiple court orders, the government simply declined to comply. Ultimately, it was rewarded for its stonewalling. Although the attorneys for the now-defunct charity were able to obtain a ruling that the government's conduct had violated FISA, the litigation was dismissed on sovereign immunity grounds.[55] Prosecutors in later cases have followed the same playbook, stonewalling in litigation by individuals wrongly placed on the no-fly list rather than disclose information about the criteria for adding or retaining someone on the list; dragging out litigation over gag orders and then dropping demands for secrecy rather than risk an unfavorable ruling on constitutionality; and dismissing minor criminal charges rather than reveal the confidential and possibly ultra vires investigative techniques that led to them.[56]

Struggles over Facilitation and Control

Within the networked information environment, the logics of culpable facilitation, digital contraband, and operational secrecy work to justify the development and implementation of new enforcement strategies directed at unauthorized information flows. Network intermediaries represent attractive targets for such strategies. As noted earlier in this chapter, the idea that otherwise lawful acts sometimes can trigger liability for culpable facilitation is not new. That idea underlies criminal "aiding and abetting" liability, theories of indirect infringement in intellectual property law, and a variety of statutory prohibitions. The dominant justification for imposing liability on facilitators is instrumental. Such prohibitions exploit valuable cost efficiencies and, when effective, work to dry up the market for assistance to violators. If enforcement efficiency were the only relevant standard, it might make sense to treat network intermediaries as essential partners in a wide variety of network-based malfeasance. Most commentators and judges, however, have thought efficiency-based reasoning insufficient to serve as the sole justification for imposing liability. To avoid unfairness and preserve the social benefits that third-party activities often provide, theories of culpable facilitation typically have incorporated substantive protections that incorporate tests of moral responsibility, such as requirements of culpable knowledge or intent, and have been invoked in settings where procedural and evidentiary safeguards are available. [57]

The new interdiction rules are different in both form and effect. Within the Hohfeldian framework that has guided the inquiry in this part of the book, entitlements to pursue third-party facilitators of unlawful conduct are not simply rights, although they are often justified that way, because they do not simply impose correlative duties. Instead, they confer authority to require such facilitators to perform their own activities differently to avoid civil or criminal liability. In Hohfeldian terms, interdiction mandates are most aptly classified as powers to alter the legal obligations of others and to impose liability

for noncompliance.[58] Those powers, moreover, increasingly are defined and implemented in ways that de-emphasize traditional substantive and procedural protections and emphasize instead the bare force of legal authority. As the logics of fiat interdiction have begun to work themselves into information law and policy, they have melded and recombined to produce hybrids that reflect origins in both national security and intellectual property enforcement practice.

At the same time, however, struggles over interdiction rules have come to reflect the unexpected power and influence of network intermediaries, and particularly of the dominant platform firms. Recall from Chapter 3 that during the drafting of the Communications Decency Act, opponents of the proposed anti-smut law achieved what seemed to be a limited victory in the form of an immunity provision for internet access providers that simply redistributed speech made by others. Described as a "good Samaritan" provision, section 230 of the CDA was intended to encourage internet access providers to develop and voluntarily adopt measures for filtering out undesirable content or enabling users to do so.[59] As we saw in Chapter 3, section 230 has become the cornerstone of a legal regime that shelters internet service providers of all sorts—including platform providers that play very active roles in shaping the universe of information that users see—from accountability for both old and new information harms. And the nascent industry that it was designed to protect has become one of the most powerful in the world.

As network intermediaries have resisted efforts to write the logic of the exception into law, they have become masters at both public relations and inside-the-Beltway political positioning. The result is a legal and media landscape characterized by complex power struggles among the dominant interests. In those struggles, platforms do not simply play defense. Rather, they have worked to position themselves as both essential partners and competing sovereigns in the quest to instantiate states of exception algorithmically.

Finding and Paying for Contraband

In the domain of copyright, the logics of digital contraband and culpable facilitation have melded to produce a deep and seemingly permanent shift in the nature of enforcement activity. Thirty years ago, the principal enforcement tool was the civil infringement lawsuit. Criminal enforcement was relatively rare, and capabilities for technical enforcement were virtually nonexistent.[60] Today, all that has changed. Third-party facilitators have become principal targets of efforts to block unauthorized flows and eliminate unauthorized channels. The interdiction game is played on multiple fronts simultaneously—in courtrooms, legislative hearings, rulemakings, and treaty negotiations—and targets every stage in the process of finding and paying for digital content. Efforts to impose broad mandates fail with some regularity but often are followed by private initiatives that achieve similar results and that enable platforms to assert their own authority over the terms and conditions of information flow.

On the civil enforcement side, one important strategy for interrupting flows of digital contraband relies on a statutory "notice and takedown" regime for obtaining removal of publicly posted content. Enacted as part of the Digital Millennium Copyright Act of 1998, the regime exploits the interplay between the statutory procedures and

background doctrines governing indirect infringement liability. Generally speaking, indirect infringement liability requires some form of culpable knowledge. Compliance with the notice and takedown regime confers safe harbor from liability, but failure to remove infringing material after learning of it vitiates the safe harbor—and, given the scope of many online intermediaries' operations, threatens crushing liability. The regime therefore encourages speedy removal triggered by notice without prior judicial review. (To help make this work, interdiction imperatives relating to digital contraband also figure prominently within neighboring legal regimes. Intellectual property enforcement is a categorical limitation on the immunity granted to online service providers under section 230 of the CDA, and it has been a categorical exception to both net neutrality rules adopted by the Federal Communications Commission (FCC).[61]) Although the notice and takedown regime regularly elicits significant numbers of meritless or legally questionable takedown notices (many generated by automated processes for detecting infringement), it has been implemented around the world as a result of pressure exerted by U.S. trade negotiators.[62]

The emergence of the platform business model at the turn of the twenty-first century placed the copyright industries and the internet industries on a collision course with regard to the scope of the statutory safe harbors. The DMCA's separate safe harbors for hosting and information location services were drafted before the emergence of automated search, content aggregation, and social networking technologies began to blur such easy distinctions. From the copyright industry perspective, new platform-based technologies for storing, indexing, and sharing uploaded information seemed designed to encourage infringement. In a series of high-profile lawsuits, powerful copyright owners have argued that the platform business model falls outside the scope of the safe harbors, and that the venture capitalists, law firms, and payment processors that work with platforms to facilitate access to digital content also should be held accountable for the widespread availability of digital contraband. In Congress, they have pressed their case for affirmative filtering obligations and other new mandates.

Copyright industry efforts to impose stricter obligations on platforms, however, have failed repeatedly. Over and over again, litigation designed to win rulings unambiguously extending indirect infringement liability to platforms and other alleged third-party facilitators of infringement failed to produce the desired results.[63] Meanwhile—and partly as a result of the copyright wars—the internet industry gradually found its political voice. Although internet businesses did not play a major role in the debates over the notice and takedown provisions, as dominant platforms began to emerge, the political landscape began to shift. The events surrounding enactment of the DMCA had sparked a vibrant, populist backlash against maximalist copyright enforcement, out of which emerged both new organizations constituted to speak on behalf of the public domain and new entrepreneurial ventures, such as the Creative Commons movement, offering alternative legal platforms for content distribution. In addition to emphasizing the now-familiar theme of permissionless innovation, the new platform firms learned to appropriate other strands of anti-maximalist rhetoric for their own purposes, latching onto the themes of commons, open content, and fair use to advance their own interests. And as platforms became more adept at flexing their political muscle, defeating wave after wave

of proposed new legislation, the copyright legislative juggernaut began to lose momentum.[64]

Matters came to a head in 2011, when the motion picture, recording, and major league sports industries convinced several members of Congress to propose legislation that would empower courts to cut off the services provided by payment processors and other infrastructure providers upon ex parte application by an aggrieved rightholder. The Stop Online Piracy Act (SOPA) and its companion bill, the Protect Intellectual Property Act (PIPA), were expected to pass by a wide margin. Instead, Google and other platform firms coordinated a massive mobilization of the online community that effectively shut down many of the internet's most popular sites. Shortly thereafter, Congress tabled the legislation and has not revived it.[65] The SOPA and PIPA debacle signaled a sea change in the politics of intellectual property—the end of uniform and unwavering support for the protectionist legislative agenda that dominated the 1990s and 2000s. In subsequent years, the rate of proposals for new legislation has slowed dramatically—although, as Chapter 7 will discuss, attempts to ensure that new trade agreements include strengthened enforcement obligations have continued.[66]

Yet this recounting of legislative and litigation failures to impose mandates for what legal theorist Jack Balkin calls "digital prior restraint" overlooks the extent to which interdiction of infringing content by search, social networking, and payment providers increasingly has become the norm. Every major platform that hosts user-provided content uses automated filtering technology to prevent the posting of infringing content, and the major payment providers increasingly have followed suit, entering agreements with the major copyright trade associations that obligate them to restrict access by entities and sites identified as infringing.[67] Similarly, following its successful campaign against legislated domain-blocking requirements, Google announced that it would begin demoting or removing entirely from search results sites that generate repeated takedown notices.[68] Platforms such as Google's YouTube also offer copyright owners the opportunity to monetize unauthorized uses of their content by claiming a portion of the advertising revenues.

From the platform perspective, decisions to institute voluntary automated filtering represent a pragmatic response to background legal doctrines that establish indirect liability for contributing to infringement. Although courts have resisted interpreting those doctrines in ways that would make liability flow near-automatically to platforms or payment providers, they have indicated that the details of platform design and behavior matter. Copyright litigation between the major industry players can be prolonged and expensive—litigation between Viacom and Google over infringing videos on YouTube dragged on for seven years—and, as already noted, the penalties for guessing wrong include statutory damages potentially running into millions of dollars.[69] But automated filtering also does not simply amount to capitulation; platforms have declined to disclose their methods or to give copyright industries a say in their implementation.

