View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Duke Law Scholarship Repository

INTERNET UTOPIANISM AND THE PRACTICAL INEVITABILITY OF LAW

JULIE E. COHEN

INTRODUCTION

Writing at the dawn of the digital era, 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 both Barlow and the cyberlaw scholars who took up his call 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 they 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. More generally, in the networked information era, protections for fundamental human rights—both on- and offline—have begun to fail comprehensively.

Cyberlaw scholarship in the Barlowian mold isn't to blame for the worldwide erosion of protections for fundamental rights, but it also hasn't helped as much as it might have. In this essay, adapted from a forthcoming book on the evolution of legal institutions in the information era,[2] I identify and briefly examine three intersecting flavors of internet utopianism in cyberlegal thought that are worth reexamining: utopianism about platforms for distributed cultural and political production (and concomitant failure to reckon with the transformative force of informational capitalism); utopianism about anonymity as a force for institutional disruption (and concomitant failure to acknowledge the essential role of institutions in cabining the human capacity for malice and mayhem); and utopianism about the relationship between information and communication networks and human freedom (and concomitant failure to contend with the powerful and inherently informational mechanisms by which existing protections for human rights are increasingly outflanked and coopted). It has become increasingly apparent that functioning legal institutions have

---

[1] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 18 DUKE L. & TECH. REV. 5, 5 (2012) (originally published on Feb. 8, 1996).

[2] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (Oxford University Press, forthcoming 2019).

indispensable roles to play in protecting and advancing human freedom. It has also become increasingly apparent, however, that the legal institutions we need are different than the ones we have.

I. THE PLATFORMIZATION OF EVERYTHING: DISTRIBUTED PRODUCTION, DATA PRIVACY, AND THE PROBLEM OF INFORMATIONAL CAPITALISM

Some of the scholars and activists who took up Barlow's call prophesied that decentralized coordination of cultural and political activity by networked communities of peers would increasingly displace centralized, top-down control of cultural and political production, with transformative and broadly freedom-promoting effects.[3] Without question, decentralized production strategies have expanded access to information and political capacity-building for people all around the world and have come to be regarded as essential tools for fostering human freedom in the networked information era. The grander visions of wholesale, democratizing transformation in political economy and in government have not materialized, however. Instead, strategies for decentralized cultural and political production have fueled a very different kind of transformation, organized around the emergence of dominant global platforms that afford new vantage points for surveillance, data harvesting, surplus extraction, and manipulation.

Some of the obstacles to commons-based cultural and political production were predictable. Leading software firms initially 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.[4] The major content industries have resisted

---

[3] *See, e.g.*, YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006); Dan Hunter & F. Gregory Lastowka, *Amateur-to-Amateur*, 46 WM. & MARY L. REV. 951 (2004); David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law*, *in* COORDINATING THE INTERNET 62–91 (Brian Kahin & James H. Keller eds., 1997).

[4] *See* David S. Evans & Anne Layne-Farrar, *Software Patents and Open Source: The Battle over Intellectual Property Rights*, 9 VA. J.L. & TECH. 1 (2004); Bryan Pfaffenberger, *The Rhetoric of Dread: Fear, Uncertainty, and Doubt (FUD) in Information Technology Marketing*, 13 KNOWLEDGE, TECH. & POL'Y 78 (2000).

commons-based production and open-access distribution strategies for educational and cultural materials and have devised a continuing stream of legal and technological methods for asserting control over their products and business models.[5] Political activists, for their part, quickly learned that the networked digital information environment afforded not only unprecedented scope for dissent and resistance but also new, hidden control points for state censorship and surveillance.[6]

Other failure modes for commons-based production were wholly unanticipated, and that was so in part because internet utopian projects elevated openness and freedom from control over all other priorities, most notably including privacy and data protection. Evangelists for internet openness, confident in the ability of enlightened netizens to assert their own privacy interests, painted calls for stricter regulation as threats to the net's most fundamental values.[7] But openness has proved a double-edged sword. The allure of open content models has been a powerful factor driving the emergence of new information businesses whose revenue models are based on harvesting and monetizing the data flows generated by content developers and content users, including global platform giants Google, Facebook, and Amazon and a host of

