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

Chapter 8
The Future(s) of Fundamental Rights

"Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."

-- John Perry Barlow, "A Declaration of the Independence of Cyberspace"

For some commentators on the emerging informational economy, the prospect of continued and ever more severe regulatory destabilization is a joyous one—a necessary period of disruption en route to a more perfectly free (and substantially deregulated) digital future. Although many digital entrepreneurs and information-economy pundits self-identify as iconoclasts, that view of the digital networked world has a very traditional pedigree. Writing at the dawn of the digital era, self-appointed cyber-philosopher John Perry Barlow proclaimed cyberspace to be a new domain of pure freedom. Addressing the nations of the world, he cautioned that their laws, which were "based on matter," simply did not speak to conduct in the new virtual realm.[1] As Barlow himself recognized, that was not so much a statement of fact as it was an exercise in deliberate utopianism. But it has proved prescient in a way that he certainly did not intend. The "laws" that increasingly have no meaning in online environments include not only the mandates of market regulators but also the guarantees that supposedly protect the fundamental rights of internet users, including the expressive and associational freedoms whose supremacy Barlow asserted.

This chapter considers the effects of digital disruption on the recognition and enforcement of fundamental human rights. It maps three overlapping and mutually reinforcing sets of trends.

First, traditional mechanisms for defining and enforcing human rights have begun to unravel. New, hybrid modes of infringement that involve private economic power and privately developed surveillance infrastructures and information services play an important part in that shift, but other changes set in motion by the movement to informational capitalism are equally important. Highly informationalized forms of rights discourse and practice that link human rights to development and sustainability have confronted difficult implementation challenges, and new techniques for data-driven, algorithmic surveillance and control also have proved powerfully resistant to traditional forms of human rights oversight. Meanwhile, like the other evolving institutional formations that Part II has studied, evolving institutional formations for human rights practice have been progressively overtaken by the managerial turn, increasingly emphasizing "corporate social responsibility" over more stringent accounts of moral and legal obligation and deferring to opaque and often privatized arrangements for expert supervision of algorithmic processes.

Second, the vision of a cyberutopian golden age that Barlow so vividly described has proved a mirage. The internet activists and communities that took up Barlow's call quickly grasped the transformative potential of new technological capabilities for expression, association, and bottom-up organization. As we have seen throughout this book, however, they failed to reckon with the equally transformative potential of informational capital, and they also have consistently ignored or downplayed the human capacity for malice and mayhem. The chapter's middle section revisits those failures. Networked digital information technologies enable new kinds of communication but also supply new infrastructural points of control; platform-based, massively intermediated media infrastructures both facilitate and co-opt bottom-up cultural and political production; and algorithmic intermediation processes optimized for behavioral tuning and user engagement amplify both benevolence and malevolence. It has become increasingly apparent that functioning legal institutions have an indispensable role to play in protecting and promoting fundamental human rights in the networked information era.

Finally, the chapter considers a cluster of emergent discourses about the nature and importance of fundamental rights that reinforce the normative authority of powerful, nonhuman actors. Within the political economies of the global North, the turn to neoliberal governmentality has produced forms of rights discourse that invite cooptation by corporate entities seeking to privilege their own profit-making activities. An alternative way of conceptualizing the political economy of informationalism, ascendant in China and gaining ground globally, emphasizes instead the virtues of publicness, accountability, and cooperation with state authority. Under both approaches, the fundamental rights of human beings and communities—to flourishing, self-determination, and the hope of a sustainable future—are afterthoughts.

Institutions Unmoored

In the networked digital age, protections for fundamental human rights have begun to fail comprehensively. Practically speaking, private economic interests wield increasing power over the conditions of human freedom. In particular, surveillant assemblages that combine private and public elements have effectively disintermediated traditional, state-centered mechanisms for protecting rights to privacy, freedom of expression, and freedom of association while at the same time facilitating new modes of infringement with unprecedented scope and reach.[2]

Other challenges are conceptual and institutional. Critics of traditional, liberty-based rights frameworks have asserted (or reasserted) the importance of resource distribution, collective self-determination, and environmental sustainability for human flourishing. At the same time, platform-based, massively intermediated information systems have destabilized long-standing assumptions about the material conditions of possibility for privacy, intellectual freedom, and political self-determination. Both developments have underscored the inadequacies of traditional, court-centered approaches to defining and vindicating rights claims. They also have created points of entry for new discourses and practices organized around managerial and technical expertise and neoliberalized assertions of corporate social responsibility.

Intermediating Freedom and Evading Review

Around the world, new patterns of mobility, networked communication, and networked economic power have thrown traditional, state-centered paradigms for human rights definition and enforcement into disarray. Embodied subjects encounter threats to life and liberty as they move across borders and between sovereign territories. Flows of networked communications also cross borders, and states can act remotely on those communications and their traces in ways that affect the people with whom they are associated regardless of where in physical space those people happen to be located.[3] Powerful transnational corporations that channel global flows of information and other resources wield increasing power, including sometimes the power of life or death, over the individuals and communities whom those flows affect. And the pervasive *entanglement* of corporate and state surveillance activity has left existing treaty and constitutional frameworks unable to constrain either public or private surveillance power in any meaningful way.

Concern about the unaccountability of private economic power is a long-standing theme within human rights scholarship and activism. Within domestic and international discourses about fundamental human rights, the paradigmatic legal guarantees are those that structure sovereign states' dealings with embodied subjects located within their territorial borders. According to theory, state obligations to protect fundamental rights flow from the sovereign monopoly over the use of violence, simultaneously acknowledging that monopoly and subjecting it to limits.[4] That way of reasoning about the primacy of state power does not allow for the possibility of private power over the conditions of human freedom, and it has produced human rights institutions that speak to private power indirectly, if at all. In some countries, including the United States, constitutional restrictions apply only to government actors. Although some human rights instruments, such as the European Convention on Human Rights, purport to encompass both state and private conduct, they do not authorize enforcement directly against private companies. In 2008, the United Nations Secretary-General appointed a Special Representative to supervise the development of a framework and a set of guiding principles intended to nudge multinational corporations toward behavior more consistent with existing human rights norms. Guiding principles and special reports intended to constrain corporate conduct have no independent legal force, however, and the unprecedented power of capital over the conditions of human freedom has continued to grow.[5] In particular, giant transnational corporations that construct global networked supply chains wield vast power over their workers and the surrounding communities.

More recently, the unaccountability of private communications intermediaries has become a topic of special concern. By the mid-2000s the importance of the internet for communication, political self-determination, and economic opportunity—and the correspondingly powerful positions enjoyed by internet intermediaries—had become impossible to ignore. At the same time, a growing chorus of industry observers had begun to argue that internet platforms' easy adaptability to networked surveillance was an urgent global problem. Pointing to a series of unnerving events—including the Chinese government's enlistment of Yahoo! and Google to identify dissenters and block communication about prohibited topics, the Saudi and Iranian regimes' use of server-level firewalls to control internet traffic into and out of their countries, and Egyptian and

Libyan governments' use of server-level surveillance capabilities to identify and target citizens using social media for political organizing—they urged technology firms, democratic regimes, and transnational human rights institutions to institute more effective protections for communicative rights and freedoms in the networked digital environment.[6] The Global Network Initiative (GNI), founded in 2008 by a coalition of platform firms, academics, and human rights NGOs, represented an attempt both to coordinate resistance to censorship demands by authoritarian states and to respond to criticisms levied at platforms for acceding to such demands. The United Nations also initiated what become a series of special reports dealing with the power of information intermediaries and the threats that counterterrorism efforts pose to fundamental rights and liberties.[7] Compliance with the GNI's principles and the special rapporteurs' recommendations, however, remains voluntary and inconsistent.

Some academic commentators argue that privately operated communications providers fulfill an important separation of powers function without which the potential for human rights abuses would be far greater, but the evidence supporting that proposition is mixed at best.[8] As we saw in Chapter 4, to the extent that courts have engaged at all with questions about the legality of programmatic state surveillance of networked communications, resistance by communications intermediaries has been instrumental in helping to frame the legal challenges. Information technology firms also have rightly chastised governments for developing (and, inevitably, losing control of) exploits that jeopardize network security.[9] But communications intermediaries—including especially the dominant global platform firms—also have complied with surveillance and censorship requests by host governments around the world.

Even more basically, arguments about the essential structural role of communications intermediaries fail to consider those intermediaries' roles in the construction of sociotechnical assemblages for data harvesting, behavioral microtargeting, and maximizing user engagement. State-centered conceptions of protection for fundamental rights and freedoms sit uneasily alongside a reality in which flows of information to, from, and about network users are intermediated by and through privately owned and operated communications infrastructures and platforms, and in which those flows encompass information of an astonishing variety, granularity, and intimacy.

The vast and growing extent of commercial surveillance facilitates a pervasive entanglement of public and private power, producing a practical reality within which each feeds off the other and neither can be effectively constrained. Post-Snowden, collection and analysis of data generated by networked communications intermediaries have become acknowledged pillars of national security surveillance. The ready availability of data generated by networked communications intermediaries also has begun to alter ordinary law enforcement practice. In the U.S., for example, police have begun issuing subpoenas to communications intermediaries to identify the owners of all mobile devices who were near the scenes of crimes in progress, and police departments in a growing number of cities use predictive policing tools supplied by private vendors to predict the likelihood of individuals' becoming involved in violent crimes.[10] New data-driven assertions of power that blend private self-interest and public force in varying combinations range from intensive surveillance and repression of minority and dissident

populations to state-sponsored disinformation campaigns designed to weaken democratic institutions and regimes.[11] Private employers, meanwhile, use a variety of networked digital surveillance technologies to monitor the productivity, health, communications, and political activities of their employees and contractors, and private economic interests and political organizations exploit platform-based capabilities for content targeting for their own purposes.[12]

The continued ascendancy of private economic power and the deepening entanglement of public and private surveillance power leave populations worldwide simultaneously exposed to new threats and cut off from traditional institutional mechanisms for vindicating the rights that are threatened. These developments are combining to constitute the spaces of transnational economic activity and networked digital communication as spaces devoid of protections for vital human rights and freedoms—even as the activities conducted in those spaces become more and more fundamental to the exercise of those rights and freedoms.

Networks and Standards Revisited

Other challenges to traditional paradigms for human rights definition and enforcement involve alternative forms of rights discourse and contestation over the practices those discourses might require. In particular, important strands of discourse about the necessary conditions for human flourishing and a sustainable future hold that securing human rights for all of the world's peoples requires moving beyond liberty-based, individualistic formulations of fundamental rights to frameworks that encompass a broader variety of economic, institutional, and environmental factors. Within the model of network-and-standard-based governance developed in Chapter 7, those discourses represent efforts to redefine the standards at the core of transnational human rights practice. Such efforts have struggled, however, to gain an institutional foothold. Traditional, court-centered mechanisms for rights enforcement are unresponsive (by design) to certain kinds of economic and self-determination claims, and processes for standard-making and enforcement within legal-institutional arrangements for transnational economic and network governance have evolved in directions that increasingly decouple them from human rights considerations. Efforts to develop new forms of human rights discourse and practice organized around capabilities for human flourishing also have confronted new forms of co-optation rooted in the logics and imperatives of the managerial turn.

Scholars, activists, and advocates for marginalized communities worldwide have long argued that it is one thing to articulate formal statements of fundamental rights and quite another to guarantee freedom and self-determination for all peoples. The leading human rights instruments developed and ratified in the post-World War II era consisted for the most part of relatively simple, aspirational statements of the various civil and political or social and economic liberties to which individuals should be entitled.[13] To some, those statements represented important, albeit incompletely realized progress toward a more humane international order. To others, the emphasis on individual civil and social liberties reflected a deliberate effort to disempower more radical, anticolonialist movements emanating from the global South while bolstering the emergent neoliberal global order.[14] At minimum, it has long been clear that exercising fundamental rights and freedoms—whether civil and political or economic and social—

also requires resources and capabilities that many lack, particularly (but not only) in the world's least developed countries.

Gradually, claims sounding in distributive justice have engendered alternative forms of human rights discourse within which individual rights, collective self-determination, and economic and institutional development are inextricably intertwined. One such discourse is based on philosophical theories about capabilities for human flourishing—a formulation that encompasses the resources required for physical wellbeing, intellectual development, cultural participation, and political self-determination.[15] Another concerns the relationship between human flourishing and systemic environmental degradation. Environmental scientists, legal scholars, activists, and advocates have long argued that environmental threats represent acute threats to the future of humanity that require a strong collective response. In 1988, the UN established a permanent intergovernmental panel on climate change to collect and synthesize information on the effects of climate change and recommend mitigation options. In 2015, it formally endorsed the Sustainable Development Goals, a set of recommendations that is widely understood as having important human rights implications.[16]

Human rights discourses organized around capabilities and sustainable development, however, underscore the defects of existing institutional approaches to rights enforcement. The problem is not simply that transnational tribunals charged with enforcing international instruments lack authority to compel signatory states to remedy violations or that signatory states lack the will to do so.[17] More fundamentally, considerations relating to capabilities and sustainability have been difficult to recast as concrete obligations amenable to judicial enforcement.[18] In part the reasons are political and ideological and involve resistance to large-scale redistributive change. Legal reasoning about the privileged status of civil and political rights and the purported conceptual unruliness of economic and social rights also has played an important role in discouraging doctrinal and process innovations designed to advance substantive economic equality.[19]

Last and importantly, network power also matters. Within emergent legal-institutional arrangements for network-and-standard-based transnational governance, human rights courts and their concerns are increasingly marginalized. As a practical matter, then, the network-and-standard-based institutions for transnational economic and network governance described in Chapter 7 have become the front lines for many struggles to realize capabilities and sustainability goals. In theory, such institutions are well equipped to advance those goals, both because they operate via highly informationalized standard-making and because the mechanisms of network power obviate the need for legal compulsion. Other features of network-and-standard-based economic governance, however, cut the other way.