To similar effect, the enforcement playbook that eventually emerged for addressing the widespread use of peer-to-peer file-sharing technologies is pragmatic and relies heavily on the voluntary actions of service providers. Because peer-to-peer file-sharing technologies are designed to eliminate central indexing, winning indirect

infringement lawsuits against their providers has proved difficult, and when claims do succeed, they tend to result in remedial orders that are impossible to enforce. Additionally, the notice and takedown regime applies only to hosting and information location providers, not to internet access providers whose services are used to engage in file-sharing. Some copyright owners have used automated investigative tools to discover and attempt to identify individual users of peer-to-peer technologies who appear to be downloading proprietary files, but suing users directly has never been the preferred enforcement strategy.[70] Additionally, although U.S. courts have rejected privacy challenges to subpoenas for production of subscriber information, within the more privacy-protective European legal environment, there is ongoing tension between interdiction and privacy imperatives. Consensus on the appropriate balance remains elusive, with directives concerning intellectual property enforcement and data protection imposing arguably conflicting mandates.[71]

Many peer-to-peer downloads, however, eventually come to rest in cloud storage, and cloud storage providers are vulnerable to both civil suits for contributory infringement and criminal enforcement proceedings. Both in the United States and around the world, criminal copyright enforcement has become far more frequent. Over the course of the 1990s and 2000s, in response to rising panic about the uncontrolled spread of information contraband, Congress amended the criminal provisions of the federal intellectual property laws nine times, expanding the categories of conduct eligible for prosecution, increasing penalties, and giving both prosecutors and copyright owners new and powerful tools for site-wide blocking and domain forfeiture.[72] At the urging of trade negotiators from the United States and other developed countries, similar provisions have spread throughout the world.[73] For companies seeking to establish themselves as providers of legitimate services, the possibility of prosecution is more than just theoretical. Federal prosecutors have issued several indictments against cloud storage providers, including the widely publicized proceedings against MegaUpload and its colorful principal, Kim Dotcom, for criminal copyright violations. Unsurprisingly, major cloud storage firms serving the U.S. market have implemented automated systems for scanning clients' stored content to detect files with cryptographic signatures (or "hashes") that match those supplied by rightholders.[74]

Circumventing Digital Barriers

Another important strategy for online copyright enforcement involves new prohibitions on circumvention of technical access protections, trafficking in circumvention technologies, and knowingly obtaining valuable trade secrets through improper means. Through these strategies, which meld the logics of culpable facilitation and digital contraband with that of operational secrecy, copyright enforcement efforts have become efforts to rearrange information flows within circuits of authorization. Legal prohibitions target both unauthorized access and dissemination of technical expertise that might disrupt secure channels for information flow.

In addition to establishing a notice-and-takedown regime for removal of content posted without authorization, the DMCA included other provisions prohibiting circumvention of technologies applied to protect copyrighted works against unauthorized access and banning trafficking in circumvention technologies.[75] According to the internal

logic of those provisions, circumvention technologies themselves are dangerous knowledge. Those distributing such technologies are culpable facilitators, as are those who attempt to understand circumvention protocols and share information about them without following proper procedures.

Following their enactment, the anti-trafficking provisions became the cornerstone of a litigation campaign designed to deter the unauthorized development of systems for accessing and rendering copyrighted content. Unlike litigation against platform providers based on theories of indirect infringement, that campaign has been an unqualified success. A series of court rulings interpreting the provisions to bar the development of unauthorized devices for rendering content, even if the content itself was lawfully acquired, gives copyright holders and their licensed technology developers comprehensive de facto control over the design and functionality of digital media players, video recorders, and gaming systems.[76] As a result, licensing of access control protocols has become widespread. The major commercially available systems for delivering and playing audio and audiovisual content now incorporate functionality designed to defeat unauthorized copying and prevent retransmissions to unauthorized platforms and devices.[77] Like interdiction imperatives directed at digital contraband, struggles between copyright interests and communications providers over secure digital protocols also have spilled over into neighboring legal regimes; most recently, a rule proposed by the FCC to enable competition in the provision of cable set-top boxes was defeated after copyright lobbyists mobilized against it.[78]

Exceptions to the anti-trafficking provisions for software reverse engineering, security research, and encryption research do exist but are crafted in ways that largely precludes their use by ordinary members of the public. Those conducting encryption research must make "a good faith effort to obtain authorization" and can claim exemption from anticircumvention liability only if factors including their purpose and their credentials suggest that it is warranted. Those engaged in software reverse engineering may share operational information about technical protection systems with others only for the purpose of creating a separate interoperable computer program, and those conducting computer security testing must use their findings "solely" to promote the network owner's security.[79] The overall—and likely intended—effect of these provisions is twofold. The restrictions on information sharing conflict with the foundational commitments of open source software communities and therefore burden those communities in particular. More generally, the emphasis on credentialing and tightly controlled sharing operates to foreclose unauthorized experimentation and innovation of all sorts.[80]

The DMCA's anti-circumvention provisions, meanwhile, authorize the Copyright Office to declare exceptions on a case-by-case basis, but only if it finds that users are likely to be "adversely affected" in their ability to make use of "particular classes" of works.[81] Those criteria, and the procedure more generally, sit in substantial tension with the innovative ethos that supposedly defines the information era. Although "ask forgiveness, not permission" has become a Silicon Valley mantra, those wishing to engage in acts of circumvention must ask permission, not forgiveness, and must agree to stay within narrow, well-defined limits. The lists of exceptions requested and granted since the process began, which includes actions such as transferring a mobile phone

between provider networks and repairing automotive components, reveal that the anti-circumvention provisions have been invoked not simply to protect copyrights but also and more fundamentally to stifle competition in important consumer markets.[82]

A related frontier for struggles over interdiction authority is the concept of a "right to repair" the software in consumer devices, vehicles, and appliances. Assuming that one can gain access to the software in one's mobile phone, car, or tractor under an exception to the circumvention ban, the process of diagnosis and repair may create the factual predicate for a copyright infringement claim. The Copyright Act permits owners of copies of software to take the necessary steps to repair those copies, but software copyright owners typically structure end-user transactions as licenses and argue that the statutory protections for owners do not apply. A "right to repair" movement has begun to emerge at the state level; so far, however, it has produced little momentum for change at the federal level.[83]

Platform firms have an ambivalent relationship to the anti-circumvention and anti-trafficking provisions. The DMCA does not mandate use of any particular technical protection system or standard but rather encourages private development of technical protection measures and, ultimately, private standard-setting. As a practical matter, those processes have different effects on established firms that are major players in content distribution markets and smaller or start-up firms. Participation in industry-driven standards processes is costly and tends to require both long-term commitment and a preexisting organizational track record. Such processes therefore tend to favor established providers, including dominant platform firms like Apple and Microsoft that are also personal computing and consumer electronics firms. More generally, the rise of "walled gardens" for access to proprietary content is compatible with the "rich-get-richer" principle of network organization (discussed in Chapter 1) and reinforces the platform business model. Smaller and start-up firms have difficulty gaining access to processes dominated by industry insiders and confront higher litigation risk when they try to design around existing case law.[84]

The momentum to entrench technical protection of digital content appears to be accelerating at the global level. As Chapter 7 will discuss, at least some internet standards organizations have begun to look more favorably on efforts to develop network standards that are compatible with technical protection protocols. According to the official positions of the United States and other developed countries, strong intervention in the online environment on behalf of intellectual property owners is entirely consistent with solicitude for freedom of speech.[85] Technical protection protocols, though, can be deployed in many different ways—for example, to privilege content authorized by state sovereigns and disfavor dissident content or content circulated anonymously. As a practical matter, then, as democratic states have intensified their commitments to technical protection measures for copyright enforcement, that stance opens the door to other kinds of hard-coded interdiction as well.

Keeping Unauthorized Secrets

In the context of the government's desire to stop dangerous information from flowing, the logic of culpable facilitation disfavors concealment and suggests instead that network intermediaries should provide government investigators with unimpeded access

to private communications. That logic has set in motion cycles of reaction and counterreaction that are increasingly extreme. Technologists and activists have worked to develop techniques for more effective digital privacy and security; additionally, as Chapter 8 discusses in more detail, in the networked information era, anonymous online action has become a potent and unruly source of political power. The prospects of enhanced concealment and anonymous direct action in turn have inspired more intensive and often lawless surveillance practices. As government officials have pushed for more seamless access to private communications, network intermediaries have pushed back, citing both civil liberties and network security considerations. And yet platform interventions in debates about surveillance reform often have seemed calibrated first and foremost to preserve their own authority vis-à-vis threatened intrusions by government actors.

From one perspective, the most effective way of enabling governments to detect transmissions of dangerous information would involve modifying core internet standards and protocols to make them surveillance-ready. As noted earlier in this chapter, many authoritarian states already require internet intermediaries operating within their borders—including backbone providers, search engines, and social networking sites—to block a broad array of content deemed subversive. Embedding capabilities for surveillance and policing more deeply within the internet's protocol stack might seem a logical next step. Countries with democratic political traditions, however, have regarded that approach as inconsistent with core commitments to fundamental human rights. In global internet standards proceedings, they have opposed proposals for surveillance-ready standards introduced by some authoritarian governments.[86]

In democratic states, the logic of the exception has pushed surveillance policy and practice in the opposite direction, toward development of interception capabilities that can be deployed at the network's endpoints in particular cases. Following the failure of early attempts to control the spread of encryption code, law enforcement agencies have worked continuously to preserve lines of access into networked communications systems and devices. In 1994, Congress enacted legislation requiring telecommunications providers to design and maintain wiretap capability, but efforts to legislate similar "back door" capabilities for digital microprocessors were defeated after strong opposition from both the computer industry and academic computer scientists.[87] Continued technological evolution has disrupted that fragile equilibrium, however. The intercept capabilities mandated by statute are increasingly obsolete in an era in which communications by voice, text, and email all travel over digital networks and in which capabilities for strong communications encryption are increasingly widespread.