---

[5] *See, e.g.*, Andi Sporkin, *Publishers Applaud "Research Works Act," Bipartisan Legislation to End Government Mandates on Private-Sector Scholarly Publishing*, ASS'N OF AMERICAN PUBLISHERS (Dec. 23, 2011), https://perma.cc/M5Y5-UJZC; Ian Graber-Stiehl, *Science's Pirate Queen*, VERGE (Feb. 8, 2018), https://perma.cc/DY7H-7D4Y. *See generally* Anne-Marie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 ORE. L. REV. 81 (2010); Anne-Marie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1524 (2015); Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 GEO. L.J. 1 (2006); Julie E. Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347 (2005); Rebecca Tushnet, *All of This Has Happened Before and All of This Will Happen Again: Innovation in Copyright Licensing*, 29 BERKELEY TECH. L.J. 1447 (2014).

[6] REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 51–66 (2012); ZEYNEP TUFECKI, TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST 251–54 (2017).

[7] *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142–62 (1998). *But see* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

others.[8] Platform protocols invite commons-based production arrangements, and commons-based production arrangements in turn reinforce platform logics of data harvesting and proprietary, algorithmic knowledge production.[9]

The results of distributed cultural and political production also are not inevitably democracy-promoting, and predictions to the contrary have, in retrospect, come to seem extraordinarily naïve. The particular quality-control mechanisms that keep open source software robust and secure and Wikipedia reliable and (mostly) objective work far less well (or not at all) within massively-intermediated environments that are optimized to advertiser-driven platform revenue models. In such environments, the vaunted "wisdom of crowds" is a scalar, not a vector. Algorithmic processes optimized to boost click-through rates and prompt social sharing heighten the volatility of online interactions, and surveillant assemblages designed to enhance capabilities for content targeting and behavioral marketing create powerful—and easily weaponized—stimulus-response feedback loops.[10] The result is a sociotechnical apparatus that is also optimized for stoking outrage and deepening preexisting political, ideological, and cultural divisions.

Under conditions of pervasive, data-driven intermediation—enabled in part by thought leaders' failure to take privacy and data protection seriously as worthy and freedom-advancing projects—power from below becomes power directed toward whatever purpose its organizers want to advance. Platform-based, massively-intermediated environments have become fertile breeding grounds for conspiracy theories (including coordinated campaigns to foster denialism about climate change, vaccination, and similar matters), disinformation campaigns designed to discredit political actors and institutions, and virulent forms of bigotry, ideological extremism, and ethnic

---

[8] *See* TOM SLEE, WHAT'S YOURS IS MINE: AGAINST THE SHARING ECONOMY (2017); Guy Pessach, *Beyond IP—The Cost of Free: Informational Capitalism in a Post IP Era*, 54 OSGOODE HALL L. REV. 225 (2016).

[9] *See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213 (2018); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 153–61 (2017).

[10] On clickbait and social sharing strategies, see Bryan Gardiner, *You'll Be Outraged at How Easy It Was to Get You to Click on This Headline*, WIRED (Dec. 18, 2015), https://perma.cc/4QXK-5M56; Alice Marwick, *Why Do People Share Fake News? A Sociotechnical Model of Media Effects*, 2 GEO. L. TECH. REV. 474 (2018), https://perma.cc/DT4C-94E. On surveillance as behavioral conditioning, see generally SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

nationalism.[11] 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. It has become more difficult to enlist networked publics in the work of building movements capable of growing, sustaining themselves, and organizing for change in the real world.[12]

Among scholars and commentators who write about digital media, a debate has raged about whether it is fair to blame dominant 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.[13] Others argue that such explanations unfairly blame platforms for longstanding dysfunctions that are not of their creation.[14] Without question, part of the problem with Facebook and others is the preexisting social and cultural divisions that information cascades amplify. That logic, though, undercuts the optimism about bottom-up organization that the Internet's founding visionaries expressed. Part of the problem with Facebook and other platforms is people, easily distracted, highly susceptible to misinformation, and prone to herd behavior. It also undercuts the logic that designated the internet and its networked virtual spaces as sites of utopian separation for the life of the mind. Platform-based environments are inextricably embedded in real-world societies; platform governance requires real-world, institutional (i.e., non-utopian) solutions.