We saw in Chapter 7 that the mandatory structure of networked legal-institutional arrangements favors efforts to shape the governing standard in directions that are compatible with the dominant standard's underlying policy commitments and disfavors efforts to reorient those commitments. So, for example, legal-institutional arrangements for trade governance privilege global flows of extractive activity and for the most part treat local protective regulation as network damage. In many cases, claims about capabilities- and sustainability-related imperatives must be framed as justifiable

deviations from scientifically derived international standards that are more lenient. Other types of networked economic governance institutions have a relationship to rights enforcement that is simply haphazard. For example, financial stability standards have indirect implications for a range of capabilities- and sustainability-related goals, but making those connections takes work that the customary practices of financial standard-making organizations may not accommodate.

Meanwhile and perhaps predictably, as human rights discourses organized around capabilities and sustainability have encountered transnational legal-institutional arrangements for economic and network governance, they have undergone other kinds of transformation. New forms of human rights-related economic development practice emphasize efforts to make measurable improvements in the human condition, and those practices exemplify the themes of sociotechnical change and informationalization that this book has explored. They make intensive use of technological capabilities for collecting, communicating, and processing large quantities of information, and they rely on compact, information-intensive indicators to facilitate measuring, monitoring, and communicating about progress toward identified goals.[20] Those characteristics in turn have invited informationalism's distinctive institutional failure modes.

One long-standing critique of new forms of highly informationalized human rights discourse and practice engages the turn to neoliberal managerialism that earlier chapters have explored. As new enterprise models for development have emerged, those models sometimes have seemed more concerned with proper management of development efforts and development-based business plans than with whether those efforts and plans are producing meaningful change on the ground. Activists, advocates, and scholars have raised persistent concerns about the methodological tyranny of utilitarianism in the articulation of development goals and benchmarks.[21] As development discourses have become increasingly expert-driven and inaccessible to the populations whose futures they affect, they also exacerbate the problem of public reason that Chapter 7 explored.

More recently, human rights discourses and practices addressed to private economic power also have undergone a novel form of institutional cooptation that relocates them inside corporations themselves. Within network-and-standard-based economic governance contexts, a fast-growing sector of corporate-facing human rights practice has become "corporate social responsibility" (CSR) practice. As Chapter 7 noted, CSR standard-making has become a principal mechanism through which the UN attempts to govern the conduct of private actors on a variety of matters relating to human rights, economic well-being, and sustainability. In particular, the United Nations Global Compact, a framework for encouraging sustainable development, has worked in partnership with both public and private entities to formulate and encourage implementation of standards for corporate social responsibility covering a wide variety of topics, many of which intersect with human rights.[22] CSR discourses and initiatives have begun to proliferate and have spawned new academic journals and new practices of their own. Yet those discourses and initiatives also have sparked resistance; as one pair of scholars puts it, some argue that "CSR is bad capitalism" and others contend that "weak CSR is bad development."[23]

As those criticisms suggest, CSR advocates and initiatives occupy a uniquely equivocal position within corporate decision-making processes and network-and-standard-based governance arrangements. They seek to inform and shape a wide variety of corporate decisions and actions, but mechanisms for exacting compliance are weak. From one perspective, initiatives such as the UN Global Compact represent pragmatic and flexible solutions to pressing global governance problems; from another, they are powerful expressions of neoliberal governmentality. They rely exclusively on political and hortatory strategies to extract commitments that may or may not be honored. At the same time, they project an image of consensus around virtuous privatization of rights enforcement.[24] It remains to be seen whether efforts to incorporate CSR standards into other standard-making processes can achieve higher levels of compliance and whether, if so, compliance with CSR standards actually translates into concrete progress toward development and sustainability goals.

Ghosts in the Machine

New technologies for data-driven, algorithmic surveillance and intermediation raise different conceptual and institutional challenges for human rights enforcement that reside in the realm of the sociotechnical rather than the socioeconomic. Even if fundamental rights guarantees extended unambiguously and enforceably across the public-private divide, and even if network-and-standard-based institutions for transnational economic governance were ready and willing to accommodate such guarantees, such technologies alter the material conditions of possibility for the exercise of fundamental rights in ways that both liberty-based and capabilities-based formulations fail to capture. And they operate in ways that both traditional modes of court-centered enforcement and new modes of network-and-standard-based governance fail to constrain.

Until relatively recently, discourses about fundamental rights have relied on a set of unstated and unexamined assumptions about the material environment's affordances—the conditions of possibility that the material environment offers for individual, collective, and organizational activity.[25] So, for example, large-scale surveillance of telephone communications was impossible, and surveillance of movements in physical space was resource-intensive and could be difficult to conceal. Personalized targeting of information and advertising was something about which marketers could only dream, and microtargeting based on such considerations as political views, personality types, or emotional states was inconceivable. Relatively limited capabilities for surveillance and targeted intermediation engendered correspondingly open-ended possibilities for privacy, association, and intellectual and personal exploration.

Advances in networked digital communication and information have exposed the contingency of those assumptions, making clear that it is a mistake to take materiality for granted. As we have seen throughout this book, networked digital information and communications technologies have radically expanded the horizons of possibility for communication, association, and intellectual exploration, but they also have expanded the horizons of possibility for surveillance, control of expression and association, and highly granular, microtargeted intermediation of the information environment.

The rapid and dramatic changes in affordances for surveillance, control, and targeted intermediation pose novel challenges for traditional ways of conceptualizing and

detecting rights violations. Legal scholars have paid special attention to the relationships between algorithmic pattern-detection and unlawful discrimination in violation of fundamental rights to equal treatment, so it is useful to begin there. As we saw in Chapter 2, data-driven algorithmic epistemologies sort and classify individuals probabilistically in ways that are simply inconsistent with traditional ways of thinking about the kinds of reasoning necessary to justify, for example, decisions about investigation, sentencing, and eligibility for parole in criminal cases or decisions about access to important economic resources such as employment, housing, and credit. Data-driven epistemologies that rely on machine learning also optimize and reoptimize in ways that persistently elude review. Those processes can produce additional examples of the phenomenon that we encountered in Chapter 1: a systematic dismantling of the Polanyian protective countermovements instituted to protect workers and consumers in an earlier economic era. For example, a system forbidden to use race as a variable might use other data, such as media consumption or purchases of hair care products, to infer race and adjust the offered pricing or services accordingly, and it might use factors that themselves reflect preexisting patterns of discrimination, such as lower scores on standardized tests or longer commuting distances to the site of a new job, as decision-making proxies.[26] Machine-learning epistemologies also may embed discrimination in policing more systematically while clothing it in a veneer of automated neutrality. For example, facial recognition software trained on predominantly white faces does poorly at recognizing nonwhite faces, and the increasingly widespread use of such technologies renders individual members of racial minority groups more vulnerable to misrecognition and mislabeling.[27]

The problem of discrimination, however, is merely one manifestation of a more complex rule-of-law problem that inheres in the networked, algorithmically-intermediated communications environment. Smart digital technologies operate continually and immanently, producing decisions that are ad hoc, personalized, and pattern-based rather than principled and generalizable. They don't give reasons for—or even draw attention to—the choices they make. And they are designed to learn, producing outcomes that their designers did not directly specify. As Mireille Hildebrandt explains, these attributes contradict the principles of generality, stability, equality, and publicness that are foundational to the idea of the rule of law—and that establish predicate conditions for human rights protection. Pointing to the ways that printing facilitates stability, replication, deliberation, and universal application, Hildebrandt contends that the rule of law is itself an artifact of sociotechnical relations organized around print and text.[28] That conclusion may prove too much—it is possible that new rule-of-law criteria for evaluating the effects of networked digital technologies could be developed (and, as we saw in Chapter 7, new rule-of-law criteria capable of constraining the operation of network-and-standard-based governance institutions also are urgently needed). But algorithmic processes optimized for particular goals continually assert and reassert their own internal logics, which will resist interpolation of other values unless they are redesigned to incorporate new parameters.

Here again, institutional deficits compound the conceptual and operational difficulties. Consider policing again: For generations of lawyers and policymakers, the paradigmatic form of police work has been the individualized investigation. A crime is

committed, and afterward investigators search for clues that may enable them to identify the perpetrator(s) and prove the connection in court beyond a reasonable doubt. Modern police work, however, increasingly relies on the ability to access information collected through techniques for routine, population-wide surveillance. When courts attempt to resolve disputes about use of information acquired via population-wide surveillance using legal rules developed in the context of traditional, targeted investigations, they confront a mismatch that is both temporal and doctrinal. Judicial review is retrospective by design. Even a request for a warrant presupposes an already-committed crime and a discrete investigation that has produced results to which a judicial decision-maker can respond. And the questions that constitutional law empowers courts to ask—Is there probable cause? Was there a search? Was the search reasonable?—demand simple, yes-or-no answers that do not mesh well with a reality in which surveillance practices are ongoing. Doctrinal frameworks that focus on the moment of collection and impose few (if any) restrictions on subsequent access and use are poorly calibrated to address questions about the governance of contemporary, data-driven investigative methods and techniques.[29]

In the United States, some of the reasons for courts' refusal to supervise programmatic surveillance are historical and ideological. During the early twentieth century, police work became increasingly professionalized, a shift that sprang in part from a Progressive-Era ethos of scientific improvement. Law reformers saw criminal behavior as presumptively amenable to systematic study and criminal investigation as presumptively amenable to expert management.[30] As Progressive-Era ideologies about scientific management of the criminal justice process have given way to neoliberal managerialism, beliefs about the appropriate roles of professional discretion, informationalized management, and technical expertise in law enforcement have become ever more deeply entrenched. Narratives about the linear, depoliticized nature of technological progress do important background work, suggesting, for example, a neutral and generally optimistic stance toward the outputs of pattern-detection algorithms and biometric matching techniques.[31]

More generally, however, the same characteristics that defy traditional rule-of-law formulations make the new modes of programmatic surveillance highly resistant to the institutional concerns and competencies of courts. Courts and other institutions tasked with enforcing human rights guarantees traditionally have focused on impermissible *reasons* or *results*, but trying to govern algorithmic processes of surveillance and intermediation by focusing on discrete and particular outputs—whether one is contesting the results of a predictive policing search, a denial of employment or credit, or the results of a process for content removal—is like trying to produce sustainable improvements in water quality by removing individual impurities with a sieve. The design of automated machine-learning processes includes a number of steps that prohibitions directed to reasons and results do not capture. Data collection, data cleaning, algorithm design, and algorithm training all entail value-laden choices. The goals to be served must be defined computationally, and designers typically must choose which one(s) to prioritize by defining trade-offs among different training parameters. Eliminating or minimizing undesirable results is possible only if the tools are subject to continual audit and retraining.[32] Institutions unable to oversee those processes are almost perfectly optimized to leave programmatic surveillance initiatives and the intermediaries that operate them

unaccountable for the real and very consequential roles that they play in defining the material conditions of possibility for human freedom.

Viable alternatives or complements to judicial oversight, however, have yet to emerge. In the United States, the tradition of relying on courts has discouraged experimentation with new institutional forms for administrative oversight of law enforcement activity.[33] Paradoxically, such forms are somewhat better developed in the national security context. As we saw in Chapter 4, the logic of secrecy that surrounds and permeates national security operations disrupts conventional processes for ex post judicial oversight of investigations. Even the FISA court has found it necessary to rely more heavily on oversight by senior law enforcement officials, and over the years Congress has tasked those officials more explicitly with developing and formalizing certain types of oversight procedures.[34] The lessons such procedures might teach about the design of criminal administrative procedure more generally are largely hypothetical, however, because of the pervasive secrecy that surrounds their day-to-day use. In jurisdictions where ex ante regulation of programmatic surveillance is more extensive, there is little consensus about what might constitute effective operational oversight of policing activities. Courts seem to limit themselves to determining whether the laws as written include certain basic safeguards, and structures for operational oversight are unclear.[35]

As described in the previous section, network-and-standard-based institutions for transnational economic and network governance are for the most part neither accountable for human rights consequences nor directly concerned with fulfilling human rights mandates. But it is also unclear what standards those institutions would apply to ensure algorithmic accountability if they were so inclined. A baseline requirement of network-and-standard-based governance arrangements is the ability to define an applicable standard and invite compliance with it, and regulatory toolkits for ensuring algorithmic accountability are rudimentary.