The political equilibrium briefly attained after the "crypto wars" of the 1990s has also become unstable. The Snowden leaks did not simply expose mass surveillance programs conducted under color of law based on overbroad interpretations of existing statutes. They also revealed a variety of equally longstanding but far more clearly lawless government surveillance practices that included hacking into overseas data centers to scoop up communication flows outside the territorial United States, remotely accessing privately owned computers and installing keyloggers or commandeering built-in cameras and microphones, and compromising network security protocols to permit repeated access.[88] Subsequent leaks from other sources have also revived the specter of

COINTELPRO, revealing that the government has conducted routine ongoing surveillance of civil rights and social justice activists even as it has downplayed the large and growing problem of domestic terrorism and discontinued an official program to track home-grown extremist groups that actually advocate violence.[89]

Unlike the surveillance debates of the 1990s, however, contemporary debates about the scope of government surveillance authority have unfolded against a backdrop of ongoing struggle between governments and dominant global platform firms, with each vying for both the moral high ground and the practical upper hand. In 2008, after several widely-publicized capitulations by platform firms to authoritarian regimes' demands for censorship, a coalition of platform firms, academics, and nongovernmental organizations formed the Global Network Initiative, the website for which proudly proclaims: "Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age."[90] The documents leaked by Snowden, however, revealed both traditional telecommunications providers and new digital platform firms to be essential participants in ongoing and seemingly unconstrained government surveillance operations. Subsequently, the dominant global platform firms have worked hard to restore and burnish their civil libertarian public personae, publicizing their legal challenges to government surveillance efforts and positioning themselves as the principal line of defense for individuals and groups concerned about government overreach.[91]

As a practical matter, meanwhile, two of the principal strategies that have been deployed to check national security surveillance strengthen the privileged position of private-sector communications intermediaries. One strategy involves control over data retention. As noted previously, post-Snowden, Congress enacted legislation narrowing the government's authority to request production of telecommunications metadata; as amended, the FISA statute now requires such requests to be structured by appropriately defined selectors and effectively bans bulk collection.[92] Self-evidently, the amendments do not limit communications intermediaries' power to collect and retain data for their own purposes, but rather depend on their continuing to do exactly that. The year beforehand, the Court of Justice of the European Union had invalidated a European Union directive mandating data retention by communications providers, ruling that the mandate imposed a disproportionate burden on citizens' fundamental rights. That ruling, however, did not speak directly to purportedly consensual platform activities that result in equally comprehensive collection and retention of data about users, and a separate directive governing data collection and processing for law enforcement purposes unambiguously authorizes governments to compel production of such data.[93]

A very different strategy for limiting communications surveillance by state actors involves platform provision of strong communications encryption. After the Snowden revelations, platform giant Apple spearheaded a push to make strong encryption the marketplace default for both voice and text communications. That campaign received an important boost when Facebook agreed to enable encryption by default for users of its WhatsApp messaging service, used by billions of people worldwide.[94] Once again, however, questions about lines of access for government investigations have become hotly contested. In the wake of the 2015 terrorist attack in San Bernardino, California, after which investigators acquired but could not readily access one terrorist's iPhone, law

enforcement and national security officials mounted an aggressive campaign, still continuing as of this writing, to convince both Congress and the courts to impose decryption mandates on communications firms that provide strong encryption capabilities to their users. Technology experts, in turn, have renewed their earlier arguments that mandatory decryption "back doors" will make the network less secure for everyone, and the rising tide of data breach incidents has made those arguments even more compelling.[95]

Notably, strong encryption is an increasingly toothless safeguard against *commercial* surveillance, so even a complete shift to strong encryption for communications would not disrupt the platform business model much, if at all. As we saw in Chapters 2 and 3, that model revolves around the application of machine learning techniques to the digital traces of people's activities in real and virtual spaces. Communications data provide useful inputs to that process, but those inputs are neither the only nor the most important kinds of information on which the platform business model relies. To the contrary, within the behaviorist framework that animates platform logics, what people say to each other matters far less then what they do. Even with strong communications encryption, digital traces of what people do remain available to the platform provider—location-based information collected from mobile devices, sensor-based techniques for tracking cursor movements, click-through information for items in newsfeeds and social network status updates, DNS level information for tracking web browsing, and so on.

Network architectures constructed for widespread, sensor-based data harvesting in turn have affordances that facilitate opportunistic data grabs by state actors, and when such data grabs occur, laws purporting to safeguard communications privacy do not interpose significant obstacles. The surveillance economy and the surveillance state are inextricably intertwined in more ways than one. As the sensing net extends more broadly throughout and deeply into the everyday lives of ordinary people, the scope for unauthorized secret-keeping narrows.

Publicizing Forbidden Knowledge, Part 1: Enforcing Government Secrecy

Government efforts to preserve and expand operational secrecy, meanwhile, have harnessed a variant of the logic of digital contraband, within which the government's quasi-proprietary interest in secret information trumps the public's right to know. Just as the idea of digital property has come to signal a definitional exception to protections for expressive freedom, so the strategies deployed to block flows of information that the government wishes to keep secret have begun to signal equally absolute exceptions to ordinary principles of due process and government accountability.

Consider first the WikiLeaks/Manning and Snowden episodes described earlier in this chapter. The historical precedent most directly comparable to the leaks by Manning and Snowden is the Pentagon papers episode. In 1971, Daniel Ellsberg, a high-ranking analyst for the RAND Corporation, had become increasingly disillusioned with the Johnson administration's publicly stated justifications for continuing the Vietnam War. Ellsberg copied documents revealing previously undisclosed information about the extent of U.S. military involvement in Southeast Asia and shared them with the *New York Times*, which began publishing selected excerpts.[96] The government indicted Ellsberg for

violations of the Espionage Act and sued the *Times* in an attempt to enjoin additional disclosures of classified information. The episode did not, however, end with Ellsberg imprisoned and the *Times* cowed into submission; instead, it revealed a judicial system that was fiercely independent and robustly accountable to overarching principles of expressive freedom and the rule of law. The Supreme Court handed the *New York Times* a sweeping victory, ruling that freedom from prior restraint was essential in order for the press to "fulfill its essential role in our democracy" and that the government had not met the very heavy burden that would be necessary to override that freedom.[97] (Three justices, however, thought that the government's assertion of national security considerations warranted greater deference.) Subsequently, after revelations that government investigators seeking to discredit Ellsberg had themselves committed multiple criminal acts, the government's attempted prosecution of Ellsberg ended in dismissal.[98]

Decades later, the prosecution of then-Bradley Manning for distributing classified materials to WikiLeaks and the controversy over the Snowden leaks have unfolded very differently. Ellsberg had been a civilian; Manning was a member of the U.S. armed forces and was court-martialed before a panel of military judges, a tribunal relatively insulated from the influence of public opinion. The Espionage Act criminalizes willful publication of classified information detrimental to the United States without regard to the motive underlying publication, which over the years has made it a convenient vehicle for prosecution of whistleblowers attempting to shed light on government misdeeds.[99] In an effort to mitigate the eventual punishment, defense counsel called Harvard Law professor and internet law expert Yochai Benkler to testify that WikiLeaks should be regarded as a legitimate journalistic endeavor and that the charges against Manning threatened to chill the practice of investigative journalism. Observers were unsurprised, however, when Manning was convicted and sentenced to 35 years in prison.[100] Edward Snowden, who had fled the country before sharing the documents about bulk NSA surveillance, faces charges that carry the death penalty, and remains in Russia on the advice of counsel.[101] Meanwhile, the pattern of prosecuting leakers and whistleblowers has continued. Most recently, Reality Winner, a national security contract employee and former military officer, now faces a 10-year prison sentence for providing the press with a document prepared by the NSA confirming Russian attempts to compromise U.S. digital voting systems before the 2016 presidential election.[102]

Perhaps because the *New York Times* precedent so clearly shields media organizations from criminal liability for publishing materials of public concern, no charges were brought against the long list of established media organizations that published excerpts from the Manning and Snowden leaks, but other organizations and individuals have been less fortunate. Documentary film-maker Laura Poitras, who later served as one of Snowden's initial contacts, was subjected to systematic surveillance and repeated border detentions after having filmed an Iraqi family watching an American military operation from the roof of their home. Freelance journalist Barrett Brown, who embedded himself with hackers to research the operation of the hacker collective Anonymous, was tried and convicted for violating the federal computer fraud and abuse laws and served four years in prison. Federal prosecutors secretly filed charges against WikiLeaks founder Julian Assange and have pursued his extradition to the United States,

even though he is not a U.S. citizen and was not within U.S. territory when he took the actions that incurred the government's displeasure.[103] Leaving nothing to chance, organizations such as the *Times*, the *Washington Post*, and *The Guardian* have worked to distance themselves from WikiLeaks and its methods, stating publicly that they do not simply publish information received from whistleblowers, but instead conduct due diligence to guard against endangering covert agents or undermining military operations.[104]

The logic under which the government asserts a free-floating interest in operational secrecy often blurs state and private economic interests, giving the secrecy claims a distinctly proprietary cast. Since its enactment in 1966, the Freedom of Information Act has exempted trade secret information submitted by private parties from the disclosure obligations that ordinarily attach to information about how the government operates.[105] As digital technologies and capabilities furnished to the government by private contractors have become more central to national security and law enforcement operations, both the privileged status of trade secrets and the legal justifications asserted for protecting secrecy have changed. The criminal prohibitions in the Economic Espionage Act of 1996 explicitly refer to both private economic and national security concerns stemming from the misappropriation of valuable information.[106] As Laura Donohue has shown, many post-9/11 cases in which the state secrets privilege is asserted involve government contractors. Many of those cases are really disputes about trade secrecy, in which the state secrets privilege functions as a tool for preserving economic advantage. Similarly, in ordinary criminal proceedings, federal and state prosecutors have begun to assert contractual obligations to respect trade secrecy as a way of shielding information about privately-sourced surveillance technologies from disclosure.[107]

A newer collection of techniques used by state actors to protect operational secrecy also echoes the intellectual property enforcement playbook. After it published the cache of diplomatic cables provided by Manning, WikiLeaks suddenly found itself without DNS and Web hosting providers and without a way to process donations. Although government officials denied that official pressure on EveryDNS.net, Amazon.com, and PayPal, which formerly had provided those services to WikiLeaks, caused those sites to terminate their relationships, industry observers who had watched the developments closely concluded otherwise.[108] In 2009, British law enforcement conducted a warrantless raid and seizure of computer equipment at premises owned by the operator of a Web server used by IndyMedia, an independent journalism collective founded to provide an alternative perspective on current events to that offered by giant media corporations. The stated purpose was to obtain removal of personal information posted about a judge, but the information had already been removed by the site operator.[109] The national security letters that demand production of communications and financial records include nondisclosure provisions that mimic those commonly found in trade secrecy licensing agreements. State authorities also have deployed credentialing tactics to suppress unwanted criticism of the way they do their jobs; recently, an Oregon administrative board fined a critic of its traffic light timing protocols for practicing engineering without a license.[110]

Platform firms have publicly resisted some government efforts to protect operational secrecy, but here again both the extent and the purpose of that resistance are

hotly debated and difficult to parse. Google, Twitter, and other communications intermediaries have filed lawsuits to challenge the secrecy surrounding government programs for communications surveillance and have scored some important victories. Although, as already noted, courts remain reluctant to second-guess government threat assessments, they have treated demands to maintain secrecy indefinitely with greater skepticism. Arguing that the public has a right to be informed about the fact of government surveillance activity, communications intermediaries also have developed a "warrant canary" system to circumvent the nondisclosure requirements in national security letters. These actions have garnered accolades from digital civil liberties groups. Other commentators, more skeptical, observe that platforms challenge only a very small number of the orders they receive and that important information about the level and nature of the cooperation between platform firms and law enforcement entities remains undisclosed and undiscovered.[111]

Publicizing Forbidden Knowledge, Part 2: Competing Sovereignties

Other government efforts to prevent the spread of forbidden information involve materials distributed by terrorist, extremist, and organized hate groups. Here the logics of dangerous information and culpable facilitation collide more directly with platforms' interest in maintaining their own operational secrecy—and also with the logics of innovative and expressive immunity that Chapter 3 explored. Government efforts to enlist platforms in efforts stop dangerous information from flowing have triggered protracted, still-unresolved struggles over the nature of platforms' obligations, the adequacy of their disclosures, and the extent of their power.