---

[11] *See* Jonathan Albright, *Untrue-Tube: Monetizing Misery and Disinformation*, MEDIUM (Feb. 25, 2018), https://perma.cc/Y6BM-CQCD; Rob Faris, et al., *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*, BERKMAN KLEIN CTR. FOR INTERNET AND SOCY' AT HARVARD UNIV. (Aug. 16, 2017), https://perma.cc/8SCW-R9HE; Alice Marwick & Rebecca Lewis, *Media Manipulation & Disinformation Online*, DATA & SOC'Y (2017), https://perma.cc/356L-XZQA; Christopher Paul & Miriam Matthew, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, RAND CORP.: PERSPECTIVES (2016), https://perma.cc/CLB5-A5AG; Julia Carrie Wong, *How Facebook and YouTube Help Spread Anti-Vaxxer Propaganda*, GUARDIAN (Feb. 1, 2019), https://perma.cc/3NN6-R5Q7.

[12] *See* TUFECKI, *supra* note 6, at 189–222 (discussing examples).

[13] SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 1 (2018).

[14] *See, e.g.*, Alexis C. Madrigal, *India's Lynching Epidemic and the Problem with Blaming Tech*, ATLANTIC (Sept. 25, 2018), https://perma.cc/MBA8-LNYZ.

II. UNBUNDLING INSTITUTIONS: ANONYMITY, TRUST AND THE PROBLEM OF SCALE

Other scholars and activists who took up Barlow's call focused on enabling capabilities for distributed, anonymous communication and coordination, and here again the scorecard is mixed. It is indisputable that anonymity has played an essential structural role in modern democratic societies and equally indisputable that networked information and communication technologies have provided anonymous dissenters with invaluable tools for naming and challenging abuses of economic and political power. Around the world, both activists pursuing social change and journalists reporting on controversial topics now rely on capabilities for anonymous, networked communication to protect themselves and their sources, and projects dedicated to creating, maintaining, and improving such capabilities have become sites of ongoing research and activism in their own right.[15] Persistent and intractable questions remain, however, about the extent to which behaviors that historically have functioned as safety valves within more complex institutional structures can assume more central roles in the project of securing fundamental rights and freedoms for all people.

To begin with, and continuing the themes developed in the previous section, anonymous online activity has valences that are more complicated than romanticized narratives equating anonymity with press freedom and democratic self-determination acknowledge. The projects of building and sustaining utopia require utopians—people united in their unequivocal commitment to the ground truths and operating norms of a utopian project. Some utopian ground truths and operating norms are ugly and unworthy of anyone's allegiance. 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.

---

[15] *See* MACKINNON, *supra* note 6, at 227–37; Eva Galperin, *Cell Phone Guide for Occupy Wall Street Protesters (and Everyone Else)*, ELEC. FRONTIER FOUND. (Oct. 14, 2011), https://perma.cc/7NAC-M9YB; Eva Galperin, *Don't Get Your Sources in Syria Killed*, COMMITTEE TO PROJECT JOURNALISTS (May 21, 2012), https://perma.cc/37NY-TZAQ; Andy Greenberg, *Laura Poitras on the Crypto Tools That Made Her Snowden Film Possible*, WIRED (Oct. 15, 2014); Jenna McLaughlin, *The FBI vs. Apple Debate Just Got Less White*, INTERCEPT (Mar. 8, 2016), https://perma.cc/LM53-CRJG.

More generally, the trajectories of projects designed to scale up certain types of anonymous interaction and communication demonstrate that breaking things is easier than rebuilding them. Consider two much-discussed examples involving anonymous infrastructures for enabling fundamental market and governance functions. The first is the blockchain, a set of technological protocols for enabling distributed, secure authentication of transactions and credentials. In theory, such technologies might be deployed within existing institutional fabrics in ways that eliminate opportunities for corruption, waste, and rent-seeking.[16] 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.[17] The second example is WikiLeaks, which rapidly attained heroic status among civil liberties advocates for its stated commitment to facilitating anonymous whistleblowing about powerful wrongdoers. WikiLeaks, however, is not a free press advocacy organization. It rejects certain essential editorial and quality control functions that the press as an institution typically has performed and espouses an endgame that is far more disruptive.[18] WikiLeaks' evolving role in the era of ascendant platform-based disinformation campaigns is proof that the distinction matters.[19]

---

[16] *See generally* PRIMAVERA DEFILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018).

