Saving Governance-By-Design

Deirdre K. Mulligan* & Kenneth A. Bamberger**

Governing through technology has proven irresistibly seductive. Everything from the Internet backbone to consumer devices employs technological design to regulate behavior purposefully by promoting values such as privacy, security, intellectual property protection, innovation, and freedom of expression. Legal and policy scholarship has discussed individual skirmishes over the political impact of technical choices—from whether intelligence and police agencies can gain access to privately encrypted data to debates over digital rights management. But it has failed to come to terms with the reality that "governance-by-design"—the purposeful effort to use technology to embed values—is becoming a central mode of policymaking, and that our existing regulatory system is fundamentally ill-equipped to prevent that phenomenon from subverting public governance.

DOI: https://doi.org/10.15779/Z38QN5ZB5H

* Associate Professor, School of Information, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology.

** The Rosalinde and Arthur Gilbert Foundation Professor of Law, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology. We owe a deep debt of gratitude to Kerry Tremain, and to Amit Elazari, for their heroic editing and research contributions to this Article, and to the Berkeley Center for Law and Technology for its generous support. Our appreciation goes as well to Michael J. Berger for research assistance; to Elaine Sedenberg, Leslie Harris, Nicholas Doty, Richmond Wong, and Joseph Lorenzo Hall for collaborations on other work that contributed significantly to background knowledge essential to this project; and to Michael Birnhack, Tal Zarsky, and commentators at the April 2017 conference on Privacy by Design held at the University of Haifa, and co-organized with Tel Aviv University.

Far from being a panacea, governance-by-design has undermined important governance norms and chipped away at our voting, speech, privacy, and equality rights. In administrative agencies, courts, Congress, and international policy bodies, public discussions about embedding values in design arise in a one-off, haphazard way, if at all. Constrained by their structural limitations, these traditional venues rarely explore the full range of other values that design might affect, and often advance, a single value or occasionally pit one value against another. They seldom permit a meta-discussion about when and whether it is appropriate to enlist technology in the service of values at all. And their policy discussions almost never include designers, engineers, and those that study the impact of socio-technical systems on values.

When technology is designed to regulate without such discussions—as it often is—the effects can be even more insidious. The resulting technology often hides government and corporate aims and the fundamental political decisions that have been made. In this way, governance-by-design obscures policy choices altogether. Such choices recede from the political as they become what "is" rather than what politics has determined ought to be.

This Article proposes a detailed framework for saving governance-by-design.

Through four case studies, the Article examines a range of recent battles over the values embedded in technology design and makes the case that we are entering an era of policymaking by "design war." These four battles, in turn, highlight four recurring dysfunctions of governance-by-design:

First, governance-by-design overreaches by using overbroad technological fixes that lack the flexibility to balance equities and adapt to changing circumstances. Errors and unintended consequences result.

Second, governance-by-design often privileges one or a few values while excluding other important ones, particularly broad human rights.

Third, regulators lack the proper tools for governance-by-design. Administrative agencies, legislatures, and courts often lack technical expertise and have traditional structures and accountability mechanisms that poorly fit the job of regulating technology.

Fourth, governance-by-design decisions that broadly affect the public are often made in private venues or in processes that make technological choices appear inevitable and apolitical.

If we fail to develop new rules of engagement for governance-by-design, substantial and consequential policy choices will be made without effective public participation, purposeful debate, and relevant expertise. Important values will be sacrificed—sometimes inadvertently, because of bad decisions, and sometimes willfully, because decisions will be captured by powerful stakeholders.

To address these critical issues, this Article proposes four rules of engagement. It constructs a framework to help decision makers protect values and democratic processes as they consider regulating by technology. Informed by the examination of skirmishes across the battlefields, as well as relevant Science and Technology Studies (STS), legal, design, and engineering literatures, this framework embraces four overarching imperatives:

1. *Design with Modesty and Restraint to Preserve Flexibility*
2. *Privilege Human and Public Rights*
3. *Ensure Regulators Possess the Right Tools: Broad Authority and Competence, and Technical Expertise*
4. *Maintain the Publicness of Policymaking*

These rules of engagement offer a way toward surfacing and resolving value disputes in technological design, while preserving rather than subverting public governance and public values.

INTRODUCTION

Nearly twenty years after Larry Lessig labeled technology as a mode of regulation,[1] technologists, system designers, advocates, and regulators increasingly seek to use the design of technological systems for the advancement of public policy—to govern "by design." Designing technology to "bake in" values offers a seductively elegant and effective means of control. Technology can harden fundamental norms into background architecture, and its global reach can circumvent jurisdictional constraints, sometimes out of public view. And as technology's power to shape and control human behavior, often imperceptibly, extends into the farthest corners of our public and private lives, information and communication technology has increasingly become the new locus for settling policy debates.