It is useful to begin by noting an obvious disconnect within emerging logics of fiat interdiction: Despite the increasingly draconian nature of such logics and the undeniable fact that platform-based intermediation works to target flows of information toward recipients identified as especially willing to receive them, nobody has prosecuted platforms for, say, material facilitation of terrorism. In the United States, although the possibility of prosecution undoubtedly has been the subject of private discussions both at the Department of Justice and in platform C suites, the *public* struggles over the extent of platforms' interdiction obligations generally have concerned whether and under what conditions platforms must permit communications to flow, not whether and under what conditions they should be required to block them. Civil suits filed against platforms for facilitating the spread of terrorist information have been quickly dismissed. As we saw in Chapter 3, that result follows straightforwardly from the language of section 230 of the Communications Decency Act and its accompanying logic of expressive immunity, and it has been greeted with widespread approbation.[112]

In Europe and elsewhere around the globe, debates about platform obligations have followed a somewhat different path. Following a series of terrorist attacks in Europe and Britain by homegrown perpetrators who had been radicalized in part by online recruiting materials, government authorities began publicly pressing platforms to block certain types of content more aggressively and effectively. As of this writing, Germany has enacted legislation requiring platforms to remove "unlawful content" within a period of time ranging from 24 hours to seven days. Russia has proposed legislation requiring deletion of "illegal content" within 24 hours, and the European Commission has issued a

proposed regulation that would impose liability for failure to remove "terrorist content" within one hour. Predictably, these developments have elicited howls of protest and dire warnings about the incipient triumph of state censorship from U.S. commentators.[113]

The dominant U.S. platform firms initially resisted pressure from European governments to alter their content removal policies, invoking the "technologies of freedom" ideal and the logics of innovative and expressive immunity. As it became clear that European policymakers had no intention of emulating their American counterparts' pliability on matters of platform autonomy, however, they gradually became more amenable to negotiation and compromise. In 2017, Facebook, YouTube, Microsoft, and Twitter announced plans to begin developing a shared registry of content identified as terrorist-affiliated and marked for removal—and framed the initiative as a voluntary act of good corporate citizenship.[114] In 2018, Facebook announced that it would host a delegation of French authorities for closed-door discussions about possible improvements to its content removal protocols.[115]

Under pressure from European governments, U.S. platform firms also become more amenable to discussing aspects of their content removal policies publicly. From time to time, journalists and scholars had extracted bits of information about platforms' policies and practices for content flagging, review, and removal, and in May 2017, leaked Facebook training manuals and other documents afforded a more comprehensive picture of then-existing policies regarding harassing, suicide-related, hate-related, and terrorist-related content. Subsequently, Facebook and other platforms began to release more detail about their "content moderation" policies and practices.[116]

At the same time, however, platforms have mobilized both their own logics of operational secrecy and narratives about heroic civil libertarian opposition to state censorship to manage the terms of the public debate about content removal, mandated and otherwise. We have already seen in Chapter 3 that releases of takedown information can be highly selective and strategic. So, for example, Google and other platform firms have labored both to provide information about takedowns pursuant to the European right to be forgotten and to do so in ways that express their opposition to the new requirements. The major platform firms also have developed new "transparency reports" to publicize information about takedown notices served by copyright owners and firms acting on their behalf. Platform responses to demands for interdiction of terrorist and extremist content have followed the same general pattern. Information about takedown statistics for other unlawful content is a core component of the new strategy of engagement with European governments, and so are efforts to publicize politically motivated requests for content removal.[117]

Other interventions by platforms assert their own innovative and technical authority over the logistics of content moderation and content removal. Conference presentations by representatives of a number of leading firms play up themes of technical and managerial expertise, stressing the scale of their operations, the technical and contextual difficulties that surround identifying the relevant content, and the human resources challenges entailed in managing the workers tasked to review it.[118] Notably, however, when discussions about interdiction of terrorist and hate speech turn toward the operational details of platforms' content *recommendation* practices, however, the

newfound commitment to openness ends. As earlier chapters have described, platforms work hard to keep information about the ways in which their intermediation practices foster *im*moderation out of court and out of public view.

My goal here is not to litigate whether platforms are doing enough or too much (or, perhaps, not enough and too much at the same time) but rather to focus the reader's attention on the ways that the outcomes just described are both inconsistent with the logics of existential threat and fiat interdiction that this chapter has traced and entirely consistent with the larger patterns explored in earlier chapters. The complex interplay between law and private economic power is reshaping both information-related entitlements and practical enforcement realities across a variety of contexts. To the ledger listing reasons for U.S. authorities' relatively hands-off approach to platforms must be added tacit acknowledgement of the central organizational role that platforms play in the political economy of informational capitalism and deep internalization of the neoliberalized logics of innovative and expressive immunity that platforms and other information businesses have so vigorously asserted. Interdiction mandates arising outside the United States, meanwhile, exist in unavoidable tension with platforms' day-to-day operational control—and dominant platform firms' pockets are very deep indeed.

Information Power and the Reconstruction of Law (and Order)

Commentators have disagreed vigorously about how to evaluate each of the developments that this chapter has described. Some warn of rapidly metastasizing government overreach, while others worry that the government should be doing more to protect the security of borders, critical infrastructures, and civilian populations. Some argue that technology-based copyright enforcement initiatives threaten both expressive freedom and creative experimentation, while others worry about the social and economic costs of the copying that evades existing protections. Meanwhile, those attempting to evaluate the complex landscape of platform behavior have debated whether to count platforms as civil libertarians, rapacious appropriators of creative labor, obstructors of justice, or privatized extensions of the surveillance state.

Those debates are important, but it is also essential to consider the larger patterns that are emerging as a result of the repeated, strategic interactions between and among the competing interests. For my purposes here, two aspects of that pattern are especially worth underscoring.

First, the "new normal" in the platform-based, massively intermediated information economy is a condition in which fiat-based prohibitions on information flow are both increasingly routine and increasingly inscrutable. Even as state actors, intellectual property owners and platform firms have struggled to claim the moral high ground in particular disputes, the logics of fiat interdiction have become more closely intertwined and more resistant to disruption. Across a wide variety of contexts, the combination of powerful secrecy rules, privatization of interdiction functions, and exceptionalist procedural tactics works to shield such logics from critical interrogation.

Second, and relatedly, the landscape of arrangements for interdiction and control of information flows is only partly comprised of state mandates. Compromises that

involve voluntary filtering shift much day-to-day authority over management of information flows to platforms and at the same time make such decisions more difficult to contest. The "new normal" in the platform-based, massively intermediated information economy is a condition in which platform businesses enjoy increasing autonomy both to define the terms of their own compliance with mandates promulgated by state actors and to create and refine their own operational arrangements. The normative and practical authority of platforms—including, increasingly, their sovereign power to determine the exception—has become both something taken for granted and a powerful force reshaping the law in its own image. In Part II, we will explore the consequences of that transformation unfolding across multiple institutional domains.

---

[1] Carl Schmitt, *Political Theology*, trans. George Schwab (Cambridge, Mass.: MIT Press, 1985), 5.
[2] Kim Lane Scheppele, "Law in a Time of Emergency: States of Exceptions and the Temptations of 9/11," *University of Pennsylvania Journal of Constitutional Law* 6 no. 5 (2004): 1001-1083.
[3] Giorgio Agamben, *Homo Sacer: Sovereign Power and Bare Life*, trans. Daniel Heller-Roazen (Stanford: Stanford University Press, 1998), 51-52; see also David Dyzenhaus "*Schmitt v. Dicey*: Are States of Emergency Inside or Outside the Legal Order?," *Cardozo Law Review* 27 no. 5 (2006): 2005-2040 (elaborating a theory of legal "grey holes").
[4] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012), 31-61.
[5] For what appears to have been the first use of the term, see Timothy C. May, "Crypto Anarchy and Virtual Communities," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, Mass.: MIT Press, 2001), 67.
[6] Executive Order 12356: National Security Information, 47 Fed. Reg. 14874 (Apr. 2, 1982).
[7] Philip R. Zimmermann, "Cryptography for the Internet," *Scientific American* 279 no. 4 (1998): 110-115. For a comprehensive history of U.S. government cryptography policy, see Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, Mass.: MIT Press, 2007).
[8] Junger v. Daley, 209 F.3d 481, 484-85 (6th Cir. 2000); Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996), *aff'd sub nom.* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *withdrawn and reh'g granted,* 192 F.3d 1308 (1999).
[9] Bernstein v. U.S. Dep't of Commerce, No. C 95-0582 MHP, 2004 WL 838163, at *2, *5 n.2 (N.D. Cal. Apr. 19, 2004).
[10] For the regulations, see 15 C.F.R. § 734.17 (2017); 15 C.F.R. Pt. 774, Supp. 1, Cat. 5, Part 2 (2017). On government use of the regulations for ongoing leverage, see Avidan Y. Cover, "Corporate Avatars and the Erosion of the Populist Fourth Amendment," *Iowa Law Review* 100 no. 4 (2015): 1441, 1473-76; Michael Hirsch, "How America's Top Tech Companies Created the Surveillance State," *National Journal* (July 25, 2013), https://perma.cc/Z5T8-MSVW; Shane Harris, "Google's Secret NSA Alliance: The Terrifying Deals between Silicon Valley and the Security State," *Salon* (Nov. 16, 2014), https://perma.cc/DFR2-U3ZZ.
[11] Charles Warren, "What Is Giving Aid and Comfort to the Enemy?," *Yale Law Journal* 27 no. 3 (1918): 331-347; Gillars v. United States, 182 F.2d 962, 966 (1950). For the current version of the law, see 18 U.S.C. § 2381.
[12] For a good history of the evolution of federal antiterrorism legislation, see Robert M. Chesney, "The Sleeper Scenario: Terrorism Support Laws and the Demands of Prevention," *Harvard Journal on Legislation* 42 no. 1 (2005): 1-89. For the current version of the material support law, see 18 U.S.C. § 2339A(b).
[13] Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).
[14] David Cole, "The First Amendment's Borders: The Place of *Holder v. Humanitarian Law Project* in First Amendment Doctrine," *Harvard Law and Policy Review* 6 no. 1 (2012): 147-178
[15] For discussion of the amendments, see *Humanitarian Law Project*, 561 U.S. 1, 10-13 (2010).