[17] *See, e.g.*, Binyamin Appelbaum, *Is Bitcoin a Waste of Electricity, or Something Worse?*, N.Y. TIMES (Feb. 28, 2018), https://perma.cc/7G2H-W9T6; Nellie Bowles, *Making a Crypto Utopia in Puerto Rico*, N.Y. TIMES (Feb. 2, 2018), https://perma.cc/BZL4-AC5K. *See generally* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (2018).

[18] *Compare* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311 (2011) (painting WikiLeaks heroically), *with* ANDY GREENBERG, THIS MACHINE KILLS SECRETS: HOW WIKILEAKS, CYPHERPUNKS, AND HACTIVISTS AIM TO FREE THE WORLD'S INFORMATION 285–313 (2012) (developing a more neutral account); *see also* Bill Keller, *Dealing With Assange and the Wikileaks Secrets*, N.Y. TIMES MAG. (Jan. 26, 2011), https://perma.cc/XP5Y-525Z (discussing editorial considerations). On the institutional functions of the press, see Erin C. Carroll, *Platforms and the Fall of the Fourth Estate: Looking Beyond the First Amendment to Protect Watchdog Journalism*, 79 MD. L. REV., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300966.

[19] *See* Mark Fenster, *'Bullets of Truth': Julian Assange and the Politics of Transparency* (Univ. of Fla. Levin Coll. of Law, Research Paper No. 19-12, Jan. 27, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3323950; David A. Graham, *Is WikiLeaks a Russian Front?*, ATLANTIC (Nov. 29, 2018),

As both of those examples illustrate, moreover, other obstacles to coding scalable, anonymity-centered, democratic institutions are cultural. As Gabriella Coleman has shown, hacker culture speaks the intertwined languages of liberal individualism and libertarianism and posits enlightened self-reliance and, by necessary implication, technical meritocracy as cardinal virtues.[20] Those commitments in turn complicate efforts to transform digital anonymity from a tool for resistance to the foundation of a stable framework for guaranteeing fundamental rights and freedoms. Understood as (anti-)institutional projects, both WikiLeaks and blockchain-based cryptocurrency projects reflect ideologies that are powerfully utopian but not particularly democratic. They express and reproduce a particular kind of moral and ideological purity that is inconsistent with a broadly inclusive social compact. And they illustrate powerfully that, although capabilities for anonymous online communication and coordination have played and will continue to play an important role in efforts to secure fundamental rights and freedoms for all people, such capabilities cannot stand in for other kinds of institution-building. Structurally speaking, anonymous dissent and opposition are safety valves. Achieving durable, effective protection for fundamental rights and freedoms also requires other mechanisms.

III. UNRAVELING FUNDAMENTAL RIGHTS: INFORMATION, NETWORKS, AND THE PROBLEM OF POWER

Both strands of utopian thinking about internet-enabled governance that I have just described are rooted in a more general habit of utopian thinking about the relationship between information and human freedom. That habit is deeply ahistorical. Networked information technologies are not simply instruments of liberation, nor do they simply afford new avenues for control and cooptation. Over the course of many decades, social and legal institutions have come to reflect the shaping influence of the "control revolution" that began with the introduction of automated information systems into industrial-era factories and

---

https://perma.cc/W3HT-RMV5; *see also* Andy Greenberg, *How Reporters Pulled Off The Panama Papers, The Biggest Leak in Whistleblower History*, WIRED (Apr. 4, 2016), https://perma.cc/WJF9-EUMP (describing investigative journalists' use of encryption tools to coordinate a controlled leak of documents detailing a massive scheme for global tax evasion).

[20] *See generally* GABRIELLA COLEMAN, HACKER, HOAXER, WHISTLEBLOWER, SPY: THE MANY FACES OF ANONYMOUS (2014); GABRIELLA COLEMAN, CODING FREEDOM: THE ETHICS AND AESTHETICS OF HACKING 183–205 (2012).

businesses.[21] The processes of institutional evolution have produced new institutional configurations and competencies that are intensively informational in character and that have posed difficult challenges for traditional approaches to conceptualizing and enforcing fundamental human rights.