Indeed, as regulators, security officials, private companies, industry groups, technologists, standard setters, and legislators have come to realize the power of technology design to regulate behavior, battles over its use have spread across a broader swath of human activity. Unsurprisingly, across and among stakeholders, agencies, and legislators, there are divergent views of which values—privacy, security, innovation, copyright, freedom of expression, fairness, equality, consumer protection, and more—to prioritize. Various stakeholders compete over affordances, designs, and information flows that privilege the values that they consider most important. Thus, design war increasingly constitutes the *modus operandi* for determining how American and global society governs our homes, our dignity, our safety, our exercise of democracy, our travel, our property, and our expression.

Unfortunately, governance-by-design has taken us down the path towards governance dystopia. Our existing institutions and processes of democratic and administrative governance have proven to be defective design-war battlefields. They are structurally unsuited to the deliberative decisionmaking necessary for governance-by-design. No domestic venue exists for the broad conversation about which values to embed in which circumstances. Administrative process frequently fails even to recognize technology design choices as matters of public policy, rather than private choice or government procurement. Agencies generally lack both the technical expertise and the mandate to consider fully the implications of embedding values in design. Constrained by mission and statute,

1. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 20–21 (1999).

individual agencies possess neither the constitutional ability nor the structural incentives to consider competing values outside their narrow ambit. Such agency-by-agency decisionmaking creates downstream ripple effects, prioritizing certain values and precluding reasoned deliberation over others. First movers, particularly those that exercise the greatest sway over the private sector, may co-opt technology to their agencies' particular missions.

These shortcomings appear also at the legislative level, where members of Congress lack technical expertise and face a paucity of trusted, non-ideological, and credible external technical experts. The legislative committee structure fosters a subject-matter tunnel vision that obscures institutional responsibility for the full range of public interests implicated in technical design.

Internationally, conversations about values in technical design are scattered across multiple entities, none of which has the ability to drive or implement a resolution. Multinational standard setting organizations have urged restraint and are developing approaches for thinking more rigorously about human rights in design. But we lack a comprehensive approach—a doctrine, a set of metrics, as well as tools—for resolving design wars while accounting for the range of human rights and other public values.

In the private sector, arguments about technical progress and efficiency often hide the fundamental political decisions at stake. Public values, such as security, are often ignored or sacrificed in service of other values, such as innovation, proprietary design, or cost. These choices remain invisible until called to public attention by events such as the October 2016 botnet attack, which shut down large segments of the U.S. Internet by hacking into, and commandeering, an army of "Internet of Things" (IoT) devices.[2]

Likewise, private technology design can be used in ways that obscure government aims. Governments can lean on companies to embed choices that advance a specific value, such as accountability, at the cost of another, such as anonymity. Or they make procurement decisions that generate markets for technology that align with certain values at a cost to others. For example, in 2016, the Obama Administration announced that it would not seek legislation requiring companies to build crypto backdoors; instead, they intended to work with and "lean heavily on" companies directly.[3] President Trump appears to favor this approach to technology policy, telling Silicon Valley executives: "You'll call my

2. Brian Krebs, *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, KREBSONSECURITY (Oct. 21, 2016, 5:57 PM), https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage [https://perma.cc/3H7R-Z5QS].

3. Chris Williams, *FBI Boss: No Encryption Backdoor Law (But Give Us Backdoors Anyway)*, REGISTER (Oct. 9, 2015, 11:41 PM), http://www.theregister.co.uk/2015/10/09/us_encryption_backdoor_law_latest [https://perma.cc/9XMW-BTU7].

people, you'll call me—it doesn't make any difference—we have no formal chain of command around here."[4]

As these approaches succeed, we face the threat of a governance-by-design dystopia. Future generations may experience the lack of privacy from government as a feature of digital technology, rather than as a political choice against strong encryption due to the difficulties it presents for law enforcement. Such actions undermine the fundamental values that undergird democratic governance: deliberation, participation, transparency, the capacity for flexibility in the face of changing circumstances and new information, and, frequently, democratic legitimacy itself.

Public policy debates and scholarship have both largely failed to address, or even fully recognize, the challenge to public values and purposive democratic government posed by a wholesale design-war era. Eager legislators and regulators are largely blind to the challenges and perils of embedding values in technology design. Consistent with a perception of design battles as limited and isolated, a small body of scholarship has focused on particular skirmishes over the use of code to harden a discrete set of values.[5] But neither the legal literature nor policy analysis has moved beyond the individual case to identify governance-by-design as an accelerating form of control that transcends context, and to explain how regulating it through traditional policymaking venues inevitably subverts procedural and substantive public norms. Their engagement with fundamental insights of the social science values-in-design research has been sporadic and limited. Existing scholarship has not, moreover, articulated a better framework for structuring the discussions about the full range of rights and values on the design-war battlefield.