As in the case of the capabilities and sustainability discourses described in the previous section, the resulting competency gap has invited new forms of governance that reflect well-known pathologies of managerial oversight. External oversight of the national security establishment now increasingly consists of production, publication, and review of aggregate performance data—numbers of production orders requested and granted, numbers of nefarious plots successfully thwarted, and so on. As in other contexts, however, such reporting is itself a type of performance, designed to express a generic commitment to accountability without exposing the types of operational information that might enable meaningful scrutiny of the underlying processes.[36] The operational secrecy surrounding national security and law enforcement uses of networked digital capabilities remains endemic.

Emergent arrangements for privatized governance of algorithmic content moderation processes similarly privilege expert management over public accountability. Debates about content moderation in a wide variety of contexts—copyright takedowns, the emergent right to be forgotten, child pornography, terrorist recruiting videos, and hate speech—increasingly revolve around the aggregate performance metrics prepared and released by communications intermediaries.[37] Some intermediaries, including notably Facebook, have produced "community guidelines" and have shared those guidelines with

regulators and with the public.[38] External observers are forced to rely on those disclosures—which are mostly about results and to some extent also about reasons—because no intermediary has provided operational detail about its algorithmic moderation processes, and none has been willing to allow interrogation of underlying practices of optimizing for *im*moderation in the first place. As practiced by the dominant platform firms and a host of smaller ones, algorithmic governance via "content moderation at scale" depends on elite management to define its parameters and oversee its operation, and it also asserts the sufficiency of elite management to correct for the ensuing and inevitable errors.

Power from Below?

In the face of these developments, broad coalitions of technologists, internet users, and digital rights activists have pursued two complementary sets of strategies for production and protection of fundamental rights and freedoms, one involving decentralized cultural and political production and the other involving anonymous resistance to and disruption of political and economic power. In platform-based, massively-intermediated information environments, however, both sets of digital-rights strategies have encountered a variety of obstacles. Platform-based, massively-intermediated environments magnify the effects of distributed, peer-produced cultural, social, and political activity but also co-opt the processes and outputs of distributed production in the service of data-driven profit strategies. Networked digital communications technologies afford new opportunities for anonymous resistance but also new points of control for state surveillance and censorship.

More fundamentally still, the results of anonymous online activism and distributed cultural and political production are not inevitably democracy-promoting, and predictions to the contrary have, in retrospect, come to seem extraordinarily naïve. Technological protections for anonymous online communication have enabled powerful new forms of resistance but have been far less successful at underwriting new institutional forms dedicated to ensuring more widespread protections for all people.

The Gift That Keeps on Giving

At the dawn of the internet era, some scholars and activists prophesied that decentralized production of various social, cultural, and political goods by communities of peers would largely displace centralized, top-down coordination and control in a wide variety of domains, with transformative and broadly freedom-promoting effects. In the ensuing years, decentralized production strategies have expanded access to information and political capacity-building for peoples all around the world and have come to be regarded as essential tools for fostering human freedom in the networked information era.[39] The grander visions of wholesale transformation in political economy and in politics have not materialized, however. Instead, strategies for decentralized cultural and political production have reinforced platform logics and business models, fueling the emergence of dominant information platforms and affording new vantage points for data harvesting, surplus extraction, and manipulation of information flows.

Chapters 1 and 3 described some of the new forms of decentralized, collective cultural production that networked information and communication technologies have enabled. The two most well-known examples, the open source software movement and the Creative Commons movement, were self-consciously designed as efforts to develop sustainable, "copyleft" alternatives to the existing copyright regime—arrangements that would permit and encourage open access, copying, sharing, tinkering, repurposing, and remixing content created by others.[40] The trailblazing crowd-sourced encyclopedia, Wikipedia, uses Creative Commons licensing to keep its content open and freely accessible. Open source software has been at the forefront of efforts to make computing resources widely available to people in developing economies.

Networked information and communication technologies also have catalyzed new approaches to grass-roots political organizing. Some of the most transformative gains from such approaches have come in the global South. Grassroots organizers around the world have appropriated networked, platform-based communication tools—including Facebook pages, Twitter hashtags, applications for multiparty messaging, and many more—for a wide variety of purposes, ranging from the storied uprisings of the Arab Spring to voter-registration drives in emerging African democracies to efforts to organize workers in Asian garment and high technology factories to local struggles over failure to provide municipal services.[41]

Some of the obstacles to commons-based cultural and political production were predictable or at least familiar. Leading software firms waged public and creative campaigns against open source software, labeling it unreliable, insecure, and a point of entry for organized crime. Although open source products and accompanying services eventually achieved widespread penetration in certain industry sectors and some once-formidable opponents have become adherents, persistent, thorny issues continue to surround the interfaces between open source and proprietary systems and modules.[42] The major content industries have resisted commons-based production and open-access distribution strategies for educational and cultural materials, and as Chapter 4 described, they have devised a continuing stream of legal and technological methods for asserting control over their products and business models.[43]

Political activists, for their part, quickly learned that the networked digital information environment afforded not only unprecedented scope for circulating dissenting ideas and coordinating political resistance but also new, hidden control points for state censorship and surveillance. Surveillance capabilities built into backbone servers and similar equipment—some of it supplied by Chinese technology firms but some sourced from the United States and other Western countries—have given governments across the Middle East, Africa, and Asia leverage to counter uses of social media to fuel popular protests and uprisings. In most of the countries where the Arab Spring uprisings occurred, they were quickly followed by government crackdowns that exploited networked surveillance capabilities, and that pattern has continued elsewhere.[44] In the United States, where communications intermediaries generally have resisted installing "back doors" for law enforcement and national security officials, electronic surveillance laws nonetheless afford only limited protections to communications metadata, and the relative ease of acquiring such data has enabled law enforcement to monitor and track activists and social movement organizers.[45]

Other failure modes for commons-based production were wholly unanticipated. In terms of political economy, openness has proved a double-edged sword. Platform protocols invite commons-based production arrangements and commons-based production arrangements in turn reinforce platform logics of datafication, data harvesting, and proprietary, algorithmic knowledge production. Like the gig workers and creative freelancers discussed in Chapter 1, content developers within open content ecosystems gain an extra measure of agency and content users an extra measure of information access, but both groups also double as voluntary information workers for platforms and their business affiliates.[46] And the peer-based quality control mechanisms that keep open source software robust and secure and Wikipedia reliable and (mostly) objective work far less well within massively intermediated environments that are optimized to advertiser-driven platform revenue models.

More fundamentally, algorithmic processes optimized to manufacture outrage, boost click-through rates, prompt social sharing, and enhance capabilities for behavioral microtargeting are agnostic as to underlying political and ideological commitments. As Chapter 3 explained, networked, massively intermediated communication technologies are crowd enhancers—they amplify whatever the crowd wants, while at the same time making the crowd easier to manipulate. Under such conditions, power from below becomes power directed toward whatever purpose its organizers want to advance, and crowdsourcing strategies for political consciousness-raising and political action lend themselves to actors pursuing a wide variety of ends. One result is that platform-based, massively intermediated environments have become fertile breeding grounds for virulent forms of ethnic nationalism and ideological extremism. Around the world, authoritarian regimes and nationalist movements use social media cascades to warn majority groups that they are under threat, spreading rumors and lies designed to provoke fear, incite small-scale acts of hatred and violence, and catalyze more systematic campaigns of ethnic cleansing.[47] At the same time, and paradoxically, the increasingly pronounced orientation toward manufactured outrage and political polarization within such environments also dissipates other kinds of political energy. As Zeynep Tufecki explains, in the networked information era, it has become easy to organize a protest (or simply to elicit cascades of viral sharing) but more difficult to enlist networked publics in the work of democratic capacity-building in the real world.[48]

Among scholars and commentators who write about digital media, a debate has raged about whether it is fair to blame platforms for these problems. According to media scholar Siva Vaidhyanathan, "the problem with Facebook is Facebook," and more specifically the combination of Facebook's global reach, its optimization-based business model, and the ways that its information feeds have displaced other, potentially moderating sources of information.[49] By similar reasoning, the problem with WhatsApp is WhatsApp, which offers secure encryption but permits contact harvesting and message chaining to reach large groups; the problem with Twitter is Twitter, which boosts the visibility of trending topics and selectively amplifies them based on predictive profiling; the problem with Google is Google, which elevates search results to positions of supremacy and purported objectivity if they are popular enough; and the problem with YouTube is YouTube, which facilitates targeted and extraordinarily effective audiovisual indoctrination by conspiracy theorists of all stripes. Others argue that such explanations

unfairly blame platforms for long-standing dysfunctions that are not of their creation.[50] Part of the problem with Facebook (and WhatsApp and so on) is the preexisting social and cultural divisions that information cascades amplify—white supremacist politics in the United States, Hindu-Muslim tensions in India, and so on.

For my purposes here, the important point (which Vaidhyanathan also makes), is that debates about the root causes of popular bigotry and irrationality and the overriding importance of free information flow tend to elide the essential roles of other institutions, both public and private, that might modulate and selectively amplify or dampen features of public discourse. Part of the problem with Facebook (and WhatsApp and so on) is people, easily distracted, highly susceptible to misinformation, and prone to herd behavior. And part of the problem is the systematic disintermediation and delegitimation of the other legal and social institutions that formerly debunked unfounded rumors, suppressed public expressions of bigotry, and moderated populist excesses. In the networked information era, preserving fundamental rights and freedoms for all people requires an institutional foundation that encompasses not only rights to speak, to access information, and so on but also other structural safeguards—safeguards designed to preserve a well-functioning networked public sphere and inoculate it sufficiently against cascading misinformation and hatred.[51] The idea that digital direct democracy will produce the latter seems increasingly difficult to countenance.

Anonymity, Trust, and the Problem of Scale

Other scholars and activists who took up Barlow's call for enlightened cyberliberarianism focused on building capabilities for distributed, anonymous communication and coordination. Although many of the developments discussed in this book have made anonymity in daily life illusory for most ordinary people, deliberately constructed online anonymity has become a site of ongoing research and activism. Several decades into that project, however, persistent and intractable questions remain about the extent to which behaviors that historically have functioned as safety valves can assume more central roles in the project of securing fundamental rights and freedoms for all people. Some anonymous online actors have worked to advance democracy, equality, and broadly distributed enjoyment of civil rights and liberties in contexts all around the world, and others have worked just as hard to subvert those goals. The challenge of designing infrastructures and institutions for anonymous action that are reliably democracy-promoting remains unanswered.

Discussions about the promise or peril of anonymity often are framed in terms of absolutes. So, for example, some argue that persistent identification enables censorship and oppression, while anonymity shelters dissent and fosters the capacity for criticism and political self-determination. Others contend that identification engenders trust and fosters beneficial accountability, while anonymity encourages irresponsibility and antisocial behavior.

In reality, a wealth of historical and contemporary evidence supports *both* sets of arguments, suggesting that the relationships among anonymity, democratic self-determination, and social benefit depend very much on context. The virtues of anonymity are not just theoretical. Throughout history, anonymous and pseudonymous advocates, activists, and whistleblowers have catalyzed public debate about vital issues of political

accountability, and in the modern era, state surveillance and human rights abuses have been closely linked.[52] In other contexts, however, there is broad consensus that easy anonymity would strain the social compact too far. So, for example, corporations must register with the state and disclose the names and addresses of their directors. Transfers of corporate stock must be registered by the purchaser or the purchaser's agent, as must transfers of internet domains. Applicants for professional licenses must provide identifying information. Systemic incentives to record real property purchases are so pervasive that registration is essentially mandatory.[53] There are good reasons for all of these rules, which enable government to provide for the public safety and welfare and to hold accumulations of private economic power accountable in certain basic ways.

The spectrum of anonymous online action mirrors these complexities. Around the world, anonymous online actors have used networked communication capabilities to name and challenge abuses of political and economic power. They organize protests and acts of civil disobedience and maintain networks and sites for unmonitored exchange of information, anonymous discussion of forbidden topics, and anonymous publication of dissident and whistleblower content. Activists pursuing social change and journalists reporting on controversial topics rely on capabilities for anonymous communication to protect themselves and their sources.[54] In the wake of the Snowden revelations, the general public also has shown more sustained interest in such capabilities. Some information businesses, including most notably Apple but also others, have come to view market offerings designed to enable secure, anonymized communication as a point of competitive advantage.[55]

But the story of online anonymity also is more complicated than romanticized narratives equating anonymity with press freedom and democratic self-determination make it out to be. In networked spaces, cadres of technological cognoscenti wield anonymity as a new and potent source of social and political power to be deployed toward a wide variety of ends. They orchestrate large-scale whistleblowing, operate safe channels for journalists, and distribute samizdat on behalf of political dissidents—and also spread hate speech, disinformation, and fascist and nationalist ideologies. They hack into government and corporate networks to expose corruption and disrupt secrecy—and also to obtain and release the private documents and photographs of those who incur their displeasure. The counterpower of anonymity can expose and discomfit the powerful, and it also can be deployed to profoundly antisocial and destructive ends.