[16] Elisabeth Bumiller, "Video Shows U.S. Killing of Reuters Employees," *New York Times* (Apr. 5, 2010), https://perma.cc/5U6U-DRQ3; Noam Cohen & Brian Stelter, "Airstrike Video Brings Attention to Whistle-Blower Site," *New York Times* (Apr. 6, 2010), https://perma.cc/AL47-CFP5; Garance Franke-Ruta, "Web Site Releases Video of Baghdad Attack That Killed 2 Journalists," *Washington Post* (Apr. 5, 2010), https://perma.cc/PF35-KQG5.
[17] Stephanie Strom, "Pentagon Sees a Threat from Online Muckrakers," *New York Times* (Mar. 17, 2010), https://perma.cc/2XQA-EDNU.
[18] Elisabeth Bumiller, "Army Leak Suspect Is Turned in, by Ex-Hacker," *New York Times* (June 7, 2010), https://perma.cc/X5BE-7HPR.
[19] Transcript of Oral Argument, supra note , at 42-46; Brief for the Respondents at 56, Humanitarian Law Project, 561 U.S. 1 (Nos. 08-1498, 09-89).
[20] *Humanitarian Law Project*, 561 U.S. at 37.
[21] *Humanitarian Law Project*, 561 U.S. at 32.
[22] On the construction of terrorism as an existential threat, see Wadie Said, "*Humanitarian Law Project* and the Supreme Court's Construction of Terrorism," *Brigham Young University Law Review* 2011 no. 5 (2011): 1455-1508.
[23] David Cole, "The New McCarthyism: Repeating History in the War on Terrorism," *Harvard Civil Rights-Civil Liberties Law Review* 38 no. 1 (2003): 1-30; Steven Schulman, "Victimized Twice: Asylum Seekers and the Material-Support Bar," *Catholic University Law Review* 59 no. 4 (2010): 949-964.
[24] Peter H. Lewis, "New Concerns Raised Over a Computer Smut Study," *New York Times* (July 16, 1995), https://perma.cc/YC5K-MG9L; Peter H. Lewis, "The Internet Battles a Much-Disputed Study on Selling Pornography On Line," *New York Times* (July 17, 1995), https://perma.cc/8TFF-XYY6. For the study, see Marty Rimm, "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories," *Georgetown Law Journal* 83 no. 5 (1995): 1849-1934.
[25] Communications Decency Act of 1996, Pub. L. No. 104-104, title V, § 502(a)(1)(A)-(B), 110 Stat. 133, 134-35, codified at 47 U.S.C. § 223, repealed, Higher Education Amendments of 1998, Pub. L. No. 105-244, Part H § 981, 112 Stat. 1581.
[26] Reno v. ACLU, 521 U.S. 844 (1997); Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), *aff'd*, 521 U.S. 1113 (1997). The second revision was narrowly tailored to match the contours of existing case law on obscenity, and survived. Nitke v. Gonzales, 413 F. Supp. 2d 262 (S.D.N.Y. 2005), *aff'd*, 547 U.S. 1015 (2006).
[27] See, for example, James Ball, "Silk Road: The Online Drug Marketplace that Officials Seem Powerless to Stop," *Guardian* (Mar. 22, 2013), https://perma.cc/X5K6-TAH3; Jake Swearingen, "A Year After the Death of Silk Road, Darknet Markets are Booming," *The Atlantic* (Oct. 2, 2014), https://perma.cc/C5HL-7GFZ; Cyrus Farivar, "DOJ Announces Official Takedown of AlphaBay, World's Largest Dark Web Market," *ArsTechnica* (July 20, 2017), https://perma.cc/9KKL-Y57F; Samuel Gibbs & Lois Beckett, "Dark Web Marketplaces AlphaBay and Hansa Shut Down," *Guardian* (July 20, 2017), https://perma.cc/KND3-B65Y.
[28] For work collecting and analyzing these statements, see Tarleton Gillespie, *Wired Shut: Copyright and the Shape of Digital Culture* (Cambridge, Mass.: MIT Press, 2007); John Logie, *Peers, Pirates, and Persuasion: Rhetoric in the Peer-to-Peer Debates* (Anderson, S.C.: Parlor Press, 2006).
[29] See, for example, Protecting Digital Broadcast Content: Hearing Before the House Comm. on the Judicary, Subcomm. on Courts, the Internet, and Intellectual Property, 109th Cong., 1st Sess. (Nov. 4, 2005) (testimony of Mitch Bainwol, CEO, Recording Industry Association of America); Copyright Infringement and File Sharing: Hearing Before the Sen. Comm. on the Judiciary, 109th Cong., 1st Sess. (Sept. 28, 2005) (testimony of Ali Aydar, CEO, SNOCAP); Peer-to-Peer Piracy: Hearing Before the House Comm. on the Judiciary, Subcomm. on Courts, the Internet, and Intellectual Property, 109th Cong., 1st Sess. (Sept. 22, 2005) (testimony of Richard Taylor, Senior Vice President, Motion Picture Association of America).
[30] For the copyright and trade secrecy enactments, see Uruguay Round Agreements Act, Pub. L. No. 103-465, title V, § 104(A), 108 Stat. 4809, 4976 (1994), codified as amended at 19 U.S.C. § 3511 (1998); Economic Espionage Act of 1996, Pub. L. No. 104-294, title I, § 101, 110 Stat. 3488, 3488-91 (1996),

codified as amended at 18 U.S.C. §§ 1831-1839 (2018); Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, §§ 101-102, 112 Stat. 2827, 2827-28 (1998), codified at 17 U.S.C. §§ 302-304 (2018); Digital Millennium Copyright Act, Pub. L. No. 105-304, §§ 1201-1204, 112 Stat. 2860, 2863-76 (1998), codified ads amended at 17 U.S.C. §§ 1201-1204 (2018). For the Computer Fraud and Abuse Act amendments, see Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, title XXIX, § 290001, 108 Stat. 1796, 2097-98, codified as amended at 18 U.S.C. § 1030 (2018); Economic Espionage Act of 1996, Pub. L. No. 104-249, title II, § 201, 110 Stat. 3488, 3491, codified as amended at 18 U.S.C. § 1030 (2018).

[31] Eldred v. Ashcroft, 537 U.S. 186, 221 (2003); see also Golan v. Holder, 565 U.S. 302, 329 (2012).

[32] For the most well-known series of rulings, see Universal Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 332 (S.D.N.Y. 2000), aff'd sub nom. Universal Studios, Inc. v. Corley, 273 F.3d 429, 434-35, 450-52 (2d Cir. 2001). On the framing of copyright infringement as an existential threat, see Julie E. Cohen, "Pervasively Distributed Copyright Enforcement," *Georgetown Law Journal* 95 no. 1 (2006): 1-48.

[33] Tarleton Gillespie, "Characterizing Copyright in the Classroom: The Cultural Work of Antipiracy Campaigns," *Communication, Culture and Critique* 2 no. 3 (2009): 274-318, doi:10.1111/j.1753-9137.2009.01039.x.; Logie, *Peers, Pirates, and Persuasion*.

[34] David E. Pozen, "Deep Secrecy," *Stanford Law Review* 62 no. 2 (2010): 257-340.

[35] On the origins of the privilege, see Robert M. Chesney, "State Secrets and the Limits of National Security Litigation," *George Washington Law Review* 75 nos. 5-6 (2007): 1249-1332; on its contemporary uses, see Laura K. Donohue, "The Shadow of State Secrets," *University of Pennsylvania Law Review* 159 no. 1 (2010): 77-216

[36] The modern state is so sprawling and complex that neither secrecy nor transparency is entirely feasible. Instead, as Mark Fenster shows, both secrecy and transparency are essentially performative; the state withholds or provides information according to complex sets of rules, but the results do not predictably shed light on what the state actually does. See Mark Fenster, "The Implausibility of Secrecy," *Hastings law Journal* 65 no. 2 (2016): 309-362; Mark Fenster, "Seeing the State: Transparency as Metaphor," *Administrative Law Review* 62 no. 3 (2010): 617-672. On leaks and leaking, see David E. Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review* 127 no. 2 (2013): 512-635.

[37] Lee Tien, "Foreign Intelligence Surveillance Act: Frequently Asked Questions (and Answers)," Electronic Frontier Foundation (Sept. 27, 2001), https://perma.cc/46A2-3JRV; Philip Shenon, "Traces of Terror: Counterintelligence; 'Paper Court' Comes to Life Over Secret Tribunal's Ruling on Post-9/11 Police Powers," *New York Times* (Aug. 27, 2002), https://perma.cc/KJ6N-4TMU; National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report" (July 22, 2004), chapter 3, https://perma.cc/CH6M-LARB.

[38] Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1195 (9th Cir. 2007).

[39] James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times* (Dec. 16, 2005), https://perma.cc/56M4-7ZKU; Nate Anderson, "AT&T Engineer: NSA Built Secret Rooms in our Facilities," *ArsTechnica* (Apr. 12, 2006), https://perma.cc/45U5-74L8; see also Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras & James Risen, "AT&T Helped U.S. Spy on Internet on a Vast Scale." *New York Times* (Aug. 15, 2015), https://perma.cc/2XHK-YPNQ.

[40] See Hepting v. AT&T Corp., 539 F.3d 1157 (9th Cir. 2008); Hepting v AT&T Corp., 671 F.3d 881 (9th Cir. 2012).

[41] Amnesty Int'l v. McConnell, 646 F.Supp.2d 633 (S.D.N.Y. 2009), *vacated and remanded sub nom.* Amnesty Int'l v. Clapper, 638 F.3d 118 (2d Cir. 2011), *rev'd*, 568 U.S. 398 (2013).

[42] James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired* (Mar. 15, 2012), https://perma.cc/LM2L-SS4S.

[43] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

[44] For a helpful overview of the different programs, see Julia Angwin & Jeff Larson, "The NSA Revelations All in One Chart, *ProPublica* (June 30, 2014), https://perma.cc/WA9Q-SUSB.