In short, existing analysis has not provided rules of engagement for design-war governance. There is no strategy for considering the tactics that are acceptable, or even desirable, in using technology to advance a policy value. Nor have analysts developed a coherent framework that permits transparency and public debate over value choices, or articulates engineering and design practices oriented toward a positive governance-by-design agenda.

This Article offers a framework for saving governance-by-design. It responds to these failings by setting forth four rules of engagement when using technology to regulate. These rules offer institutional, decisional, and technological principles for considering the full range of values at play in the design of socio-technical systems and a method for rigorously considering how to set the relative weights and modes of protection for them. Our Article seeks to articulate a conceptual approach to guide the purposeful use of governance-by-design. It provides a set of conditions under which it is acceptable and

4. Bradd Jaffy (@BraddJaffy), TWITTER (Dec. 14, 2016, 11:41 AM), https://twitter.com/BraddJaffy/status/809121072998215680 [https://perma.cc/H6Q3-2CU7].

5. *See infra* Part II.B.

desirable to do so, and a framework for considering a conjoined set of "values at play"[6] rather than values in isolation.

At the same time, we seek to outline the key changes to the administrative state required to consider values in socio-technical systems in a comprehensive and coordinated manner. This effort aligns with the practical turn in science and technology studies (STS) and the realpolitik of design. We are guided by scholarship in sociological, historical, and political studies that explore the ways values inhere in technologies as a function of their design and construction, and which demonstrate how technology is not "neutral," but instead is thickly integrated with ethics and politics. By heeding their insights, our framework outlines a plan to equip the administrative state to wield design as a tool of governance, while at the same time future-proofing democratic norms of policymaking and substantive values as regulated activities recede into technical designs.

Our analysis proceeds as follows. Section II charts the move to a "design-war" era, the threat of a governance-by-design dystopia, and the failure of legal and policy analysis to address the repercussions.

Section III then explores four high-profile battles over values in design. In the Apple v. FBI case, a law enforcement agency sought to preempt competing values, especially privacy, in favor of law enforcement, subverting public processes by pursuing its goals in cloaked venues. The Privacy-by-Design movement has sought to protect an important value through technical designs that unintentionally preclude protection of competing ones. In the battle over the Stop Online Piracy Act (SOPA) of 2012, Congress's dearth of trusted, nonpartisan, technical experts and its structural and procedural limitations threatened to unravel key protections built into the Internet. And in the Electronic Voting debacle, important public decisions were delegated to the private voting machine companies in ways harmful to the integrity of elections.

These design-war episodes demonstrate how reliance only on existing institutions and processes for regulation through technology subverts fundamental principles at the heart of public governance. Specifically, they highlight four key governance-by-design dysfunctions:

1. Governance-by-design overreaches by using overbroad technological fixes that lack the flexibility to balance equities and adapt to changing circumstances.
2. Governance-by-design often privileges one or a few values and excludes other important ones, particularly broad human rights.
3. Governance-by-design regulators lack the proper tools, including the necessary technical expertise, administrative

6. *See generally* MARY FLANAGAN & HELEN NISSENBAUM, VALUES AT PLAY IN DIGITAL GAMES (2014) (developing a framework for identifying socially recognized moral and political values in technology in the context of digital games).

structures, and accountability mechanisms.

4. Governance-by-design decisions that broadly affect the public are often made in private venues or in processes that make technological choices appear inevitable and apolitical.

Section IV outlines a framework that moves beyond critique towards a model for successfully deploying technology as a regulatory force in defense of multiple values. It articulates four fundamental "rules of engagement" for addressing the four governance-by-design dysfunctions by advancing, grounding, and rationalizing the process of constructing and protecting values through technology. Jurisprudence reflects frameworks and strategies to guide law making that prioritize some rights over others, demand specific processes and recourse, and defer values to different branches of government depending upon countervailing priorities such as certainty and flexibility, and stability and dynamism. Similarly, we offer a framework and strategies for wielding the powerful tool of design. The framework reflects theoretical and empirical understandings of the pros and cons of assigning regulatory capacity to technology, and targets values protection at the right stage of technical design. Specifically, we propose and develop four fundamental rules of engagement:

1. Design with Modesty and Restraint to Preserve Flexibility
2. Privilege Human and Public Rights
3. Ensure Regulators Possess the Right Tools: Broad Authority and Competence, and Technical Expertise
4. Maintain the Publicness of Policymaking

These rules of engagement focus on the process of building out institutional capacity for rigorous and inclusive governance around the role of technology as a regulator. They provide a set of approaches to improve governance-by-design in a manner consistent with democratic commitments to intentional, deliberative, participatory, expert public decisionmaking, free from capture and caprice. By suggesting how to "do governance better"[7] in a design-war age, our recommendations begin to connect and fill holes in the values in design and scientific governance scholarship, and offer an approach to protecting important values—human rights, fairness, privacy, and many others—in the face of the rapid developments that threaten to overwhelm the public governance process.