Additionally, the trajectories of projects designed to scale up certain types of anonymous interaction demonstrate that breaking things is easier than building them. So, for example, in Chapter 1, we encountered the blockchain, a technical protocol for enabling distributed, secure authentication of digital transactions. Because blockchain-supported transactions can be executed without relying on centrally certified intermediaries, the technology has been heralded as a promising vehicle for restoring trust in online environments. In theory, such technologies might be deployed within existing institutional fabrics to eliminate opportunities for corruption, waste, and rent-seeking.[56] But uses for private surplus extraction and self-interested (and environmentally destructive) speculation are far more widespread, and some argue that the highest and best uses of blockchain technologies involve the creation of alternative currencies to displace state-sponsored fiat currency and ultimately the state itself. Meanwhile, a

continuing series of implosions by private cryptocurrency experiments has demonstrated that sustainable cryptocurrency systems have institutional as well as technical dimensions, and that the institutional structures underlying such systems do not automatically scale.[57]

As a second example, consider the online organization WikiLeaks, which we encountered in Chapter 4. Among digital civil liberties advocates, WikiLeaks and its flamboyant founder, Julian Assange, rapidly attained heroic status for their stated commitment to facilitating anonymous whistleblowing about powerful wrongdoers.[58] The media organizations with which WikiLeaks shared information about U.S. military operations and diplomatic cables were more circumspect. Because some kinds of leaks really can endanger lives, they engaged in careful review to determine what to publish and what to withhold, and they also made efforts to draw WikiLeaks into a conversation about how to construct institutional mechanisms for responsible whistleblowing. Without question, that conversation was complicated by the virulence of U.S.-led efforts to deprive WikiLeaks of Web hosting and payment services, label it a criminal organization in the court of international opinion, and bring its leaders to trial in the United States. But differences of opinion among WikiLeaks' principals also undermined efforts to draw the organization into discussions about institutional design questions. Assange in particular had a deeply ingrained fascination with disruption for its own sake and an equally deep distaste for the liberal, globalist commitments of his establishment interlocutors.[59] WikiLeaks has continued to pursue government transparency and to publish important leaks, but it also has been linked to state-sponsored disinformation campaigns designed to destabilize competing regimes.[60]

As these examples suggest, although anonymous online action has played and will continue to play an important role in efforts to secure fundamental rights and freedoms for all people, arguments equating scope for anonymous action with the preservation of human freedom are far too simple. Some of the relevant factors are cultural. Experiments with scaling up anonymity have tended to express complex sets of political commitments that bear closer examination. Understood as anti-institutionalist projects, WikiLeaks and many blockchain-based cryptocurrency schemes reflect ideologies that are powerfully utopian but not particularly democratic. They express and reproduce a particular kind of moral and ideological purity that is both unrealistic and inconsistent with a broadly inclusive social compact. More generally, as anthropologist Gabriella Coleman has shown, hacker culture speaks the intertwined languages of liberal individualism and libertarianism, which prize freedom from state-imposed limitations and posit enlightened self-reliance and, by necessary implication, technical meritocracy as cardinal virtues.[61] Barlow's famous declaration of independence for cyberspace resonated with those commitments, but the views it so vividly expressed have complicated efforts to transform digital anonymity from a tool for resistance to the foundation of a stable democratic framework. In any functioning system of the rule of law, dissent and opposition play vital structural roles, and anonymity therefore is an indispensable safety valve. But achieving durable, effective protection for fundamental rights and freedoms requires a broader and more diverse institutional foundation.

Taking Liberties: The New Normative Authority of Capital

A third set of significant shifts in discourses and practices relating to fundamental rights involves entrepreneurial appropriation of discourses about fundamental human rights to describe the rights and privileges of corporate entities. One form of corporate rights entrepreneurship concerns protections for corporate foreign direct investment. The rapid spread of investor-state dispute settlement provisions within the world trade system has enabled firms to frame complaints about burdensome local regulation as claims for impairment of their private property rights. Other forms of corporate rights entrepreneurship concern rights of free speech and privacy. We saw in Chapter 3 that information intermediaries based in the United States rely on the First Amendment's protection for freedom of speech to shelter their information processing activities, but the co-optation of rights discourses about free speech and privacy by powerful commercial entities also takes other forms, and the story about the emerging global economy of personal data processing is not only a story about the expanding global footprint of powerful U.S. technology companies. Two other permutations—a European story about the entailments of individual autonomy and a Chinese story about virtuous corporate citizenship as one pillar of the rule of law—are also in play.

Property Goes Rogue: The Emerging Global Law of Regulatory Takings

The network-and-standard-based institutions for world trade governance studied in Chapter 7 have facilitated a powerful form of corporate rights entrepreneurship that revolves around the asserted primacy of private property rights. Investor-state dispute settlement (ISDS) provisions in many treaties governing foreign direct investment permit nonstate investors, typically multinational corporations, to challenge various kinds of state actions that threaten their investments and to bring their claims before panels of private arbitrators rather than in the host country's courts. Over the last several decades, those provisions have become vehicles for an effort to protect the asserted private property rights of corporations against domestic regulations that would lower the value of their transnational investments.

First created in the mid-twentieth century, ISDS mechanisms were envisioned as necessary incentives for investment in developing economies because they promised to protect investing firms, typically headquartered in the global North, against corruption, favoritism toward local competitors, and possible direct expropriation of corporate assets. So understood, ISDS provisions expressed a modernized ethos of colonial expansion updated for the era of trade liberalization; they replaced claims by colonial sovereigns (though not their involvement) with claims by private capital investors.[62]

As with the processes that Chapter 7 explored, however, the decentering of state institutions laid the groundwork for other kinds of changes. Beginning in the 1990s, the ISDS landscape began to change rapidly. Today, ISDS provisions encompassing both direct and "indirect"—that is, regulatory—expropriations exist in tens of thousands of bilateral and multilateral agreements that extend around the globe and that are expressly designed to enable their assertion in any country.[63]

In large part due to the dynamics of network-and-standard-based governance studied in Chapter 7, emerging global frameworks for ISDS have begun to reflect the influence of U.S. constitutional doctrine relating to so-called regulatory takings of private

property rights. In the 1990s, following implementation of the North American Free Trade Agreement (NAFTA), U.S. scholars and policymakers grew concerned that the language of the treaty's ISDS chapter, which referred to state actions that were "tantamount to nationalization or expropriation," could support a variety of investor demands for relief from local, state, or federal laws imposing regulatory burdens. That possibility materialized in 2000 in the form of a multi-million dollar arbitral award against the Mexican government on behalf of Metalclad, a U.S. corporation whose application to operate a hazardous waste landfill had been denied for environmental reasons.[64]

Following the *Metalclad* award, the U.S. Trade Representative urged Congress to amend the ISDS mechanism to refer to the standard used in regulatory takings cases so that the results in any future arbitral proceedings against the United States would mirror those that could be obtained in the federal courts. According to that standard, first articulated in a case called *Penn Central*, a proposed regulatory change that interferes too greatly with distinct investment-based expectations regarding private property can be deemed a taking without just compensation unless it is justified as a generally applicable exercise of the state's traditional police power to protect the public welfare.[65] After Congress complied, the Trade Representative drafted a new model bilateral investment treaty that included language directly incorporating key terms from the regulatory takings case law, including the idea of government interference with "distinct, reasonable investment-backed expectations." It then began using the treaty as a template in negotiations over other bilateral and multilateral trade agreements worldwide.[66]

The U.S. attempt to discipline the ISDS mechanism by tethering it to regulatory takings doctrine but also to export clauses modeled on the NAFTA ISDS provision to the rest of the world reflects more than just protectionism. Here it is useful to consider the political and ideological history of the doctrine as it has evolved domestically. Over the past several decades, U.S. legal scholars who study property law have chronicled the emergence of a movement to limit land use regulation by expanding constitutional protection for private property rights. Like the movement to expand constitutional protection for commercial speech that Chapter 3 described, the property rights movement originated in libertarian and neoliberal think tanks and began to take shape as a coordinated litigation agenda during the 1980s.[67] As interpreted by the federal courts, the *Penn Central* standard embodies some resistance to that agenda—it is highly malleable and courts have resisted interpretations that would allow vested interests to trump all forms of protective environmental and land use regulation—but the idea of "reasonable investment-backed expectations" also came to be understood as reifying a baseline level of protection against changing public sensibilities about economic development risks and harms.[68]

The decisions to insert the *Penn Central* standard into the NAFTA investor-state dispute mechanism and subsequently to pursue its incorporation within the thickening network of bilateral and multilateral investment treaties to which the United States is party must be read in light of that history. Viewed against the backdrop of decades of coordinated resistance to environmental regulation in the name of sacrosanct property rights, the campaign to orient the network-and-standard-based processes of world trade governance to the investment-backed expectations of multinational corporate actors

cannot be characterized simply as an effort to preserve space for protective regulation. Looking to the longer term and to the transnational arena for legal standard-making, it was also a stance calculated to privilege relatively concrete and monetizable extractive interests over changing public needs.

Consistent with the increasing importance of intangible assets in the informational economy, the ISDS landscape has gradually widened to include asserted takings of intangible intellectual property interests, including patent interests and trade secrecy interests relating to research and development activities.[69] In Chapter 1, we saw that, over the last half century, both intellectual property doctrines and their accompanying narratives of justification have gradually aligned with the goals and desires of corporate rightholders. ISDS proceedings concerning intellectual property interests continue that evolutionary arc. As Rochelle Dreyfuss and Susy Frankel have observed, the outcomes of investor-state proceedings turn on narratives that do not require human creators or their creative incentives at all, but instead reframe intangible intellectual progress as the product of investment.[70] It seems sensible to predict that, over time, corporate "investors" will invoke ISDS mechanisms to protect other types of intangible interests covered under trade in services agreements. As of this writing, there is no report of any investor-state proceeding arising out of asserted state interference with cross-border flows of personal data, but such disputes seem certain to materialize.

All has not been smooth sailing for the transnational corporate property rights movement. As arbitral rulings identifying unlawful indirect expropriations have begun to emerge, public outrage and calls for reform have mounted. Opinions differ strikingly, however, on the sort of reform that is needed. The 2016 presidential election in the United States produced a number of reversals of well-established trade policy positions, including an effort to eliminate ISDS from NAFTA altogether. Canada, Mexico, and the powerful U.S. Chamber of Commerce all opposed elimination, and, as of this writing, the finalized U.S.-Mexico-Canada Agreement preserves ISDS, but only for a drastically narrowed class of disputes.[71] European debates reflect similar disagreements. In a 2018 decision in a case challenging an arbitral award against Slovakia under a bilateral investment treaty with the Netherlands, the European Court of Justice held that the treaty provision creating the ISDS procedure impermissibly impaired the autonomy of European law. Meanwhile, the European Commission has been attempting to design a new ISDS mechanism with more robust rule-of-law characteristics, including publicly appointed judges, public proceedings, prescribed grounds for invalidating state regulatory determinations, and provisions for an appellate body. It also has proposed multilateral negotiations on a new convention establishing a multilateral dispute settlement court.[72]

Both the sheer number of ISDS provisions in existing treaties and their distributive politics, however, suggest that investor-state dispute resolution in some form is here to stay. Within the liberty-based approach to conceptualizing fundamental rights that still transnational discourses about nonnegotiable baseline obligations to persons, rights talk about investment expectations functions and is intended to function as a normative trump card. It is a way of inoculating network-and-standard-based legal-institutional arrangements for transnational economic governance against the destabilizing effects of legal standards wars that threaten to inject other, more explicitly public-regarding considerations into the standard-setting calculus.

Free Speech and Privacy through the Looking Glass: Escalating the Battle to Control Global Data Flows

For the last two decades, the United States and Europe have been engaged in protracted struggles to define and calibrate corporate obligations regarding privacy, data protection, and removal of online content, and those struggles have showcased two other forms of corporate rights entrepreneurship. In the United States, the predominant form of corporate rights entrepreneurship about privacy involves asserted corporate free speech rights. We have already explored contemporary U.S. thinking about the free speech rights of information intermediaries, and I will revisit it here only briefly. In Europe, which does not recognize corporate free speech interests to a similarly broad extent, the predominant mode of corporate rights entrepreneurship concerns the autonomy of individual data subjects.

As Chapter 3 described, the United States has for many decades been ground zero for efforts to enshrine an expansive approach to corporate free speech rights, and those efforts have begun to bear substantial fruit. Cases about the contours of the contemporary First Amendment have constructed a broad equivalence between information processing and speech, and platform entities in particular have mobilized both the traditional First Amendment frame of the marketplace of ideas and the new frame of the information laboratory to underwrite broad immunities from regulatory oversight. Internet intermediaries also enjoy broad statutory immunity from liability for civil wrongs, and conventional wisdom about the relationship between media technologies and human freedom justifies that arrangement on both speech- and innovation-related grounds.