The same networked capabilities that enable widespread public access to information also have enabled powerful corporate entities to build and manage far-flung global empires. As a practical matter, such entities wield increasing power over the conditions of human freedom. Giant transnational corporations that construct global networked supply chains enjoy nearly unlimited authority over their workers and outsize influence over the surrounding communities. The state-centered human rights discourses and institutions that emerged in the post-World War II era did not contemplate such rearrangements, and both powerful economic actors and the developed economies of the Global North have resisted reform efforts that might bring transnational norms and domestic constitutional obligations to bear directly on private economic activity.[22] In the U.S., at least, the direction of constitutional reform has run the other way.[23]

Capabilities for networked digital communication and for highly informationalized, managerial oversight also have catalyzed profound changes in the structure and operation of regulatory and governance institutions, and those changes have unfolded in ways that have accelerated the marginalization of human rights commitments. The increasing power and prominence of network-and-standard-based legal-institutional arrangements for economic governance—arrangements that exist to facilitate global flows of extractive activity and that tend to treat protective regulation as network damage—has left older human rights institutions increasingly sidelined.[24] Meanwhile, as emergent human rights discourses and practices organized around capabilities for human flourishing and sustainable development have encountered and engaged

---

[21] *See generally* JAMES R. BENIGER, THE CONTROL REVOLUTION: TECHNOLOGICAL AND ECONOMIC ORIGINS OF THE INFORMATION SOCIETY (1986).

[22] *See generally* STEFANIE KHOURY & DAVID WHYTE, CORPORATE HUMAN RIGHTS VIOLATIONS: GLOBAL PROSPECTS FOR LEGAL ACTION (2017).

[23] *See generally* ADAM WINKLER, WE THE CORPORATIONS: HOW AMERICAN BUSINESSES WON THEIR CIVIL RIGHTS (2018).

[24] On network-and-standard-based governance arrangements, see Julie E. Cohen, *Networks, Standards, and Network-and-Standard-Based Governance*, in AFTER THE DIGITAL TORNADO (Kevin Werbach, ed., forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3339351.

with economic governance arrangements, they have become increasingly expert-driven and inaccessible to the populations whose futures they affect. In particular, activists and advocates have raised persistent concerns about the methodological tyranny of utilitarianism in the articulation of development goals and benchmarks.[25] Efforts to reorient human rights discourse and practice toward the problem of private economic power also have undergone a novel form of institutional cooptation that relocates those efforts inside corporations themselves and restyles them as "corporate social responsibility" (CSR) practice. Initiatives such as the UN Global Compact rely on hortatory strategies to extract commitments that may or may not be honored and project an image of consensus around gradual forward progress that may or may not correspond to reality.[26]

The powerful global platform businesses that have emerged in the twenty-first century did not cause any of these changes, but they have proved apt at exploiting them. So, for example, as the European Union has worked to export its high standards for personal data protection to the rest of the world, U.S. platform businesses have supported efforts to insert strengthened mandates for cross-border flow into bilateral and multilateral trade agreements, including especially agreements involving the Asian nations that are increasingly significant players in the emerging cross-border data servicing economy.[27] Platform businesses also have taken an entrepreneurial approach to the CSR movement. The Global Network Initiative, founded in 2008 by a coalition of platform firms, academics, and human rights NGOs, represented an attempt both to

---

[25] *See* Sally Engle Merry & John M. Conley, *Measuring the World: Indicators, Human Rights, and Global Governance*, 52 CURRENT ANTHROPOLOGY S83 (2011); AnnJanette Rosga & Margaret L. Satterthwaite, *The Trust in Indicators: Measuring Human Rights*, 27 BERKELEY J. INT'L L. 253 (2009). S*ee generally* KEVIN E. DAVIS, ANGELINA FISHER, BENEDICT KINGSBURY & SALLY ENGLE MERRY, EDS., GOVERNANCE BY INDICATORS: GLOBAL POWER THROUGH QUANTIFICATION AND RANKINGS (2012).

[26] *See* Special Representative of the Secretary-General, *Report 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 accessed June 26, 2018); KHOURY & WHYTE, *supra* note 22, at 48–61.