I.
THE GOVERNANCE-BY-DESIGN ERA

Efforts to embed regulatory values purposefully into technology—and battles over those attempts—have accelerated rapidly since the mid-1990s, when Congress passed the Communications Assistance for Law Enforcement Act

7. Alan Irwin, *STS Perspectives on Scientific Governance*, *in* THE HANDBOOK OF SCIENCE AND TECHNOLOGY STUDIES 583, 600 (Edward J. Hackett et al. eds., 3d ed. 2008) ("Certainly, there is nothing in STS scholarship that represents a tool kit for 'how to do governance better' . . . .").

(CALEA).[8] This Act mandated surveillance "by design" by requiring telecommunications networks to enable law enforcement to access information to which they are legally entitled. Yet at the same time, Congress also rejected proposals to establish "Clipper Chip" and government key escrow systems, which would have given the government backdoors into cryptographic storage systems.[9]

Public governance has since increasingly turned to norm-enforcing, or "normative" technologies.[10] These are distinguished from other forms of technology by their intentional design to constrain and direct behavior consistent with regulations decided upon elsewhere.[11] Agencies use these technologies to carry out their mandates in diverse public sectors such as health, security, law enforcement, financial regulation, privacy, education, and justice.[12] In many cases, automated systems have become the primary decisionmaking agent.[13] They displace human decisionmaking in the allocation of public benefits on the one hand, and the direction of punishments, such as law enforcement and antiterrorism efforts, on the other.[14] Policy makers, from legislators on down, have sent public (if inconsistent) messages that those building systems and handling data cannot simply be "neutral" in their design and treatment, but must think about the human rights implications of their technical decisions.[15] Privacy regulators internationally have been clear about their desire that companies and governments collecting data embed privacy by design, through design, and in design.[16]

---

8. Communication Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012)).

9. *See* JENNIFER STISA GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHY YOU SHOULD CARE, AND WHAT TO DO ABOUT IT 264–65 (2017).

10. Bert-Jaap Koops, *Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values*, *in* REGULATING TECHNOLOGIES: LEGAL FUTURES, REGULATORY FRAMES AND TECHNOLOGICAL FIXES 157, 157–58, (Roger Brownsword & Karen Yeung eds., 2008) (coining the term).

11. *See* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 724 (2010) [hereinafter Bamberger, *Technologies of Compliance*] (discussing "technologies of compliance" that are "purportedly norm *enforcing* rather than norm *setting*").

12. *See id.* at 714–22; Peter A. Winn, *Judicial Information Management in an Electronic Age: Old Standards, New Challenges*, 3 FED. CTS. L. REV. 135 (2009).

13. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1252 (2008).

14. *See* Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. TELECOMM. & HIGH TECH. L. 235, 235–36 (2011).

15. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 3–5 (2015) (discussing the Yahoo! moral pygmies story).

16. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (relaying the Council of 27 April 2016's views on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC).

Government bodies have also enlisted technology design in administering public operations such as electronic voting and e-petitions.[17] Smartgrid, and Smartcity initiatives are building sensors and networks into our homes and urban infrastructure to reduce energy consumption and to streamline the delivery of services.[18] This phenomenon has further extended to private sector implementation of legal mandates through technical standards—a reflection of a broader governance trend towards "mixed administration" in which private and public actors share responsibility for both regulation and service provision.[19]

Scholarship has highlighted this recent trend towards regulatory delegation of public sector decisionmaking to private sector actors in specific areas of risk, including financial data, homeland security, and conflict of interest.[20] Broad policy goals in legislation and accompanying regulations are enacted, and regulated parties are then delegated the task of interpreting and implementing the policies in the context of their own operations.[21] This trend has culminated in the past several years with the delegation of automated risk assessment and compliance systems—machines and algorithms—to such private sector actors.[22]

As a result, decisions about the *design* of technology—from those made by legislatures at the high level to those made by computer programmers more granularly—have become important sites for resolving value disputes.[23] Technology is viewed as a way to durably and literally resolve such disputes, often at the expense of other important norms.[24]

The increasingly political impact of technical choices has intensified the importance of these battles and their resolution. Sometimes, skirmishes occur

17. *See, e.g.*, *We the People: Your Voice in the White House*, WHITE HOUSE, https://petitions.whitehouse.gov [https://perma.cc/8ABV-C2BA].