[45] Garrett Hatch, Congressional Research Service Report No. RL34385, "Privacy and Civil Liberties Oversight Board: New Independent Agency Status," 1-9 (Aug. 27, 2012), https://perma.cc/7H2F-KDSP.

[46] USA Freedom Act, Pub. L. No. 114-23, title I, § 101 & title IV, § 401, 129 Stat. 268, 270 & 279, codified at 50 U.S.C. §§ 1861(b)(2), (c)(3) & 1803(i) (2018).

[47] David Cunningham, *There's Something Happening Here: The New Left, The Klan and FBI Counterintelligence* (Berkeley: University of California Press, 2004); 27-41; Loch K. Johnson, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review* 64 NO. 1 (2004): 3-14 5-12.
[48] Jay Stanley, "What Powers Does the Civil Liberties Oversight Board Have?," ACLU (Nov. 4, 2013), https://perma.cc/3HQN-TUFA; Nicholas M. Horrock, "How Deeply Should the C.I.A. Be Looked Into," *New York Times* (June 22, 1975), 182.
[49] Privacy & Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted Under Sec. 215 of the USA Patriot Act & on the Operations of the Foreign Intelligence Surveillance Court" (Jan. 23, 2014), https://perma.cc/WM3Z-86NQ; Ellen Nakashima, "Independent Review Board Says NSA Phone Data Program Is Illegal and Should End," *Washington Post* (Jan. 23, 2014), https://perma.cc/R36W-UFME; Dan Roberts, "FISA Court Grants Extension of Licence for Bulk Collection of US Phone Records," *Guardian* (June 20, 2014), https://perma.cc/5BFL-RP5F; Privacy and Civil Liberties Oversight Board, "Recommendations Assessment Report" (Jan. 29, 2015), http://perma.cc/8WZ5-MG32; Spencer Ackerman, "Obama Must Finally End NSA Phone Record Collection, Says Privacy Board," *Guardian* (Jan. 29, 2015), https://perma.cc/6BK5-HRXQ; Cody M. Poplin, "NSA Ends Bulk Collection of Telephony Metadata Under Section 215," *Lawfare* (Nov. 30, 2015), https://perma.cc/E4KZ-RXUR; Privacy & Civil Liberties Oversight Board, "Recommendations Assessment Report" (Feb. 5, 2016), http://perma.cc/3ZR2-S3KP.
[50] Conor Friedersdorf, "NSA Surveillance Divides the Republican Party," *The Atlantic* (Jan. 27, 2014), https://perma.cc/D3GZ-N8ED; George Gao, "What Americans Think About NSA Surveillance, National Security, and Privacy," Pew Research Center (May 29, 2015), https://perma.cc/F726-8HCL.
[51] On the ultimate effects of the post-COINTELPRO reforms, see Brian Hochman, *All Ears: A History of Wiretapping in the United States* (Cambridge, Mass.: Harvard University Press, forthcoming).
[52] Wikimedia Fdn. v. NSA, 857 F.3d 193, 209-11, 213-15 (4th Cir. 2017); Schuchardt v. President, 839 F.3d 336, 349-54 (3d Cir. 2016); Obama v. Klayman, 800 F.3d 559, 563-64 (D.C. Cir. 2015) (opinion of Brown, J.); ACLU v. Clapper, 959 F. Supp. 2d 724, 751-56 (S.D.N.Y. 2013), *rev'd on other grounds*, 785 F.3d 787 (2d Cir. 2015); Jewel v. NSA, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015), *appeal dismissed*, 810 F.3d 622 (9th Cir. 2015).
[53] Doe v. Ashcroft, 334 F.Supp.2d 471 (S.D.N.Y. 2004), *vacated as moot sub nom*. Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006). This tactic has encountered limits, however. See Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *aff'd in part and rev'd in part sub nom.* Doe v. Mukasey, 549 F.3d 861 (2d Cir. 2008).
[54] Al-Haramain Islamic Foundation v. Bush, 451 F. Supp. 2d 1215 (D. Or. 2006), *rev'd*, 507 F.3d 1190 (9th Cir. 2007), *transferred by the Judicial Panel on Multidistrict Litigation*, *In re* National Security Agency Telecommunications Records Litigation, 564 F.Supp.2d 1109 (N.D. Cal. 2008).
[55] In re National Security Agency Telecommunications Records Litigation, 700 F. Supp. 2d 1182 (N.D. Cal. 2010), *rev'd sub nom.* Al-Haramain Islamic Foundation v. Obama, 705 F.3d 845 (9th Cir. 2012).
[56] Tim Cushing, "Government Drops Facebook Search Warrant Gag Order at Eleventh Hour," *TechDirt* (Sept. 18, 2017), https://perma.cc/855K-NQ47; Raymond Bonner, "The FBI Checked the Wrong Box and a Woman Ended Up on the Terrorism Watch List for Years," *ProPublica* (Dec. 15, 2015), https://perma.cc/L2ZH-ZBUZ; Jessica Glenza & Nicky Woolf, "Stingray Spying: FBI's Secret Deal with Police Hides Phone Dragnet from Courts," *Guardian* (Apr. 10, 2015), https://perma.cc/7AZ2-6KB5; see also Human Rights Watch, "Dark Side: Secret Origins of Evidence in US Criminal Cases" (Jan. 9, 2018), https://perma.cc/L54M-ELZB.
[57] Rodney A. Smolla, "Information as Contraband," *Northwestern University Law Review* 96 no. 3 (2002): 1099-1176.
[58] Wesley Newcomb Hohfeld, "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning," *Yale Law Journal* 23 no. 1 (2013): 16-59, 44-54.
[59] Robert Cannon, "The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway," *Federal Communications Law Journal* 49 no. 1 (1996): 51-94.
[60] Trotter Hardy, "Criminal Copyright Infringement," *William and Mary Bill of Rights Journal* 11 no. 1 (2002): 305-342.

[61] 47 U.S.C. § 230(e)(2) (2018); Federal Communications Commission, Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,738, ¶¶ 113, 304 (Apr. 13, 2015), *repealed by* Restoring Internet Freedom, 83 Fed. Reg. 7852 (Feb. 22, 2018); Preserving the Open Internet, 25 F.C.C.R. 17905, ¶¶ 107, 111 (Dec. 23, 2010), *vacated in part by* Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

[62] On the characteristics of takedown notices, see Laura Quilter & Jennifer Urban, "Efficient Process or 'Chilling Effects'? Takedown Notices under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer and High Technology Law Journal* 22 no. 4 (2005): 621-694; Wendy Seltzer, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment," *Harvard Journal of Law and Technology* 24 no. 1 (2010): 171-232. On the trade strategy, see Markham Erickson, & Sarah C. Leggin, "Exporting Internet Law through International Trade Agreements: Recalibrating U.S. Trade Policy for the Internet Age," *Catholic University Journal of Law and Technology* 24 no. 2 (2016): 317-368.

[63] See, for example, UMG Recordings v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012); Perfect 10, Inc. v. Visa Int'l Service Ass'n, 494 F.3d 788 (9th Cir. 2007).

[64] On the populist backlash against maximalist copyright, see Bill Herman, *The Fight Over Digital Rights: The Politics of Copyright and Technology* (New York: Cambridge University Press, 2013). On platforms' appropriation of anti-maximalist rhetoric, see Sean M. O'Connor, "Creators, Innovators, & Appropriation Mechanisms," *George Mason Law Review* 22 no. 4 (2015): 991-96; Tom Slee, *What's Yours Is Mine: Against the Sharing Economy* (New York, OR Books, 2017), 109-138; see also Guy Pessach, "Beyond IP—The Cost of Free: Informational Capitalism in a Post IP Era," *Osgoode Hall Law Review* 54 no. 1 (2016): 225-251. For examples of failed legislative efforts, see Consumer Broadband and Digital Television Promotion Act of 2002, Proposed Bill No. S. 2048, 107th Congress, 2nd Session; Digital Transition Content Security Act of 2005, Proposed Bill No. H.R. 4569, 109th Congress, 2nd Session; and Audio Broadcast Flag Licensing Act of 2006, Proposed Bill No. H.R. 4861, 109th Congress, 2nd Session. But see Federal Communications Commission, Commercial Availability of Navigation Devices and Compatibility between Cable Systems and Consumer Electronics Equipment, 68 Fed. Reg. 66,728 (Nov. 28, 2003) (incorporating copy-protection requirement into cable plug-and-play standard).

[65] See Jonathan Weisman, "In Fight Over Piracy Bills, New Economy Rises Against Old," *New York Times* (Jan. 18, 2012), https://perma.cc/6UDK-WEVQ; "SOPA/PIPA: Internet Blacklist Legislation," Electronic Frontier Foundation, https://perma.cc/L8BA-MVFB.

[66] In 2014, the American Bar Association's Intellectual Property Section issued a report that included recommendations for stricter interdiction mandates, which Congress uncharacteristically has ignored. Section of Intellectual Property Law, American Bar Association, "A Section White Paper: A Call for Action for Online Piracy and Counterfeiting Legislation" (2014), http://perma.cc/9GCY-3D3D; see also Mike Masnick, "The Rebranding of SOPA: Now Called 'Notice and Staydown'," *TechDirt* (Mar. 14, 2014), https://perma.cc/GHC9-JQUX.

[67] Jack Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation," *U.C. Davis Law Review* 51 no. 3 (2017): 1149-1210, 1177-79. On the implications of private-sector automated enforcement initiatives in copyright and other areas, see Annemarie Bridy, "Internet Payment Blockades," *Florida Law Review* 67 no. 5 (2015): 1524-1568; Annemarie Bridy, "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement," *Oregon Law Review* 89 no. 1 (2010): 81-132.

[68] "An Update to Our Search Algorithms," *Inside Search*, Google (Aug. 10, 2012), https://perma.cc/RG4F-B3US; see also "Continued Progress on Fighting Piracy," *Public Policy Blog*, Google (Oct. 17, 2014), https://perma.cc/5J2M-Y5WB; Adi Robertson, "Google Rolling out New Search Update to Downrank 'Most Notorious' Pirate Sites," *Verge* (Oct. 17, 2014), https://perma.cc/R6HZ-ZQYC; James Titcomb, "Google and Microsoft Agree Crackdown on Illegal Downloads," *Telegraph* (Feb. 20, 2017), https://perma.cc/NA4V-FQSV.