As we have seen throughout this book, European and U.S. legal traditions differ markedly on many privacy- and speech-related issues. European human rights law enshrines both privacy and data protection as fundamental rights, while U.S. constitutional law is more grudging, according protection to narrower interests in more piecemeal fashion.[73] The two legal traditions also differ on the circumstances that justify speech restrictions. European legal systems generally prohibit hate speech, while the U.S. does not, and European legal systems are less tolerant of unauthorized publication of personal information about private individuals. Last but not least, although European courts sometimes have permitted media companies and other fictional entities to assert interests in protecting and promoting freedom of expression, they have done so in a comparatively restrained and context-specific way.[74]

Among U.S. legal commentators and tech policy pundits, it is conventional to think that European law's relative receptiveness to certain kinds of restrictions on speech and information processing makes European citizens less free, but that conclusion does not withstand close scrutiny. In general, European nations have both robust media ecosystems and courts willing to block legislative and prosecutorial overreach. There have been some notable exceptions, but that is true on both sides of the Atlantic.[75] When European courts need to resolve asserted conflicts between one person's rights to privacy and another's freedom of speech, they use doctrines requiring interest balancing that are similar to those developed in the U.S. constitutional context, and information intermediaries sometimes benefit from that balancing. Decisions about matters such as the right to be forgotten and the scope of obligations to remove various kinds of harmful content have begun to establish clearer parameters for information intermediaries to use

in structuring their operations. Contrary to alarmist predictions by some U.S. commentators, those parameters do not insulate public figures from criticism, nor do they prohibit reporting and commentary about hate groups or terrorist acts.[76]

Questions about individual consumers' rights to *authorize* the harvesting and processing of their personal data, however, have presented difficult challenges for European legal systems. Formally, European law reserves much greater control to consumers than U.S. law does. Both the General Data Protection Regulation adopted in 2016 (GDPR) and the regime it replaced adopt the paradigm of "privacy-as-control," which emphasizes the autonomy and dignity of data subjects.[77] In European privacy practice, however, important strands of discourse about individual autonomy present opportunities for co-optation by corporate claimants seeking to privilege the choices of European consumers, and the patterns of co-optation have begun to unfold in opposite but mutually reinforcing ways.

As a practical matter, there is an intractable tension between the regulatory goal of specific, explicit consent to data collection and processing and the marketplace drift toward convenience. Formally, European data protection law imposes a strict definition of consent and forbids processing personal data in ways incompatible with the purpose for which the data was initially collected. Renewed consent can justify later processing for a new, incompatible purpose, but rolling consent is not supposed to become a mechanism for evading purpose limitations entirely. An entity providing information services may not rely on consent to justify harvesting and processing if there is "a significant imbalance between the position of the data subject and the controller."[78] Practically speaking, however, individuals wanting access to the social media services offered by global (often U.S.-based) internet companies typically elect to grant consent to data processing in the ways that those services recommend. That result accords with neoliberal ideals of self-actualization through market and consumptive choices, and when it is permitted to stand, it substantially narrows the distances between U.S. and European regimes.[79]

Less obvious but equally important, in networked, algorithmically intermediated environments, the autonomy-based privacy-as-control paradigm confronts significant and potentially fatal implementation difficulties. For example, although the scope of the requirement is disputed, European law requires that data subjects be given meaningful information about the automated logics involved in processing personal data. Important questions remain, however, about whether it is possible to explain certain types of automated processes at all and whether such explanations, if available, constitute meaningful remedies for complaints that are, at bottom, complaints about unfair treatment. It is unclear what, if anything, individual data subjects might gain from the opportunity to navigate an additional layer of complexity in aid of making wide-ranging and imperfectly informed decisions about an uncertain future.[80] Additionally, as described earlier in this chapter, machine learning-based algorithmic processes are resourceful at working around constraints, which means that even well-intentioned disclosures may be inaccurate and even clearly specified scope limitations may be ineffective. Placing individual data subjects and their choices at the center of debates about how far such processes should be authorized seems unlikely to produce either fairer markets or more coherent choices about the appropriate extent of data-driven surveillance

and intermediation.[81] Operationalizing disclosure and access rights also promises to increase both overall levels of surveillance and the severity of associated data security threats.[82]

Much has been made of the fact that the GDPR's provisions for policymaking and enforcement depart from the previous data protection regime by centralizing data protection authority in the European Commission. Some reasons for that shift were enforcement-related. Arguably, to regulate global information businesses such as Google, Facebook, and Apple in a way that effectively counters American laxity, Europe must speak with a unified voice. But the details of the change reflect corporate entrepreneurship of a different kind. European and global businesses had found the previous regime's patchwork of national compliance requirements expensive and unwieldy. The GDPR provides a mechanism for achieving Europe-wide compliance via boilerplate clauses and binding corporate rules. In so doing, however, it narrows the list of targets for regulatory capture efforts. National regulators continue to wield front-line enforcement authority, but lack power to impose new substantive requirements; they cannot lower European data protection standards, but they also cannot attempt to raise them.

Taken together, these developments reflect a still-unresolved struggle between demands for meaningful substantive protection of fundamental rights of privacy, expression, and association and demands for reduction of barriers to global economic enterprise.[83] On one view, European legal institutions have embarked on a process of human rights experimentalism aimed at extending protections for fundamental rights gradually via iterative interactions among the Commission, the courts, and national regulators who wield front-line enforcement authority.[84] On another, the vaunted European data protection framework, and by extension the larger human rights framework within which it is embedded, are undergoing a (largely unacknowledged) moment of crisis whose resolution remains uncertain.

The success or failure of European-style data protection regulation therefore will depend only in part on the Commission's willingness to wield its enhanced enforcement powers under the GDPR in the service of thicker conceptions of individual autonomy and flourishing than the ones that global information businesses have preferred. It also will depend in part on development of new competencies for achieving algorithmic accountability that do not rely exclusively on individualized autonomy and control claims to secure their realization. Additionally, as we saw in Chapter 7, it will depend on whether European regulators and consumers can marshal sufficient network-making power to propagate heightened levels of protection throughout network-and-standard-based arrangements for global economic governance—and to reinforce such arrangements vis-à-vis the growing power of the authoritarian end run.

Accountability, Authority, and Corporate Virtue in the "Red Stack"

A final important strand of the evolving global contest over the rights and privileges of informational capital concerns Chinese information technology firms and Chinese information technology policy. Like their U.S. counterparts, Chinese firms also have surveillance-based business models; unlike the U.S. government, however, the Chinese government has maintained control over domestic implementations of those

models. Domestically, Chinese information technology policy has embraced a vision of personal data collection and processing within which digital reputation is a central pillar not only of good citizenship but also of the rule of law—and in which cooperation in the construction of state-supervised reputation metrics is a marker of corporate virtue.

As noted earlier in this chapter, during the internet's early years, Western commentators marveling at the rapid growth and global spread of technology firms such as Microsoft, Yahoo!, Google, Facebook, and Apple appeared to believe that the emerging global communications network would have an inherently libertarian orientation. Users would exploit networked capabilities to evade state surveillance and censorship; consumers would demand unfiltered access to the open internet; and internet intermediaries would honor consumer preferences by resisting state demands for cooperation.[85] Time has shown those predictions to be incorrect. Although many determined Chinese citizens have resisted state surveillance, finding creative ways of discussing banned topics and circumventing filters and firewalls, the Chinese population more generally is relatively inured to state surveillance and control of permissible expression. And U.S. platform firms operating in China (and elsewhere) have largely acceded to host country demands for content filtering and identification of account users.[86]

Narratives about global information intermediaries' resistance to state surveillance also were problematic for a far more basic reason: they envisioned the nations of the global South as innovation bottom-feeders—offering new markets and new data but not their own information platforms and services—and gave correspondingly little thought to what information platforms emerging from the global South might look like. As Chapter 7 described, that assessment has proved shortsighted. A coordinated campaign combining state investment, systematic technology acquisition, and end runs around transnational norms favoring liberalization of information flows has produced the "Red Stack"—a thriving Chinese information technology sector whose products and services have capabilities for surveillance and control built in at the core.

As Chinese technology companies have thrived, they have begun partnering with state and local government authorities to develop surveillance infrastructures and capabilities along a new, distinctively Chinese model. Within that model, communications, commerce, policing, and the provision of public services are fully integrated all the way down. Chinese citizens already accustomed to the need to provide identification documents have readily transitioned to using digital platforms for interacting with government offices and even participating in virtual public hearings. For some, at least, the ready availability of those services expresses both the state's care for its citizens and the public-spiritedness of Chinese industry.[87]

Chinese technology firms' commercial offerings have straightforward affordances for state filtering and surveillance. Search engines and internet access providers are supplied with lists of items and domains to be blocked, and equipment and software for the provision of internet services must straightforwardly accommodate such demands.[88] Consumer technologies and apps also are surveillance-friendly. For example, as a condition of selling iPhones in the Chinese market, the government required Apple to contract with a Chinese cloud storage provider to store customers' iCloud encryption keys locally. One review of leading instant messaging applications gave Tencent's

WeChat application a security rating of zero because it does not attempt to counter third-party surveillance at all, and WeChat also engages in extensive, legally mandated image filtering.[89] Chinese platforms also have provided congenial environments for government-sponsored disinformation campaigns designed to distract Chinese networked publics from more serious pursuits, thereby stabilizing the ruling regime.[90]

Following the pattern described in the first half of this chapter, the thickening web of public-private surveillance also has begun to foster new state surveillance initiatives; in the Chinese model, however, the state has taken the lead in developing those initiatives, in crafting narratives about their reliability and legitimacy, and in enlisting private-sector cooperation. Among other things, it has announced its intent to develop and implement a nationwide system for "social credit scoring" by 2020, to equip its extensive network of surveillance cameras with facial recognition capabilities, and to integrate the two projects. Much Western coverage of these efforts has emphasized their potential for fostering social conformity, stifling dissent, and facilitating systematic oppression.[91] Perhaps most notably, field tests of state surveillance capabilities in the Xinjiang region have shown those capabilities being used to restrict the movements of members of the predominantly Muslim Uighur population as part of a more systematic campaign of social and cultural "reeducation."[92] In time, however, the state envisions providing every citizen with a score that encompasses far more than either past purchasing behavior or political activity and that mediates access to a wide variety of public and private privileges and services.[93]

Entrenching state political control is an undoubted goal of the emergent Chinese social credit scoring system, but there are also others that Western observers have tended to discount, and they reflect more complicated narratives about the nature and origins of both privacy rights and corporate virtue. As Xin Dai explains, other goals include both strengthening intra-governmental accountability and furthering economic development. In particular, systems for tracking and disclosing compliance with court orders and administrative fines are understood and represented to the public as advancing the rule of law. Yet another purpose is to assert state supremacy relative to what many Chinese have begun to see as the entirely unaccountable information practices of powerful Chinese platform providers.[94] Both Alibaba and Tencent were among a select group of companies initially approved by the state to develop pilot social credit scoring technologies, but both have incurred unprecedented popular criticism for their undisclosed data harvesting activities. In February 2018, the government ordered Tencent to cancel a nationwide test of its scoring project. In theory at least, the government's system will have the capacity to extend some basic data protection guarantees, including the opportunity to know one's ranking and to challenge the accuracy of particular items.[95] In both respects, the emergent Chinese regime of networked information governance stands in thought-provoking counterpoint to the neoliberal regime of reputation surveillance described in Part I, which locates both power and immunity from accountability differently.

As Chapter 7 described, the emergent Chinese regime of surveillance as state prerogative also is gaining ground globally. So far, the dominant Chinese platform firms have made only partial inroads into U.S. and European markets. Merchants that cater to Chinese tourists now accept mobile payments via WeChat and AliPay, and anecdotal evidence also suggests that an unknown number of small merchants that advertise on

U.S. platforms such as Instagram use members of Alibaba's affiliated group of companies to source merchandise directly from China.[96] In developing economies and regions, Chinese firms have a much higher profile, in part because they offer services tailored to the distinctive needs and desires of both populations and governments. Populations that, like China's, are rapidly moving online using mobile devices as the primary access points are gravitating to relatively affordable Chinese-manufactured mobile devices and to the services that Chinese platform firms excel at providing, including instant messaging, e-commerce, and mobile payment systems. Governments, meanwhile, have gravitated to the built-in surveillance capabilities offered by Chinese technology firms and platform services.[97]

Together, these developments are underwriting the global expansion of a vision of the networked public sphere in which fundamental human rights play no discernible part. The Red Stack and the distinctive form of governmentality that it expresses must be acknowledged as an entrant in the ongoing legal standards war over the appropriate extent and uses of data-driven surveillance. The implications of that development and possible responses have yet to be systematically considered.

Rule of Law 2.0 Revisited

Among all of the problems that legal institutions have confronted in the modern era, that of guaranteeing fundamental human rights and freedoms for all people has been the most difficult, and the movement to informational capitalism has exacerbated the challenges that project now confronts. If legal protections for fundamental human rights are to remain relevant and meaningful in the networked digital age, three kinds of institutional change are urgently necessary.