18. *See, e.g.*, Robert Brauneis & Ellen P. Goodman, Note, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 114–15 (2018) (describing smart city initiatives); Nikolaos G. Paterakis et al., *An Overview of Demand Response: Key-Elements and International Experience*, 69 RENEWABLE & SUSTAINABLE ENERGY REVS. 871, 878–80 (2018) (discussing deployment of demand response energy systems in U.S. cities).

19. Jody Freeman, *Private Parties, Public Functions and the New Administrative Law*, 52 ADMIN. L. REV. 813, 816 (2000).

20. *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 380 (2006).

21. *Id.* at 380–81.

22. Bamberger, *Technologies of Compliance*, *supra* note 11, at 672–74.

23. Examples of such debates in Congress and the courts are discussed below in Section III. They also occur in standard-setting bodies. *See* Cory Doctorow, *An Open Letter to the W3C Director, CEO, Team and Membership*, ELECTRONIC FRONTIER FOUND. (Sept. 18, 2017), https://www.eff.org/deeplinks/2017/09/open-letter-w3c-director-ceo-team-and-membership [https://perma.cc/U9RB-KB3R]. In the market, see Nilay Patel, *The Engadget Interview: Paul Aiken, Executive Director of the Authors Guild*, ENGADGET (Feb. 27, 2009) https://www.engadget.com/2009/02/27/the-engadget-interview-paul-aiken-executive-director-of-the-au [https://perma.cc/ZE8F-F3TT].

24. Kalev Leetaru, *Why the Apple Versus FBI Debate Matters in a Globalized World*, FORBES (Mar. 2, 2016, 3:47 PM) https://www.forbes.com/sites/kalevleetaru/2016/03/02/why-the-apple-versus-fbi-debate-matters-in-a-globalized-world/#349fb622212a [https://perma.cc/NZ5V-K47J].

very publicly, as in the cases of the "crypto wars"—the struggles over government attempts to limit public access to cryptography strong enough to resist national intelligence agency decryption (framed as a battle between privacy and national security)[25]—and the debates over digital rights management, its effect on fair use, and the balance between creators and users under legal copyright regimes.[26] But they also occur more quietly, sometimes in private, excluding key stakeholders in the battle and hiding inherently political decisions from public view.[27] In Section III below, we explore in detail four of these battles, including core regulatory efforts involving voting, privacy, nondiscrimination, and intellectual property.

Policy makers and legal scholars have been lamentably slow to address the wholesale challenges for public governance posed by the increased use of value-embedded design, to recognize the ways in which our institutions of public administration are ill-designed to such forms of governance, and to adapt public decisionmaking accordingly. Some scholars have drawn on the STS and engineering literatures,[28] which have grappled extensively with the opportunities and pitfalls inherent in attempts to embed values in design. Employing STS insights, these scholars have identified value-embedded design and described some of the challenges of effective regulation. But legal and policy scholarship has not developed a general framework to address the normative questions of when to use design or how to prioritize values in the design context. Nor has it articulated procedural norms to guide the choice of venues for debates and decisions over values in technical design to maintain democratic governance norms.

The following section explores insights from STS about the dangers that inhere in efforts to promote values through design and describes early starts in the legal and policy discussion addressing governance-by-design.

A. Values in Technology Design: Lessons From Science and Technology Studies

1. The Social Construction of Values in Design

A deep body of social science and technology research from outside the law has demonstrated the ways in which values become embedded in technology, such that the use of that technology becomes an expression of that

25. *See infra* Part III(A).

26. *See infra* pp. 130–34.

27. *See infra* Part III(E)(4); *see also* Marci Meingast, Jennifer King & Deirdre K. Mulligan, *Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport*, IEEE INTERNATIONAL CONFERENCE ON RFID, at 10–11 (2007) (describing how public understanding of privacy issues was limited because of government referencing of international standard in context of rulemaking in lieu of providing technical details within the process).

28. *See infra* Part II.A.

value.[29] Technical decisions can have social effects, both intended and unintended,[30] as evidenced by the canonical example of Robert Moses, the New York City planner who designed low bridges and overpasses on the expressway leading to Long Island. As a result, the buses and the poor people they carried were unable to travel to well-off neighborhoods or patronize their beaches.[31] Whether Moses acted intentionally is a matter of historical debate.[32] Either way, the social implications of the resulting technical "artifacts" have been profound and durable.[33]

Technology, then, should not (or cannot *only*) be understood as an independent determinant of human action. Rather, it is the product of social context and cultural values that is shaped by human action or "socially constructed."[34] The constant uptake of values by artifacts transforms the structure of future debates on those values by embedding them in technology, depoliticizing the values, and ending debate about them—at least for a while.[35] Moreover, decisions about technological information systems can be framed as

29. *See, e.g.*, Mary Flanagan, Daniel C. Howe & Helen Nissenbaum, *Embodying Values in Technology: Theory and Practice*, *in* INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY 322, 322–47 (Jeroen van den Hoven & John Weckert eds., 2008) (arguing that technology can embody values by design and developing a framework for identifying moral and political values in such technology); Bruno Latour, *Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts*, *in* SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE 225, 232 (Wiebe E. Bijker & John Law eds., 1992) ("We have been able to delegate to nonhumans . . . values, duties, and ethics."); Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 121, 123 (1980) (proposing that technical systems can reflect the "politics" of a particular community).