[69] Joe Silver, "Viacom and Google Settle $1 Billion YouTube Lawsuit," *ArsTechnica* (Mar. 18, 2014), https://perma.cc/8RSV-5V7H.

[70] Between 2004 and 2009, the Recording Industry of America filed over 30,000 lawsuits against individual users, settling most of the lawsuits for an average of $3500-$4500 each. See Steve Karnowski, "Facing the Music," *USA Today* (June 19, 2009); Justin Hughes "On the Logic of Suing One's Customers and the

Dilemma of Infringement-Based Business Models," *Cardozo Arts and Entertainment Law Journal* 22 no. 3 (2005): 725-766.

[71] Scarlet Extended SA v. Societe belge des auteurs, compositeurs et editeurs SCRL (SABAM), [2012] E.C.D.R. 4, ¶45 (discussing conflicting legal directives and concluding that courts "must strike a fair balance" between them).

[72] Copyright Felony Act, Pub. L. No. 102-561, 106 Stat. 4233 (1992), codified as amended at 18 U.S.C. § 2319 (2018); Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 320104, 108 Stat. 1796, 2110-2111 (1994), codified as amended at 18 U.S.C. § 2320 (2018); Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, § 5, 110 Stat. 1386, 1387 (1996), codified as amended at 18 U.S.C. § 2320 (2018); No Electronic Theft (NET) Act, Pub. L. No. 105-147, § 2, 111 Stat. 2678, 2678-80 (1997), codified as amended at 18 U.S.C. §§ 2319, 2319A, 2320 (2018); Intellectual Property Protection and Courts Amendments Act of 2004, Pub. L. No. 108-482, § 102, 118 Stat. 3912, 3912-15 (2004), codified as amended at 18 U.S.C. § 2318 (2018); Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, §§ 102-103, 119 Stat. 218, 218-21 (2005), codified as amended at 18 U.S.C. §§ 2319, 2319B (2018); Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, 120 Stat. 285 (2006), codified as amended at 18 U.S.C. § 2320 (2018); Prioritizing Resources and Organization for Intellectual Property Act, Pub. L. No. 110-403, §§ 202-206, 122 Stat. 4256, 4260-63 (2008), codified as amended at 18 U.S.C. §§ 2318-2320, 2323 (2018); Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, § 717, 126 Stat. 993, 1076-77 (2012), codified as amended at 18 U.S.C. § 2320 (2018); see also Digital Millennium Copyright Act, Pub. L. No. 105-304, §§ 1201-1204, 112 Stat. 2860, 2863-76 (1998), codified as amended at 17 U.S.C. § 1204 (2018).

[73] For a critical analysis, see Christophe Geiger, "Towards a balanced international legal framework for criminal enforcement of intellectual property rights," in *TRIPS plus 20: From Trade Rules to Market Principles*, eds. Hans Ullrich, et al. (New York: Springer, 2016), 645-679.

[74] See Philip S. Corwin, "MegaBust's MegaQuestions Cloud the Net's Future, *CircleID* (Feb. 13, 2012), https://perma.cc/BF7Y-BLE3; Greg Kumparak, "How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking at Your Stuff), *TechCrunch* (Mar. 30, 2014), https://perma.cc/XF2W-SU2F. For reports on enforcement activities in the U.S., see U.S. Dept. of Justice, "Pro-IP Act: Annual Report FY 2016," (Jan. 12, 2017), https://perma.cc/6EUN-2FHG; U.S. Dept. of Justice, "Pro-IP Act Annual Report FY 2015," (Apr. 29, 2016), https://perma.cc/8D7X-9AZH; Fed. Bureau of Investigation, "FBI Fiscal Year 2015 Report to Congress on Intellectual Property Rights Enforcement," https://perma.cc/W9D3-F7TG; Fed. Bureau of Investigation, "Federal Bureau of Investigation Pro-IP Act Annual Report 2014," https://perma.cc/NX5C-8RTV.

[75] Digital Millennium Copyright Act, Pub. L. No. 105-304, § 1201, 112 Stat. 2860, 2863-65 (1998), codified as amended at 17 U.S.C. § 1201 (2018).

[76] Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012), 202-07.

[77] For an overview (and a call for more empirical investigation), see Justin Hughes, "Motion Pictures, Markets, and Copylocks," *George Mason Law Review* 23 no. 4 (2016): 941-966; on the processes by which technical protection systems become implemented and normalized, see Cohen, *Configuring the Networked Self*, 158-64, 193-99.

[78] Cecilia Kang, "FCC Delays Vote on Cable Set-Top Boxes," *New York Times* (Sept. 29, 2016), https://perma.cc/LUT7-RAD6; Jon Brodkin, "FCC Chairman Pai Takes Wheeler's Set-Top Box Plan Off the Table," *ArsTechnica* (Jan. 30, 2017), https://perma.cc/92RD-8FUM.

[79] 17 U.S.C. § 1201(f), (g), (j) (2018).

[80] Wendy Seltzer, "The Imperfect Is the Enemy of the Good: Anticircumvention versus Open User Innovation," *Berkeley Technology Law Journal* 25 no. 2 (2010): 909-972; see also Cohen, *Configuring the Networked Self*, 209-13.

[81] See 17 U.S.C. § 1201(a)(1) (2018); U.S. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies: Final Rule, 65 Fed. Reg. 64,556, 64,558 (Oct. 27, 2000).

[82] For the results of the triennial rulemakings, see U.S. Copyright Office, "Rulemaking Proceedings under Section 1201 of Title 17," https://perma.cc/N4UQ-9QHS (last visited June 12, 2019).

[83]David Kravets, "Industry, and Apple, Opposing 'Right to Repair' Laws," *ArsTechnica* (Mar. 7, 2017), https://perma.cc/F8BY-V955; Kyle Wiens, "You Bought that Gadget, and Damnit, You Should Be Able to Fix it," *Wired* (Mar. 22, 2017), https://perma.cc/CW6E-AMQM. For analysis of the underlying legal and philosophical issues, see Joshua T. Fairfield, *Owned: Property, Privacy, and the New Digital Serfdom* (New York: Cambridge University Press, 2017), 186-99; Aaron Perzanowski & Jason Schultz, *The End of Ownership: Personal Property in the Digital Economy* (Cambridge, Mass.: MIT Press, 2016), 121-54.

[84] The Supreme Court has identified intent to profit from infringement and platform design as factors to be considered in contributory infringement analysis. Large, diversified technology companies can point to all of the different services that they offer, see Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 939-40 (2005), but smaller firms tend to be optimized for the functionality that prompted litigation in the first place.

[85] See, for example, Macon Phillips, "Obama Administration Responds to We the People Petition on SOPA and Online Piracy," *White House Blog* (Jan. 14, 2012), http://perma.cc/TRS-8Y4A; Letter from Hillary Rodham Clinton, Sec. of State, to Rep. Howard L. Berman (Oct. 25, 2011), http://perma.cc/K9LP-SYRA.

[86] Chris Welch, "Russia, China, and Other Nations Draft Proposal to Give ITU Greater Influence over the Internet," *Verge* (Dec. 9, 2012), https://perma.cc/M8RY-QLDL; Matt Smith, "Russia Backs Down on proposals to Regulate the Internet," *Reuters* (Dec. 10, 2012), https://perma.cc/X5FJ-TF43.

[87] Steven Levy, "Battle of the Clipper Chip," *New York Times Magazine* (June 12, 1994), https://perma.cc/AE2C-36L4; Danielle Kehl et al., "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," New America Cybersecurity Initiative (June 17, 2015), 5-11, https://perma.cc/M56H-9HUZ.

[88] Ryan Gallagher, "Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide," *Intercept* (Dec. 4, 2014), https://perma.cc/A64Z-DKLJ; Ryan Gallagher & Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware," *Intercept* (Mar. 12, 2014), https://perma.cc/B4KE-UD5E; Barton Gellman & Ashkan Soltani, "NSA 'Hacked Google and Yahoo's Data Centre Links', Snowden Documents Say," *Independent* (Oct. 30, 2013), https://perma.cc/KR9E-5XTS

[89] George Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson," *Intercept* (July 24, 2015), https://perma.cc/9F9M-BBUP*;* Glenn Greenwald & Murtaza Hussain, "Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On," *Intercept* (July 9, 2014), https://perma.cc/3GFB-PFKF; Michael German & Sara Robinson, "Wrong Priorities on Fighting Terrorism," Brennan Center for Justice at New York University School of Law (Oct. 31, 2018), https://perma.cc/MKP6-T24A.

[90] "GNI Principles on Freedom of Expression and Privacy," Global Network Initiative, https://perma.cc/J32J-GMXB (last visited Apr. 8, 2019); see MacKinnon, *Consent of the Networked*, 138-39, 179-82.

[91] Julian Hattem & Mario Trujillo, "Silicon Valley Fights to Lift 'Gag Orders'," *The Hill* (Oct. 11, 2014), http://perma.cc/WD7B-TDSR; Tim Cook, Apple CEO, "A Message to Our Customers" (Feb. 16, 2016), http://perma.cc/9VYP-WCLZ.

[92] USA Freedom Act, Pub. L. 114-23, §101, 129 Stat. 270 (2015), codified at 50 U.S.C. § 1861(b)(2) & (c)(3) (2018).

[93] Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238 (2014) (Grand Chamber, CJEU); Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J. L 119/89.

[94] Kevin Poulsen, "Apple's IPhone Encryption is a Godsend, Even if Cops Hate it," *Wired* (Oct. 8, 2014), https://perma.cc/GC98-YGPL; Joseph Cox, "Encryption is Going Mainstream, but Will People Actually Use It?," *Vice Motherboard* (Aug. 21, 2014), https://perma.cc/8CKX-3XBZ; Matthew Panzarino, "Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy," *TechCrunch* (Jun. 2, 2015), https://perma.cc/98LT-5JF4; Cade Metz, "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People," *Wired* (April 5, 2016), https://perma.cc/CJF4-9ZGK.

[95] "An Encryption Tightrope: Balancing Americans' Security and Privacy," Hearing Before the H. Comm. on the Judiciary, 114th Cong., 2d Sess. 14-15 (2016) (statement of James Comey, Director, FBI); American

Civil Liberties Union, "All Writs Act Orders for Assistance from Tech Companies", https://perma.cc/V8B8-XTU2 (last visited June 17, 2018); Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1(1) (2015): 69-79; Sara Sorcher, "The Battle Between Washington and Silicon Valley Over Encryption," *Christian Science Monitor: Passcode* (July 7, 2015), http://perma.cc/B6Y4-DFHQ.