[27] *See* Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, 2 EUR. DATA PROTECTION L. REV. 191 (2016); Graham Greenleaf, *Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains*, *in* TRANSATLANTIC DATA PRIVACY RELATIONS AS A CHALLENGE FOR DEMOCRACY 181–212 (Dan Svantesson & Dariusz Kloza eds., 2017).

coordinate resistance to censorship demands by authoritarian states and to respond to criticisms levied at platforms for acceding to such demands.[28] Compliance with the GNI's principles, however, remains voluntary and inconsistent, even as the vast and growing extent of commercial surveillance—encompassing information of an astonishing variety, granularity, and intimacy—deepens the symbiosis between public and private surveillance power.[29]

Last but not least, data-driven, algorithmic processes multiply both obstacles to accountability and opportunities for cooptation of accountability structures. Smart digital technologies produce 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 those choices are continually evolving. The design of automated machine-learning processes also includes a number of steps that scrutiny of their end results does not capture.[30] Those attributes sit in profound tension with traditional articulations of the institutional features that a commitment to the rule of law requires, and they create oversight problems that extend far outside the traditional competencies of courts.[31] And here again, efforts to devise new oversight mechanisms have offered new avenues for the assertion and reproduction of informational power: Consider, for example, the Federal Trade Commission's privacy and data security consent decrees, which rely heavily on attestations of compliance by private sector auditors that are

---

[28] *GNI Principles on Freedom of Expression and Privacy*, GLOBAL NETWORK INITIATIVE (May 2017), https://perma.cc/J32J-GMXB; *see* MACKINNON, *supra* note 6, at 138–39, 179–82.

[29] *See, e.g.*, Daithi Mac Sithigh & Mathias Siems, *The Chinese Social Credit System: A Model for Other Countries?* (EUI Dept. of Law Working Paper 2019/01), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3310085; David Cole, *"We Kill People Based on Metadata,"* N.Y. REV. BOOKS (May 10, 2014), https://perma.cc/ERY2-Z44L; Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Lineup: Unregulated Police Face Recognition in America*, CTR. ON PRIVACY AND TECH., GEORGETOWN LAW (Oct. 18, 2016), https://perma.cc/8FUT-RR3R; Caroline Haskins, *Dozens of Cities Have Secretly Experimented with Predictive Policing Software*, VICE MOTHERBOARD (Feb. 6, 2019), https://perma.cc/ZY4B-HDCH; 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.

[30] *See* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn about Machine Learning*, 51 U.C. DAVIS L. REV. 653 (2017).

[31] *See generally* MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW: NOVEL ENTANGLEMENTS OF LAW AND TECHNOLOGY 133–56, 174–85 (2015); Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQ. L. 1, (2019).

largely unverifiable and that bootstrap self-defined standards of adequacy.[32] Or consider emergent regimes for "content moderation at scale," which rely on a combination of privatized algorithmic governance and standardized performance reporting as a means of demonstrating compliance to the outside world.[33] Both developments reflect beliefs about the best uses of new informational capabilities to manage legal and regulatory processes; neither expresses a commitment to robust public accountability.

CONCLUSION

None of the problems I have described, of course, is Barlow's fault. But those who would advance the intertwined projects of human freedom and democratic self-government should choose their prophets carefully—or, perhaps, should not place their faith in prophets at all. Advancing human freedom through the absence of law was never really in the cards. The difficulty, rather, is that the information-era problems now requiring institutional solutions are profoundly unfamiliar to institutional actors whose established modes of both action and self-legitimation are backward-looking. New informational capabilities demand both new governance modalities and new institutional arrangements capable of deploying them effectively. Due in part to hard-to-break habits of framing such questions as anti-openness, anti-innovation, or conducive to censorship (or, more usually, all three), we still have vanishingly little idea what such capabilities and structures might look like and how they might be conformed in some recognizable way to rule-of-law ideals. Those are urgent projects for a post-utopian era.

---

[32] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Megan Gray, *Understanding and Improving Privacy Audits under FTC Orders* (May 5, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3165143.

[33] *See generally* TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET: PLATFORMS, CONTENT MODERATION, AND THE HIDDEN DECISIONS THAT SHAPE SOCIAL MEDIA (2018).