30. *See* Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 Info. Soc'y 169, 169–85 (2000) (discussing biases in the creation of search indexes and search results); Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM Transactions on Info. Systems 330, 330–47 (1996) (discussing preexisting, technical, and emergent bias in the context of online flight reservation systems); James H. Moor, *What is Computer Ethics?*, 16 Metaphilosophy 266, 266–75 (1985) (discussing the ethical implications of invisible abuse, emergent bias due to designers values, and bias rooted in complexity within computer systems).; Winner, *supra* note 29, at 128–34.

31. *See* Winner, *supra* note 29, at 123–24.

32. *See* Bernward Joerges, *Do Politics Have Artefacts?*, 29 SOC. STUD. SCI. 411, 416 (1999).

33. ROBERT A. CARO, THE POWER BROKER: ROBERT MOSES AND THE FALL OF NEW YORK 920–58 (1974).

34. *See* Bruno Latour, *The Moral Dilemmas of a Safety-belt (La Ceinture de Sécurité)*, 1 ALLIAGE 21, 25–26 (1989) (showing, through the analogy of a seatbelt, how technology is a reflection—indeed extension—of human values and morality); Tamara Alsheikh, Jennifer A. Rode & Siân E. Lindley, *(Whose) Value-Sensitive Design? A Study of Long-Distance Relationships in an Arabic Cultural Context*, PROCEEDINGS OF THE ACM 2011 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 75, 81 (2011) (observing how the cultural values of the participants in the study were expressed through their use of communication technology). This "social constructivist" view in turn took its inspiration from earlier scholarship in the sociology of scientific knowledge. *See* Trevor J. Pinch & Wiebe E. Bijker, *The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*, 14 SOC. STUD. SCI. 399, 400 (1984).

35. *See* Philip E. Agre, *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 29, 32–33 (Philip E. Agre & Marc Rotenberg eds., 1997).

trivial issues of implementation and discussed in bureaucratic and technocratic jargon that veils their political importance.[36] And even when the political implications of decisions are understood, members of the public and their institutions often lack the technical expertise to participate meaningfully in their resolution.[37] When government creates standards and classification schemes, and embodies and enforces them through artifacts and technology, the effect is to promote one set of values or point of view and silence others.[38]

The history of technological implementation reveals the difficulty of intentionally translating values into design requirements. Technology and law are shaped by distinctly different systems of logic. While policy tempers rule-based mandates with context-specific judgment that allows for interpretive flexibility and ongoing dispute about the appropriateness of rules, computer code operates by means of on-off rules. Thus, there is always a difference between "law in books" and "law in technology."[39] It is a fallacy to assume in technology design that "one will know what to do *in a normative sense*" once values are identified.[40]

Further distortions occur because of the social and technical environment in which regulatory norms are "translated" into code, the "systemic effects" that result when such distortions are introduced into human systems, and competing norms of technology designers such as elegance and efficiency.[41] As a result—and depending on who is involved in the process of translation—purely technical solutions for enabling, enforcing, or restricting rights and values can have unintended consequences that lead to inflexibility and privilege certain stakeholders and values at the expense of others.[42]

---

36. *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 77 (2008); Meingast, King & Mulligan, *supra* note 27 (discussing the extent to which different agencies were cognizant of the policy implications of switching to identification cards embedded with radio frequency chips).

37. Bamberger & Mulligan, *Privacy Decisionmaking*, *supra* note 36; *see also* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 165 (2015) (suggesting that regulatory agencies might lack the capabilities to "look under the hood" of highly advanced technologies).

38. GEOFFREY C. BOWKER & SUSAN LEIGH STAR, SORTING THINGS OUT: CLASSIFICATION AND ITS CONSEQUENCES 5 (1999); *see also* Geoffrey C. Bowker & Susan Leigh Star, *Invisible Mediators of Action: Classification and the Ubiquity of Standards*, 7 MIND, CULTURE, & ACTIVITY 147, 147 (2000) (arguing that standards and classification schemes are "key sites of work, power, and technology").