First, and self-evidently, institutions for recognizing and enforcing fundamental rights should work to counterbalance private economic power rather than reinforcing it. Obligations to protect fundamental rights must extend—enforceably—to private, for-profit entities if they are to be effective at all. As an example, early in the twentieth century, the U.S. courts developed a new constitutional doctrine for responding to ascendant industrial power in the form of the "company town." Under the doctrine, a private employer that had completely subsumed public functions—furnishing not only the houses in which its employees lived but also the stores in which they shopped, the streets and sidewalks on which they traveled, and the town squares in which they could gather—thereby also subjected itself to an obligation to protect their first amendment rights even when it did not like what they said.[98] The doctrine was narrow and its career short-lived, and in any event its emphasis on control of physical space and on state action as the conceptual baseline make it unsuited for direct transposition into the networked digital era. But the intuition that justified it is nonetheless instructive and has already begun to inform new ways of thinking about the legal responsibilities that should accompany the new forms of network power wielded by powerful information and communication intermediaries.[99]

Second, the importance of development, sustainability, and materiality for the conceptualization and enjoyment of fundamental rights points to the need to develop new modalities for oversight and enforcement that harness informational resources and tools

without falling into managerialist traps. Important initial steps in that project are conceptual. Securing the predicate conditions for human flourishing requires development discourses that are context-sensitive and methodologically diverse, and securing the predicate conditions for privacy, intellectual freedom, and political self-determination in the networked information era requires other kinds of universally-applicable material and operational guarantees.[100] Other steps are methodological and institutional. The task of ensuring progress toward broadly distributed development, sustainability, and algorithmic accountability is not one for courts alone or even primarily; it will also require new methods of administrative oversight and new thinking about the appropriate relationship(s) between administrators and courts.

Third and finally, protecting fundamental human rights in the networked information era requires more careful attention to the mechanisms of network-and-standard-based transnational governance, and particularly to the ways that powerful state and for-profit actors have exploited those mechanisms for their own benefit. The Red Stack is a clear threat to certain kinds of freedom, but it is also important to contend more systematically and effectively with its growing power and appeal worldwide, and it is simply wrong to think that populations worldwide see its principal competition, the U.S.-dominated regime of global informational capitalism, as a shining beacon of human freedom. The reality is both more complicated and simpler: building protection for fundamental human rights directly into institutions for economic and network governance has become an essential aspect of the rule-of-law project for transnational governance sketched at the end of the previous chapter.

---

[1] John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), https://perma.cc/H6KG-GQ7F.

[2] On the formation and operation of surveillant assemblages, see generally Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence: University Press of Kansis, 2007); Kevin D. Haggerty & Richard V. Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51 no. 4 (2000): 605-622.

[3] For thought-provoking provocations on the issues of bodies, borders, and flows see Itamar Mann, "Dialectic of Transnationalism: Unauthorized Migration and Human Rights, 1993-2013," Harvard International Law Journal 54 no. 2 (2013): 315-391; Mireille Hildebrandt, "The Virtuality of Territorial Borders," *Utrecht Law Review* 13 no. 2: 13-27 (2017), http://doi.org/10.18352/ulr.380.

[4] W. Michael Reisman, "Sovereignty and Human Rights in Contemporary International law," *American Journal of International Law* 84 no. 4 (1990): 866-876.

[5] Stefanie Khoury & David Whyte, *Corporate Human Rights Violations: Global Prospects for Legal Action* (New York: Routledge, 2017).

[6] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012); Anupam Chander, "Googling Freedom," *California Law Review* 99 no.1 (2011); 1-46.

[7] "GNI Principles on Freedom of Expression and Privacy," Global Network Initiative, https://perma.cc/J32J-GMXB; Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Fifth Annual Report, General Assembly, U.N. Doc. A/70/371 (Sept. 18, 2015) (by Ben Emmerson); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, U.N. Doc. A/HRC/29/32 (May 22, 2015) (by David Kaye); Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, General Assembly, U.N. Doc. A/69/397 (Sept. 23, 2014) (by Ben Emmerson); Special Rapporteur on the Promotion and Protection of the Right to Freedom of

Opinion and Expression, Human Rights Council, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (by Frank La Rue); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, U.N. Doc. A/HRC/17/27 (May 16, 2011) (by Frank La Rue); Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Council, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (by Martin Scheinin).

[8] Alan Rozenshtein, "Surveillance Intermediaries," *Stanford Law Review* 70 no. 1 (2018): 99-189; see also Samuel J. Rascoff, "Presidential Intelligence," *Harvard Law Review* 129 no. 3 (2016): 633, 662-64.

[9] Brad Smith, "The need for a Digital Geneva Convention" (Feb. 14, 2017), https://perma.cc/X2PG-89RG; Michael Beckerman, "Feds Must Listen to the Tech Industry if They Want to Stop Future WannaCry Attacks," *The Hill* (May 25, 2017), https://perma.cc/SZN8-VWHJ.

[10] On predictive policing, see Caroline Haskins, "Dozens of Cities Have Secretly Experimented with Predictive Policing Software," *Vice Motherboard* (Feb. 6, 2019), https://perma.cc/ZY4B-HDCH; Ali Winston, "Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology," *The Verge* (Feb. 27, 2018), https://perma.cc/3M2A-LZUC; Andrew Guthrie Ferguson, "Policing Predictive Policing," *Washington University Law Review* 94 no. 5 (2016): 1109-1189. On so-called tower dumps in criminal investigations, see Tim Cushing, "Cops Wanting To Track Movements Of Hundreds Of People Are Turning To Google For Location Records," *TechDirt* (Mar. 20, 2018), https://perma.cc/3K3Z-T8P9.

[11] On surveillance and repression of minority populations, see Margaret Hu, "Big Data Blacklisting," *Florida Law Review* 67 no .5 (2015): 1735-1810; Daithi Mac Sithigh & Mathias Siems, "The Chinese Social Credit System: A Model for Other Countries?," EUI Department of Law Working Paper 2019/01 (2019), https://perma.cc/9UNC-9H4H. On disinformation, see Henry Farrell & Bruce Schneier, "Common Knowledge Attacks on Democracy," Berkman Klein Center Research Publication No. 2018-7 (Oct. 2018), https://perma.cc/LU3Y-GB29; Ulises A. Mejias & Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture and Society* 39 no. 7 (2017): 1027-1042; Keith Collins, "See Which Facebook Ads Russians Targeted to People Like You," *The New York Times* (May 14, 2018), https://perma.cc/F4HM-WALR. On populism, nationalism, and mob violence, see Kenneth Roth, "World Report 2017: The Dangerous Rise of Populism," Human Rights Watch (2017), https://perma.cc/Q7AC-VKYS; Amanda Taub & Max Fisher, "When Countries Are Tinderboxes and Facebook Is a Match," *New York Times* (Apr. 21, 2018), https://perma.cc/LBC4-WGZQ.

[12] Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, "Limitless Worker Surveillance," *California Law Review* 105 no. 3 (2017): 735-776.

[13] For representative examples, see International Covenant on Civil & Political Rights, Dec. 16, 1966, 999 U.N.T.S. 172; International Covenant on Economic, Social & Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3; Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); Human Rights—Handbook for Parliamentarians, United Nations (2016), https://perma.cc/WG3Z-RTF3.

[14] For different perspectives, see Samuel R. Moyn, *Not Enough: Human Rights in an Unequal World* (Cambridge, Mass.: Belknap Press, 2018); Khoury & Whyte, *Corporate Human Rights Violations*, 14-17; Joseph R. Slaughter, "Hijacking Human Rights: Neoliberalism, the New Historiography, and the End of the Third World," *Human Rights Quarterly* 40 no. 4 (2018): 735-75.

[15] Some capabilities theorists, including most prominently Martha Nussbaum, have worked to develop lists of the centrally important capabilities. See Martha C. Nussbaum, *Creating Capabilities: The Human Development Approach* (Cambridge, Mass.: Harvard University Press, 2011), 31-36. A second strand of thinking about capabilities connects more directly to a radical democratic politics emanating from the global South. Its adherents, including most prominently Amartya Sen, define capabilities-related goals more generally, emphasizing the flexibility to pursue locally appropriate policies and the importance of respecting local variations in the forms of self-determination. See Amartya Sen, *Development as Freedom*, (New York: Oxford University Press, 1999); Amartya Sen, "Elements of a Theory of Human Rights," *Philosophy and Public Affairs* 32 no. 4 (2004): 315-356. Nussbaum and Sen have differed sharply on a number of matters, including the precise nature of the relationship between capabilities and rights, but those differences are unimportant for my purposes here.

[16] "IPCC Fact Sheet: What is the IPCC?," Intergovernmental Panel on Climate Change, https://perma.cc/K69J-6L8H (last visited June 26, 2018); "Sustainable Development Goals," United Nations, https://perma.cc/2L2P-V4B9 (last visited June 26, 2018).
[17] On the problem of enforceability, see Emilie M. Hafner-Burton & Kiyoteru Tsutsui, "Human Rights in a Globalizing World: The Paradox of Empty Promises," *American Journal of Sociology* 110 no. 5 (2005): 1373-1411.
[18] See, for example, Khoury & Whyte, *Corporate Human Rights Violations*; Kenneth Roth, "Defending Economic, Social and Cultural Rights: Practical Issues Faced by an International Human Rights Organization," *Human Rights Quarterly* 26 no. 1 (2004): 63-73.
[19] Katharine G. Young, *Constituting Economic and Social Rights* (New York: Oxford University Press, 2012), 2-15, 78-98, 139-91.
[20] On human rights, see Maria Green, "What We Talk about When We Talk about Indicators: Current Approaches to Human Rights Measurement," *Human Rights Quarterly* 23 no. 4 (2001): 1062-1097; Sally Engle Merry, "Measuring the World: Indicators, Human Rights, and Global Governance," *Current Anthropology* 52 no. S3 (2011): S83-S95. On sustainability, see Robert W. Kates, Thomas M. Parris, & Anthony A. Leiserowitz, "What Is Sustainable Development? Goals, Indicators, Values, and Practice," *Environment (Washington DC)* 47 no. 3 (2005): 8-21; "SDG Indicators" (July 6, 2017), United Nations, https://perma.cc/KEZ9-95U7; "The Sustainable Development Goals Report 2018," United Nations, 16-17, https://perma.cc/7R7V-LNQY. On indicators as expressions of governmentality, see Kevin E. Davis, et al., eds., *Governance by Indicators: Global Power through Quantification and Rankings* (New York: Oxford University Press, 2012).
[21] Sakiko Fukuda-Parr, Alicia Ely Yamin, & Joshua Greenstein, "The Power of Numbers: A Critical Review of Millennium Development Goal Targets for Human Development and Human Rights," *Journal of Human Development and Capabilities* 15 nos. 2-3 (2015): 105-117; Merry, "Measuring the World"; AnnJanette Rosga & Margaret L. Satterthwaite, "The Trust in Indicators: Measuring Human Rights," *Berkeley Journal of International Law* 27 no. 2 (2009): 253-315.
[22] Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, Human Rights Council, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (by John Ruggie); "The Ten Principles of the UN Global Compact," United Nations Global Compact, https://perma.cc/5LZV-AJYY (last visited June 26, 2018).
[23] Michael Blowfield & Jedrzej George Frynas, "Setting New Agendas: Critical Perspectives on Corporate Social Responsibility in the Developing World," *International Affairs* 81 no. 3 (2005): 499, 504-06.
[24] Khoury & Whyte, *Corporate Human Rights Violations*, 48-61.
[25] Environmental psychologist James Gibson coined the term "affordance" to refer to the enabling properties of physical environments and more specifically to particular kinds and ways that environments enable activity whether or not such enablement is consciously perceived or remarked. James J. Gibson, *The Ecological Approach to Visual Perception* (Boston: Houghton Mifflin, 1979), pp. 127-43. By analogy, an artifact's affordances are the kinds and ways of use that it enables whether or not such enablement is consciously perceived or remarked and whether or not particular uses were originally intended. The difference, of course, is that an artifact may be designed and redesigned to favor some affordances over others or to disafford certain uses outright. See generally Donald A. Norman, *The Design of Everyday Things* (Cambridge, Mass.: MIT Press, 1998), 9-11, 87-91; Donald A. Norman, "Affordance, Conventions, and Design," *Interactions* 6 no. 3 (May-June 1999): 38-42. Critically, the idea of an affordance does not reduce either to liberty (because affordances can also constrain) or to capability (because affordances need not translate into skill or improved flourishing); it is concerned simply with the range of uses that are possible. Like capabilities, however, affordances have collective (population-based) dimensions and implications.
[26] Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104 no. 3: (2016): 671, 677-93 (2016); Pauline T. Kim, "Data-Driven Discrimination at Work," *William and Mary Law Review* 58 no. 3 (2017): 857, 874-90.
[27] Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, "The Perpetual Lineup: Unregulated Police Face Recognition in America," Center on Privacy and Technology, Georgetown Law (Oct. 18, 2016), "E. Racial Bias," https://perma.cc/8FUT-RR3R; Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional

Accuracy Disparities in Commercial Gender Classification," in Conference on Fairness, Accountability and Transparency (New York, 2018), 77–91, https://perma.cc/G9HX-P5FX.