[96] Neil Sheehan, "Pentagon Study Traces 3 Decades of Growing U.S. Involvement," *New York Times* (June 13, 1971), 1; Floyd Abrams, *Friend of the Court: On the Front Lines with the First Amendment* (New Haven: Yale University Press, 2013), 137-146.

[97] New York Times Co. v. United States, 403 U.S. 713, 717 (1971).

[98] Martin Arnold, "Pentagon Papers Charges are Dismissed; Judge Byrne Frees Ellsberg and Russo, Assails 'Improper Government Conduct,'" *New York Times* (May 12, 1973), 1; Abrams, *Friend of the Court*, 143.

[99] Espionage Act of 1917, Pub. L. 104-294, title VI, § 602(c), 110 Stat. 3503, codified as amended at 18 U.S.C.A. § 798 (2018).

[100] Charlie Savage, "Soldiers' Lawyers Rest Case with Defense of WikiLeaks' Journalistic Role," *New York Times* (July 10, 2013), https://perma.cc/BR8B-RE9R; Ed Pilkington, "Bradley Manning Verdict: Cleared of 'Aiding the Enemy' but Guilty of Other Charges," *Guardian* (July 31, 2013), https://perma.cc/79RR-ZVQN; Paul Lewis, "Bradley Manning Given a 35-Year Prison Term for Passing Files to Wikileaks," *Guardian* (Aug. 21, 2013), https://perma.cc/347C-X9V3. President Obama later commuted the sentence to the seven years Manning had already served. Charlie Savage, "Chelsea Manning to Be Released Early as Obama Commutes Sentence," *New York Times* (Jan. 17, 2017), https://perma.cc/Z2DC-467X. On the ways that the Espionage Act has functioned as a tool for censorship and preservation of government secrecy, see Yochai Benkler, A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate," *Harvard Civil Rights-Civil Liberties Law Review* 46 no. 2 (2011): 311-398; Cole, "The New McCarthyism."

[101] Ewen MacAskill, "The Long Arm of US Law: What Next for Edward Snowden," *Guardian* (Dec. 2, 2013), https://perma.cc/VB9G-AW6K; Shaun Walker, "Edward Snowden's Leave to Remain in Russia Extended for Three Years," *Guardian* (Jan. 18, 2017), https://perma.cc/PQV5-D8AA.

[102] Krishnadev Calamur, "Who Is Reality Winner?," *The Atlantic* (June 6, 2017), https://perma.cc/4RYZ-C9GY.

[103] Andy Greenberg, "Snowden's Chronicler Reveals Her Own Life Under Surveillance," *Wired* (Feb. 4, 2016), https://perma.cc/W2S2-8VFZ; Andy Greenberg, "Anonymous' Barrett Brown Is Free—And Ready to Pick New Fights," *Wired* (Dec. 21, 2016), https://perma.cc/7J56-FYE4; David Gilbert, "Wanted Man: The U.S. Now Says Arresting Julian Assange Is A Priority," *Vice News* (Apr. 21, 2017), https://perma.cc/NTR6-EJP9; Charlie Savage, Adam Goldman, & Michael S. Schmidt, "Assange Is Secretly Charged in U.S., Prosecutors Mistakenly Reveal," *New York Times* (Nov. 16, 2018), https://perma.cc/V8HQ-CVDA.

[104] Alan Rusbridger, WikiLeaks: "The Guardian's Role in the Biggest Leak in the History of the World," *Guardian* (Jan. 28, 2011), https://perma.cc/LU6R-F8RT; Bill Keller, "Dealing with Assange and the WikiLeaks Secrets," *New York Times* (Jan. 26, 2011), https://perma.cc/XP5Y-525Z; "A Note to Readers: Piecing Together the Reports, and Deciding What to Publish," *New York Times* (July 25, 2010), https://perma.cc/Q9B6-P7DS. For additional discussion of those efforts and of the institutional design questions surrounding WikiLeaks more generally, see Chapter 8, pp. 254-57.

[105] 5 U.S.C. § 552(b)(4) (2018).

[106] 18 U.S.C. §§ 1331-1331 (2018).

[107] Donohue, "The Shadow of State Secrets"; Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System," *Stanford Law Review* 70 no. 5 (2018): 1343-1429.

[108] Ashlee Vance, "WikiLeaks Struggles to Stay Online after Attacks," *New York Times* (Dec. 3, 2010), https://perma.cc/HJ2S-5LFY; Bianca Bosker, "PayPal Admits State Department Pressure Caused It to Block WikiLeaks," *Huffington Post* (Dec. 8, 2010), https://perma.cc/V8BU-TCN5.

[109] See Sian Sullivan, Andre Spicer, & Steffen Bohm, "Becoming Global (Un)Civil Society: Counter-Hegemonic Struggle and the IndyMedia Network," *Globalizations* 8 no. 5 (2011):703-717.

[110] On the provisions of national security letters, see. Hannah Bloch-Webha, "Process Without Procedure: National Security Letters and First Amendment Rights," *Suffolk University Law Review* 39 no. 3 (2016):

367-408, 374-77. On state licensing, see George F. Will, "Oregon Is Suing Engineers for … Speaking Up about Engineering?," *Washington Post* (June 7, 2017), https://perma.cc/3A6M-VYNU.

[111] Compare Nate Cardozo, et al., "Who Has Your Back? 2017," Electronic Frontier Foundation (July 2017), https://perma.cc/S8YH-K9NN, with Cover, "Corporate Avatars"; Niva Elkin-Koren & Eldar Haber, "Governance by Proxy: Cyber Challenges to Civil Liberties," Brooklyn Law Review 82 no. 1 (2017): 105-162. On warrant canaries, see Naomi Gilens, "The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures," *Harvard Journal of Law and Technology* 28 no. 2 (2015): 525-548; Rebecca Wexler, "Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders," *Yale Law Journal Forum* 124 (2014): 158-179. On national security letters more generally, see Bloch-Webha, "Process Without Procedure."

[112] Quinta Jurecic, "EDNY Dismisses Suits Against Facebook on Hamas Attacks," *Lawfare* (May 18, 2017), https://perma.cc/P9YE-NW2J; Alexis Kramer, "Google Not Liable for Placing Ads Next to IS Videos," *Bloomberg* (Oct. 24, 2017), http://perma.cc/6CW2-V4X6; Eric Goldman, "Fourth Judge Says Social Media Sites Aren't Liable for Supporting Terrorists–Pennie v. Twitter," *Technology & Marketing Law Blog* (Dec. 10, 2017), http://perma.cc/AG5B-6JL4; David Kimball-Stanley, "Summary: Ninth Circuit Dismisses Civil Suit Against Twitter for ISIS Attack," *Lawfare* (Feb. 6, 2018), http://perma.cc/ZSJ5-8GRJ.

[113] For a summary of the German legislation and links to the texts of the German legislation and the proposed Russian law, see "Germany: Flawed Social Media Law," Human Rights Watch (Feb. 14, 2018), https://perma.cc/K77K-5EE3; for the European proposal, see Proposal for a Regulation of the European Parliament and of the Council on Preventing the Spread of Terrorist Content Online, COM(2018) 640 final, https://perma.cc/3MJ4-QABY. For a representative example of the U.S. response with links to some other examples, see Mike Masnick, "If You're Worried about Bad EU Internet Regulation, Just Wait Till You See the New Terrorist Regulation," *TechDirt* (Dec. 13, 2018), https://perma.cc/5VQA-BN7X; Citron, "Extremist Speech, Compelled Conformity, and Censorship Creep," *Notre Dame Law Review* 93 no. 3 (2018): 1035-1071.

[114] Mario Trujillo, "Tech Groups Try to Kill Terrorist Reporting Mandate in Spy Bill," *The Hill* (Aug. 5, 2015), http://perma.cc/J6C9-ADH3; Julian Hattem, "Spy Panel Drops Controversial Mandate on Web Firms, Amid Pressure," *The Hill* (Sept. 21, 2015), http://perma.cc/37HY-7NPG; Devlin Barrett & Damian Paletta, "Top U.S. Officials to Meet with Tech CEOs on Terror Concerns," *Wall Street Journal* (Jan. 7, 2016), https://perma.cc/LJC4-JQPC; Matt Burgess, "Facebook, YouTube, Twitter, and Microsoft Have Teamed Up to Fight Online Terrorism," *Wired* (June 27, 2017), https://perma.cc/YQT8-9H93; Sam Levin, "Tech Giants Team Up to Fight Extremism Following Cries that they Allow Terrorism," *Guardian* (June 26, 2017), https://perma.cc/X7FZ-ZKDH.

[115] Cyrus Farivar, "French Investigators to Work Directly with Facebook to Monitor Hate Speech," *Ars Technica* (Nov. 12, 2018), https://perma.cc/DCJ6-RMQA.

[116] See, for example, Casey Newton, "Facebook Makes Its Community Guidelines Public and Introduces an Appeals Process," *The Verge* (Apr. 24, 2018), https://perma.cc/Q63V-AVSU. For the leaked documents, see "How Facebook Guides Moderators on Terrorist Content," *Guardian* (May 24, 2017), https://perma.cc/Q28S-HL2X. On earlier, piecemeal disclosures, see Jeffrey Rosen, "Google's Gatekeepers," *New York Times Magazine* (Nov. 28, 2008), https://perma.cc/99Z2-JRL3; Sarah T. Roberts, "Social Media's Silent Filter," *The Atlantic* (Mar. 8, 2017), https://perma.cc/4DPE-4ATH; Gillespie, "Governance of and by Platforms"; Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech," *Harvard Law Review* 131 no. 6 (2018): 1598-1670. For more recent and comprehensive disclosures, see "Community Standards," Facebook, http://perma.cc/33YQ-UM82; "Video, Photos & Presentations," Content Moderation at Scale, https://perma.cc/XNF3-6ULW.

[117] On copyright takedowns, see, for example, "Transparency Report," Google, http://perma.cc/R9BZ-G372; "Search: Twitter," Lumen, (224,467 results through June 26, 2018) (last visited Apr. 8, 2019), https://perma.cc/A6TJ-2PUE. On other takedowns, see Sarah Perez, "Facebook's New Transparency Report Now Includes Data on Takedowns of 'Bad' Content, Including Hate Speech," *TechCrunch* (May 15, 2018), http://perma.cc/YCV9-UM2F.

[118] For those presentations, see "Video, Photos & Presentations," Content Moderation at Scale, https://perma.cc/XNF3-6ULW (last visited Apr. 8, 2019).