39. *See* MIREILLE HILDEBRANDT & BERT-JAAP KOOPS, FUTURE OF IDENTITY IN THE INFO. SOC'Y, A VISION OF AMBIENT LAW 22 (2007), http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf [https://perma.cc/T47H-Y3CV].

40. Noëmi Manders-Huits, *What Values in Design? The Challenge of Incorporating Moral Values into Design*, 17 SCI. ENG. ETHICS 271, 279 (2011) (describing what she calls "The Naturalistic Fallacy").

41. *See* Bamberger, *Technologies of Compliance*, *supra* note 11, at 707–11.

42. *See* Alvin M. Weinberg, *Can Technology Replace Social Engineering?, in* TECH. & FUTURE 28, 34 (Albert H. Teich ed., 11th ed. 2009).

The implications of unknowingly embedding values in systems are exacerbated further by the cognitive biases that can occur when technological systems assist human decisionmaking.[43] Humans tend to disregard or not search for contradictory information when presented with a technologically created solution.[44] The output of the technology often is accepted as unquestioningly correct. The habit of human reliance and trust on machine outputs is exacerbated by systems that provide users little indication of a variety of important issues, including: the contours or limits of the models on which the machine's decisionmaking rests; when the technology fails to flag problems;[45] or when it fails to distinguish between the different problems it flags.[46] When humans do question machines, their "correcti[ons]" tend to be biased in a single direction, favoring preexisting assumptions.[47] Other biases may lie in the algorithms upon which the technology relies,[48] the social ills and biases reflected in the data upon which such algorithms are trained,[49] or in deeper socio-political views.[50] Coupled with socio-organizational phenomena such as institutional isomorphism (the adoption of structures and practices from peer organizations to signal legitimacy),[51] these biases can become engrained and embedded in an entire sector of firms and organizations.[52] Organizations tend to "normalize deviance" through the rationalization of apparently "harmless" deviations from rules.[53] When such biases become embedded in a techno-social system, they risk becoming opaque, taken for granted, and imbued with *prima facie* legitimacy in a way that is likely to reframe future debates.[54]

For each of these reasons, the engineering and STS literatures have identified a number of challenges in designing for values, including "negative

43. *See* Bamberger, *Technologies of Compliance*, *supra* note 11, at 697–701, 710–12.

44. *See id.* at 711–12 (discussing "automation bias").

45. *See id.* at 712; *see also* Citron, *supra* note 13, at 1253-54, 1283 (noting a common belief that automatic computer systems are "error-resistant" despite their opacity).

46. The standard 404 error for web pages has been replaced by an array of error messages that communicate the source of failure, the authors' favorite being the 451 error, which signals removal by legal action and thus alerts searchers of the overtly political nature of the technical failure. *See* T. Bray, *An HTTP Status Code to Report Legal Obstacles*, INTERNET ENGINEERING TASK FORCE (Feb. 2016), https://tools.ietf.org/html/rfc7725 [https://perma.cc/YG3B-NA47].

47. *See* Citron, *supra* note 13, at 1286–87.

48. *See* Batya Friedman & Helen Nissenbaum, *Software Agents and User Autonomy*, PROCEEDINGS OF THE FIRST INTERNATIONAL CONFERENCE ON AUTONOMOUS AGENTS 466, 466–67 (1997).

49. *See* Kate Crawford, *The Hidden Biases in Big Data*, HARV. BUS. REV. (Apr. 1, 2013), https://hbr.org/2013/04/the-hidden-biases-in-big-data [https://perma.cc/MH6U-28M2].

50. *See, e.g.*, Guy Stuart, *Databases, Felons, and Voting: Errors and Bias in the Florida Felons Exclusion List in the 2000 Presidential Elections* (Kennedy Sch. of Gov't Faculty Research Working Paper Series FWP02-041, 2002).

51. Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields,* 48 AM. SOC. REV. 147, 150 (1983).

52. Bamberger, *Technologies of Compliance*, *supra* note 11, at 712–13.

53. Sheila Jasanoff, *Transparency in Public Science: Purposes, Reasons, Limits*, 69 LAW & CONTEMP. PROBS. 21, 32 (2006).