[28] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Northampton, Mass.: Edward Elgar, 2015), 174-83.

[29] For more detailed analyses, see Christopher Slobogin, "Policing as Administration," *University of Pennsylvania Law Review* 165 no. 1 (2016): 91, 93-109; Daphna Renan, "The Fourth Amendment as Administrative Governance," *Stanford Law Review* 68 no. 5 (2016): 1039, 1053-1067.

[30] Barry Friedman & Maria Ponomarenko, "Democratic Policing," *New York University Law Review*, 90 no. 6 (2015): 1827-1907, 1866-1870; Mark Tushnet, *The Hughes Court: 1930-1941: From Progressivism to Pluralism (Oliver Wendell Holmes Devise History of the Supreme Court)* (New York: Cambridge University Press, forthcoming), chapter 13.

[31] See, for example, Maryland v. King, 569 U.S. 435, 442-45 (2013) (DNA matching); Zoe Baird Budinger & Jeffrey H. Smith, "Ten Years After 9/11: A Status Report on Information Sharing," Markle Foundation (Oct. 12, 2011). On the evolution of a U.S. legal culture that has emphasized the (actual or attainable) neutrality of automated systems, see Meg Jones, "The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood," *Social Studies of Science* 47 no. 2 (2017) 216-39.

[32] Richard Berk, et al., "Fairness in Criminal Justice Risk Assessments: The State of the Art" (May 30, 2017), arXiv: 1703.09207; David Lehr & Paul Ohm, "Playing with the Data: What Legal Scholars Should Learn about Machine Learning," *U.C. Davis Law Review* 51 no. 2 (2017): 653, 669-702.

[33] For extensive analysis of the deficit and the beginnings of a "new administrativist" movement within criminal law scholarship, see Friedman & Ponomarenko, "Democratic Policing"; Renan, "The Fourth Amendment as Administrative Governance."

[34] See 50 U.S.C. § 1802(a)(1)(C)(2), § 1802(a)(4), § 1805, § 1806(a), § 1861(g), § 1881(e) (2018); Further Amendments to Executive Order 12333, United States Intelligence Activities, Exec. Order No. 13470, 73 Fed. Reg. 150 (July 30, 2008); U.S. Dept. of Justice, "The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection" (Oct. 31, 2003), https://perma.cc/R9HP-M65H; Daphna Renan, "The FISC's Stealth Administrative Law," in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, eds. Zachary K. Goldman & Samuel J. Rascoff eds. (New York: Oxford University Press, 2016), 121-40.

[35] Ira S. Rubinstein, Gregory T. Nojeim, & Ronald D. Lee, "Systematic Government Access to Private-Sector Data," in *Bulk Collection: Systematic Government Access to Private-Sector Data*, eds. Fred H. Cate & James X. Dempsey (New York: Oxford University Press, 2017), 5-46; Sarah Eskens, Ot van Daalen & Nico van Eijk, "10 Standards for Oversight and Transparency of National Intelligence Services," *Journal of National Security Law and Policy* 8 no. 3 (2016): 553-84.

[36] "Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2016," Administrative Office of the United States Courts (April 20, 2017), https://perma.cc/MPY5-2WWM. On accountability as performance, see Peter Miller, "Governing by Numbers: Why Calculative Practices Matter," *Social Research* 68 no. 2 (2001), 379-396

[37] "Transparency Reporting Index," Access Now, https://perma.cc/39KV-BZT3 (last visited June 25, 2018.

[38] Casey Newton, "Facebook Makes Its Community Guidelines Public and Introduces an Appeals Process," *The Verge* (April 24), 2018, https://perma.cc/Q63V-AVSU.

[39] See, for example, Lea Bishop Shaver, "Defining and Measuring A2K: A Blueprint for an Index of Access to Knowledge*, I/S: A Journal of Law and Policy for the Information Society* 4 no. 2 (Summer 2008): 235-269; Amy Kapczynski, "The Access to Knowledge Mobilization and the New Politics of Intellectual Property," *Yale Law Journal* 117 no. 5 (2008): 804-885.

[40] On these examples and distributed peer production generally, see Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006), 59-90.

[41] Zeynep Tufecki, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven: Yale University Press, 2017); Astrid Evrensel, ed., *Voter Registration in Africa: A Comparative Analysis*, (Johannesburg: Global Print, 2010); China Labour Bulletin, "Searching for the Union: The Workers' Movement in China 2011-2013" (Feb. 2014), 21-22, https://perma.cc/YNU6-WENY; Sanja Kelly, et al.,

"Silencing the Messenger: Communication Apps Under Pressure," Freedom on the Net 2016, Freedom House, https://perma.cc/A8F3-5L3Z.

[42] On early technology industry opposition to open source software, see Bryan Pfaffenberger, "The Rhetoric of Dread: Fear, Uncertainty, and Doubt (FUD) in Information Technology Marketing," *Knowledge, Technoogy and Policy* 13 no. 3 (2000): 78-92; Amy Harmon & John Markoff, "Internal Memo Shows Microsoft Executives' Concern Over Free Software," *New York Times* (Nov. 3, 1998), https://perma.cc/MG8C-7R8M. More recently, developers of proprietary software have used software patents as tools for defending proprietary software ecologies. For discussion and an attempted resolution, see Gideon Parchomovsky & Michael Mattioli, "Partial Patents," *Columbia Law Review* 111 no. 2 (2011): 207-253. On the difficulties that arise at the interfaces between proprietary and open licensing regimes, David S. Evans & Anne Layne-Farrar, "Software Patents and Open Source: The Battle over Intellectual Property Rights," *Virginia Journal of Law and Technology* 9 no. 3 (2004): 1-28.

[43] On coordinated resistance to open access by academic publishers, see Andi Sporkin, "Publishers Applaud 'Research Works Act,' Bipartisan Legislation to End Government Mandates on Private-Sector Scholarly Publishing," Association of American Publishers (Dec. 23, 2011), archived at https://perma.cc/M5Y5-UJZC; "Elsevier Withdraws Support for the Research Works Act" (Feb. 27, 2012), https://perma.cc/EMH9-JZXU; Samantha Murphy, "'Guerrilla Activist' Releases 18,000 Scientific Papers," *MIT Technology Review* (July 22, 2011), https://perma.cc/P4VJ-L9S9; Ian Graber-Stiehl, "Science's Pirate Queen" *The Verge* (Feb. 8, 2018) , https://perma.cc/DY7H-7D4Y.

[44] MacKinnon, *Consent of the Networked*, 51-66; Tufecki, *Twitter and Tear Gas*, 251-54.

[45] See Chapter 4, pp. 128-30.

[46] Sean M. O'Connor, "Creators, Innovators, & Appropriation Mechanisms," *George Mason Law Review* 22 no. 4 (2015): 991-96; 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; Tom Slee, *What's Yours Is Mine: Against the Sharing Economy* (New York, OR Books, 2017).

[47] Kenneth Roth, "World Report 2017: The Dangerous Rise of Populism," Human Rights Watch (2017), https://perma.cc/Q7AC-VKYS; Alexis C. Madrigal, "India's Lynching Epidemic and the Problem with Blaming Tech," *The Atlantic* (Sept. 25, 2018), https://perma.cc/MBA8-LNYZ; Farhad Manjoo, "The Problem with Fixing WhatsApp? Human Nature Might Get in the Way," *New York Times* (Oct. 24, 2018), https://perma.cc/3T57-PEPH; Amanda Taub & Max Fisher, "When Countries Are Tinderboxes and Facebook Is a Match," *New York Times* (Apr. 21, 2018), https://perma.cc/LBC4-WGZQ.

[48] Tufecki, *Twitter and Tear Gas*, 189-222.

[49] Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (New York: Oxford University Press, 2018), 1.

[50] See, for example, Madrigal, "India's Lynching Epidemic and the Problem with Blaming Tech"; Manjoo, "The Problem with Fixing WhatsApp?."

[51] On the essential structural characteristics of a networked public sphere, see Mike Ananny, *Networked Press Freedom: Creating Infrastructures for a Public Right to Hear* (Cambridge, Mass.: MIT Press, 2018); see also Erin C. Carroll, "Platforms and the Fall of the Fourth Estate," *Maryland Law Review* 78 (forthcoming 2019).

[52] On famous instances of anonymous advocacy and whistleblowing, see Victoria Smith Ekstrand & Cassandra Imfeld Jeyaram, "Our Founding Anonymity: Anonymous Speech during the Constitutional Debate," *American Journalism* 28 no. 3 (2011): 35-60; Bob Woodward, *The Secret Man: The Story of Watergate's Deep Throat* (New York: Simon and Schuster, 2005); William E. Scheuerman, "Whistleblowing as Civil Disobedience: The Case of Edward Snowden," *Philosophy & Social Criticism* 40 no. 7 (2014): 609-628. On surveillance as a tool for violation of human rights, see Edwin Black, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation* (New York: Crown Books, 2001); William Seltzer & Margo Anderson, "The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses," *Social Research* 68 no. 2 (2000): 481-513; Louise I. Shelley, *Policing Soviet Society: The Evolution of State Control* (New York: Routledge, 1996), 109-192; Sarah McKune, "'Foreign Hostile Forces': The Human Rights Dimension of China's Cyber Campaigns," *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, eds. Jon R. Lindsay, Tai Ming Cheung & Derek S. Reveron (New York: Oxford University Press, 2015), 260-293.

[53] On identification requirements in the corporate context, see, for example, 8 Del. Code §§ 131-132 (2018) (identification of registered agent of corporation), § 502(a) (disclosure of names and addresses of corporate directors on annual franchise tax report). On identification requirements in connection with stock transfers and domain name transfers, see 6 Del. Code §§ 8-401 *et seq* (2018). (registration of stock transfers); "Will My Name and Contact Information Become Publicly Available?," FAQs, ICANN (Jan. 21, 2014), https://perma.cc/68QL-55KJ. On identification of professional license applicants, see 21 N.C. Admin. Code §12.0505 (2018) (contractor licensing); 20 Leyes Puerto Rico Ann. § 133f (2018) (medical professional licensing). On land transfer recordation, see, for example, Florida Stats., tit. XL § 695.01(1) (2018).

[54] On uses of encryption by journalists and activists around the world, see MacKinnon, *Consent of the Networked*, 227-37; Andy Greenberg, "Laura Poitras on the Crypto Tools That Made Her Snowden Film Possible," *Wired* (Oct. 15, 2014); Eva Galperin, "Don't Get Your Sources in Syria Killed," Committee to Project Journalists (May 21, 2012), https://perma.cc/37NY-TZAQ; Roland Taylor, "The Need for a Paradigm Shift toward Cybersecurity in Journalism," *National Cybersecurity Institute Journal* 1 no. 3 (2015): 45-47. On the U.S. and Canada more specifically, see Eva Galperin, "Cell Phone Guide for Occupy Wall Street Protesters (and Everyone Else)," Electronic Frontier Foundation (Oct. 14, 2011), https://perma.cc/7NAC-M9YB; Jenna McLaughlin, "The FBI vs. Apple Debate Just Got Less White," *The Intercept* (Mar. 8, 2016), https://perma.cc/LM53-CRJG.

[55] Brian X. Chen, "Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.," *New York Times* (Sept. 27, 2014), https://perma.cc/RY6Q-VX9K; Bruce Schneier, "Worldwide Encryption Products Survey" (Feb. 11, 2016), https://perma.cc/5V9S-JYCN; 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.

[56] Primavera DeFilippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, Mass.: Harvard University Press, 2018).

[57] On cryptocurrency projects and social irresponsibility, see Binyamin Appelbaum, "Is Bitcoin a Waste of Electricity, or Something Worse?," *New York Times* (Feb. 28, 2018), https://perma.cc/7G2H-W9T6; Nellie Bowles, "Making a Crypto Utopia in Puerto Rico," *New York Times* (Feb. 2, 2018), https://perma.cc/BZL4-AC5K**.** On the institutional dimensions of cryptocurrency projects, see Kevin Werbach, *A New Architecture of Trust: Law, Governance, and the Blockchain* (Cambridge, Mass.: MIT Press, 2018); see also Primavera De Filippi & Benjamin Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure," *Internet Policy Review* 5 no. 3 (2016): DOI: 10.14763/2016.3.427.

[58] See, for example, 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.

[59] Mark Fenster, "'Bullets of Truth': Julian Assange and the Politics of Transparency," https://perma.cc/GA8W-8VAZ (last visited Jan. 27, 2019); Andy Greenberg, *This Machine Kills Secrets: How Wikileaks, Cypherpunks, and Hactivists Aim to Free the World's Information* (New York: Plume, 2012), 285-313; Bill Keller, "Dealing With Assange and the Wikileaks Secrets," *New York Times Magazine* (Jan. 26, 2011), https://perma.cc/XP5Y-525Z; see also Andy Greenberg, "How Reporters Pulled Off The Panama Papers, The Biggest Leak in Whistleblower History," *Wired* (April 4, 2016), https://perma.cc/WJF9-EUMP.

[60] Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" (Jan. 6, 2017), 2-5, https://perma.cc/FPA6-NAZX; David A. Graham, "Is WikiLeaks a Russian Front?," *The Atlantic* (Nov. 29, 2018), https://perma.cc/W3HT-RMV5.

[61] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (New York: Verso, 2014); Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton: Princeton University Press), 183-205.

[62] On the ways that developing norms regarding bilateral investment treaties align with or depart from different economic theories about international investment flows, see Kenneth J. Vandevelde, "The Political Economy of a Bilateral Investment Treaty," *American Journal of International Law* 92 no. 4 (1998): 621-41.

[63] Joachim Pohl, Kekeletso Mashigo,& Alexis Nohen, "Dispute Settlement Provisions in International Investment Agreements: A Large Sample Survey," OECD Working Papers on International Investment 2012/02 (2012), https://perma.cc/VN6T-GT64.

[64] Metalclad Corp. v. The United Mexican States, 40 I.L.M. 36 (NAFTA ch. 11 Arb. Trib. Aug. 30, 2000). For the relevant provision of NAFTA, see North American Free Trade Agreement, U.S.-Can.-Mex., ch. 11, art 1110, Dec. 17, 1992, 32 I.L.M. 289 (1993).
[65] Penn Central Transportation Co. v. New York City, 438 U.S. 104, 124-25 (1978); see also Tahoe-Sierra Preservation Council, Inc. v. Tahoe Regional Planning Agency, 535 U.S. 302, 336 (2002); Murr v. Wisconsin, 137 S. Ct. 1933, 1937 (2017).
[66] U.S. Model Bilateral Investment Treaty, Annex B.4 (2012); see Vicki Been & Joel C. Beauvais, "The Global Fifth Amendment? NAFTA's Investment Provisions and the Misguided Quest for an International Regulatory Takings Doctrine," *New York University Law Review* 30 no. 1 (2003): 30-143.
[67] Christine Willmore, "Of Missiles and Mice: Property Rights in the USA," in *Modern Studies in Property Law*, vol. 1, ed. Elizabeth Cooke (Portland, Ore.: Hart Publishing, 2000), 99, 106-08; see also Steven J. Eagle, "The Birth of the Property Rights Movement," Policy Analysis No. 558, Cato Institute (Dec. 15, 2005), https://perma.cc/Q9U2-V55U.
[68] The classic analysis is Frank I. Michelman, "Property, Utility, and Fairness: Comments on the Ethical Foundations of 'Just Compensation' Law, *Harvard Law Review* 80 no. 6 (1967): 1165-1258.
[69] For useful summaries, see James Gathii & Cynthia Ho, "Regime Shifting of IP Lawmaking and Enforcement from the WTO to the International Investment Regime," *Minnesota Journal of Law, Science and Technology* 18 no. 2 (2017): 427-516; Peter K. Yu, "The Investment-Related Aspects of Intellectual Property Rights," *American University Law Review* 66 no. 3 (2017): 829-910.
[70] Rochelle Dreyfuss & Susy Frankel, "From Incentive to Commodity to Asset: How International Law Is Reconceptualizing Intellectual Property," *Michigan Journal of International Law* 36 no. 4 (2015): 557-602. Peter Yu observes that the trend toward reconceptualizing intellectual property interests as investments has been underway for longer than Dreyfuss and Frankel recognize. Yu, "The Investment-Related Aspects of Intellectual Property Rights," 837-45.
[71] William Mauldin, "Canada, Mexico Reject Proposal to Rework NAFTA Corporate Arbitration System," *Wall Street Journal* (Jan. 28, 2018), https://perma.cc/65HB-SK3J; Richard Holwill, "New NAFTA May Put 'America First,' but It Puts U.S. Investors Last," *The Hill* (Nov. 17, 2018), https://perma.cc/AMK7-HJEC.
[72] Court of Justice of the European Union, Press Release, Judgment in Case C-284/16, Slowakische Republik v. Achmea BV, 6 March 2018; European Commission, Press Release, Commission proposes new Investment Court System for TTIP and other EU trade and investment negotiations, 16 Sept. 2015, https://perma.cc/RZP3-AZKG; European Commission, Recommendation COM(2017) 493 final for a Council Decision authorising the opening of negotiations for a Convention establishing a multilateral court for the settlement of disputes, 13 Sept. 2017, https://perma.cc/TEG8-FF7A. For discussion, see Rob Howse, "Designing a Multi-Lateral Investment Court: Issues and Options," *Yearbook of European Law* 36 no. 1 (2017): 209-236.
[73] European Convention on Human Rights, art. 8; U.S. Const. amdts. I, IV, V, IX.
[74] For an attempt to systematize the European approach to corporations as bearers of fundamental rights, see Peter Oliver, "Companies and their Fundamental Rights: A Comparative Perspective," *International & Comparative Law Quarterly* 64 no. 3 (2015): 661-696.
[75] On European overreach, see, for example, Tim Cushing, "Italian Government Criminalizes 'Fake News,' Provides Direct Reporting Line To State Police Force," *TechDirt* (Jan. 24, 2018), https://perma.cc/7BCJ-7SSC; Tim Cushing, "Spanish Citizen Sentenced To Jail For Creating 'Unhealthy Humoristic Environment'" *TechDirt* (May 5, 2017), https://perma.cc/MJC7-USWD. On U.S. overreach, see, for example, Jaclyn Peiser, "Journalist Swept Up in Inauguration Day Arrests Faces Trial," *New York Times* (Nov. 14, 2017), https://perma.cc/XCW6-Z3QP; Richard Wolf, "First Amendment Victory is Florida Man's Second at Supreme Court," *USA Today* (June 18, 2018), https://perma.cc/H5ZC-GH3U.
[76] Stefan Kulk & Frederik Zuiderveen Borgesius, "Privacy, Freedom of Expression, and the Right to be Forgotten in Europe," in *The Cambridge Handbook of Consumer Privacy*, eds. Evan Selinger, Jules Polonetsky, & Omer Tene (New York: Cambridge University Press, 2018), 301-320; Kyu Ho Youm & Ahran Park, "The 'Right to Be Forgotten' in European Union Law: Data Protection Balanced With Free Speech?," J*ournalism & Mass Communication Quarterly* 93 no. 2 (2016): 273-295, 284-290; "Factsheet—Hate Speech," European Court of Human Rights (March 2019), https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.

[77] On privacy-as-control generally, see Daniel J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 no. 7 (2013): 1880-1903.
[78] Regulation (EU) 2016/679, 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 and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, Art. 7, 2016 O.J. (L 119); see also Opinion of the Article 29 data protection working party 07/2011 on the definition of consent (WP 187). On purpose limitation, see Regulation (EU) 2016/679, Art. 5(1)(b); Opinion of the Article 29 data protection working party of 03/2013 on purpose limitation (WP 203).
[79] On the role and the impossibility of consent within the European system, see Bert-Jaap Koops, "The Trouble with European Data Protection Law," *International Data Privacy Law* 4 no. 4 (2014): 250-261.
[80] On the existence and scope of the right to an explanation, see Andrew D. Selbst & Julia Powles, "Meaningful Information and the Right to an Explanation," *International Data Privacy Law* 7 no. 4 (2017): 233-242. On the difficulties associated with operationalizing it, see Lilian Edwards & Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law and Technology Review* 16 (2017): 18-84; Andrew D. Selbst & Solon Barocas, "The Intuitive Appeal of Explainable Machines," *Fordham Law Review* 86 no. 3 (2018): 1085-1139.
[81] For more detailed development of this argument, see Julie E. Cohen, "Turning Privacy Inside Out," *Theoretical Inquiries in Law* 20 no. 1 (2019):1-31.
[82] On the tradeoffs and conflicting incentives created by "privacy by design" mandates and data subject access rights, see Michael Veale, Reuben Binns, & Jef Ausloos, "When Data Protection by Design and Data Subject Rights Clash," *International Data Privacy Law* 8 no. 2 (2018): 105-123.
[83] As Paul Schwartz explains, this struggle is deeply embedded in the history of data protection law. Paul Schwartz, "The E.U.-U.S. Privacy Collision." *Harvard Law Review* 126 no. 7 (2013): 1966-2009.
[84] Cf. Grainne de Burca, "Human Rights Experimentalism," *American Journal of International Law* 111 no. 2 (2017): 277-316.
[85] For a through and intrinsically optimistic account of the potential for corporate resistance, see example, Chander, "Googling Freedom."
[86] Margaret E. Roberts, *Censored: Distraction and Diversion inside China's Great Firewall* (Princeton; Princeton University Press, 2018), 21-36, 137-188; Human Rights Watch, "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship" (Aug. 2006), 15-17, https://perma.cc/RM5N-RVNG.
[87] See, for example, Yao Yang, "Towards a New Digital Era: Observing Local E-Government Services Adoption in a Chinese Municipality," *Future Internet* 9 (2017): doi:10.3390/fi9030053. On the Chinese model generally, see Min Jiang, "Authoritarian Informationalism: China's Approach to Internet Sovereignty," *SAIS Review of International Affairs* 30 no. 2 (2010): 71-89; Min Jiang & King-Wa Fu, "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?," 10 no. 4 (2018): 372-92.
[88] MacKinnon, *Consent of the Networked*, 34-50.
[89] "How Private Are Your Favorite Messaging Apps?," Amnesty International (Oct. 21, 2016), https://perma.cc/G4AM-ENSB; John Naughton, "What Price Privacy When Apple Gets Into Bed with China," *Guardian* (Mar. 4, 2018), https://perma.cc/U5TL-S48Q; Jeffrey Knockel, et al., "(Can't) Picture This: An Analysis of Image Filtering on WeChat Moments," Citizen Lab (Aug. 14, 2018), https://perma.cc/DZ67-GHX4.
[90] Roberts, *Censored*, 80-90, 190-222.
[91] See, for example, Anna Mitchell & Larry Diamond, "China's Surveillance State Should Scare Everyone," *The Atlantic* (Feb. 2, 2018), https://perma.cc/S8XS-EJ5Z; Vicky Xiuzhong Xu & Bang Xiao, "China's Social Credit System Seeks to Assign Citizens Scores, Engineer Social Behaviour," ABC News (Apr. 1, 2018), https://perma.cc/K42Q-TZNY.
[92] James A. Millward, "What It's Like to Live in a Surveillance State," *New York Times* (Feb. 3, 2018), https://perma.cc/J4M5-QJF3; Chris Buckley, "China Is Detaining Muslims in Vast Numbers. The Goal: Transformation," *New York Times* (Sept. 8, 2018), https://perma.cc/A7TM-764J.
[93] For some examples, see Charles Rollet, "The Odd Reality of Life under China's Social Credit System," *Wired* (June 5, 2018), https://perma.cc/VFJ2-PY6F.
[94] Xin Dai, "Toward a Reputation State: The Social Credit System Project of China," working paper (June 10, 2018), http://dx.doi.org/10.2139/ssrn.3193577.

[95] Lucy Hornby, Sherry Fei Ju, & Louise Lucas, "China Cracks Down on Tech Credit Scoring," *Financial Times* (Feb. 4, 2018), https://perma.cc/S8GD-FTM9; Mac Sithigh & Siems, "The Chinese Social Credit System: A Model for Other Countries?."
[96] "The Mobile Payments Race: Why China Is Leading the Pack — for Now," Knowledge@Wharton, Jan. 17, 2018, https://perma.cc/XA3N-PSLN; Alexis C. Madrigal, "The Strange Brands in Your Instagram Feed," *The Atlantic* (Jan. 10, 2018), https://perma.cc/8B32-Z6V5.
[97] On consumer offerings, see "The Mobile Payments Race: Why China Is Leading the Pack — for Now," Knowledge@Wharton (Jan. 17, 2018), https://perma.cc/XA3N-PSLN; "China's WeChat Hits 1bn User Accounts Worldwide," *Financial Times* (Mar. 5, 2018), https://perma.cc/Z7Z7-PGV5; "Alibaba and Amazon Look to Go Global," *Economist* (Oct. 28, 2017), https://perma.cc/FHM4-BJXD. On surveillance-ready offerings for governments, see Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *The Atlantic* (June 18, 2018), https://perma.cc/YFY8-KYM5.
[98] Marsh v. Alabama, 326 U.S. 501 (1946); for a good summary of the doctrine's emergence and decline, see State v. Wicklund, 589 N.W.2d 793 Minn. (1999).
[99] Kiel Brennan-Marquez, "The Constitutional Limits of Private Surveillance," *Kansas Law Review* 66 no. 3 (2018): 485-521; see also Christoph B. Graber, "Bottom-Up Constitutionalism: The Case of Net Neutrality," *Transnational Legal Theory* 7 no. 4 (2016): 524-53.
[100] For development of these and similar ideas, see.Cohen, "Turning Privacy Inside Out"; see also Mireille Hildebrandt, "Agonistic Machine Learning," *Theoretical Inquiries in Law* 20 no. 1 (forthcoming 2019); Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Mass.: Harvard University Press, 2018).