54. Bamberger, *Technologies of Compliance*, *supra* note 11, at 713.

(unintended) consequences on the realization of other social values"; uncertainty in "the effective realization of values," especially "when applied in combined and complex systems"; inadequate consideration of "exceptions"; and the shifting of "costs or other burdens to parties not involved in decisionmaking."[55]

In *Code and Other Laws of Cyberspace*, Larry Lessig brought this earlier STS scholarship to legal scholarship.[56] Building on a small body of other legal writing[57] and reflecting literature in philosophy[58] and STS,[59] his famous admonition that "code is law" was a reminder that the software and hardware architecture of the Internet could determine its structure and use.[60] He warned that market and government forces were causing a regulatory shift to an "environment of perfect control" through code.[61] He was particularly concerned that governance through technology would enable the government to hide its tracks and motives behind the veil of technological progress and corporate action. But he was not completely pessimistic about the future of cyberspace. Rather, he argued that the Internet could be designed or coded in ways that would protect fundamental values.[62]

Even before internet law scholars began exploring the interaction between values and technical systems, civil society advocates saw possibilities to protect and advance values through the "plasticity" that information technology offered. In particular, advocates for civil liberties worked with technical standard setting bodies and companies to build standards and products that would support freedom of expression.[63] These advocates helped develop a technical standard to

55. Carsten Orwat & Roland Bless, *Values and Networks—Steps Toward Exploring Their Relationships*, 46 COMPUTER COMM. REV. 25, 28 (2016).

56. Lessig, *supra* note 1; *see also* LAWRENCE LESSIG, CODE: VERSION 2.0 (2006) [hereinafter LESSIG, CODE: VERSION 2.0].

57. *See* LESSIG, CODE: VERSION 2.0, *supra* note 56, at 347–48 (citing Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN (1995).

58. Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 INFO. SOC'Y 169 (2000).

59. James H. Moor, *What is Computer Ethics?*, 16 METAPHILOSOPHY 266 (1985).

60. LESSIG, CODE: VERSION 2.0, *supra* note 56, at 5.

61. *Id.* at 4.

62. *Id.* at 6–8. His work has generally been very well accepted, although more recently, he has faced some criticism. Viktor Mayer-Schönberger argues that Lessig's theory relies too heavily on notions of technological determinism that have been long deprecated in the STS literature, as well as on flawed economic assumptions. Viktor Mayer-Schönberger, *Demystifying Lessig*, 2008 WIS. L. REV. 713 (2008). Other critics have taken Lessig to task for what they see as a flawed application of his theories to the practical realm of online privacy. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001); Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743 (2000).

63. *See PICS Statement of Principles*, WORLD WIDE WEB CONSORTIUM (W3C), https://www.w3.org/PICS/principles.html [https://perma.cc/Z8VM-ZGCX] (describing membership as a "broad cross-section of companies from the computer, communications, and content industries, as well as trade associations and public interest groups"); Paul Resnick & James Miller, *PICS: Internet Access*

support voluntary labeling and filtering of online content and promoted products to help individuals control the information they and their children accessed online, as alternatives to government censorship.[64] Other advocates saw risks in pursuing this strategy, foreseeing today's challenges with the oversized role corporate policies and technologies play in moderating public discourse.[65] Both groups, however, were keenly aware of the regulatory power of code and understood that the technical standards of the Internet and World Wide Web would shape the future of First Amendment protections. The availability of filtering and blocking technologies ultimately provided the basis for a landmark Supreme Court decision extending the highest form of First Amendment protection to the Internet.[66]

Similar insights spurred a range of both scholarship and activism, demonstrating the ways that Internet protocols and standards are politically and socially constructed, and, in turn, have social implications.[67] Some have argued that if code really "is law," then technical standards-setting bodies could act, at least in some ways, analogous to legislative bodies.[68] Realizing this early on, some civil society organizations actively sought to use the technical standards to advance values such as privacy,[69] and developed a specification that supported policy impact assessments of technical specifications generally.[70] Standards bodies such as the Internet Engineering Task Force have continued and expanded upon those early advocate-led efforts to incorporate public policy considerations into their decisionmaking process.[71]

Controls Without Censorship, 39 COMM. ACM 87 (1996); Paul Resnick, *Filtering Information on the Internet*, 276 SCIENTIFIC AM. 62 (1997).

64. *Id.*

65. *Fahrenheit 451.2: Is Cyberspace Burning?*, AM. CIVIL LIBERTIES UNION (Aug. 1997), https://www.aclu.org/other/fahrenheit-4512-cyberspace-burning [https://perma.cc/DC96-CP2D].

66. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997) (holding unconstitutional two provisions of the Communications Decency Act of 1996 (CDA) that criminalized providing indecent materials to minors on the internet on grounds that it violated the First Amendment).

67. *See* LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE (2009).

68. LESSIG, *supra* note 1; Nick Doty & Deirdre K. Mulligan, *Internet Multistakeholder Processes and Techno-Policy Standards: Initial Reflections on Privacy at the World Wide Web Consortium*, 11 J. TELECOMM. & HIGH TECH. L. 135, 157 (2013); A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749 (2003); Charles Vincent & Jean Camp, *Looking to the Internet for Models of Governance*, 6 ETHICS & INFO. TECH. 161 (2004).

69. Michelle E. Danley, Deirdre Mulligan, John B. Morris, Jr. & Jon Peterson, *Threat Analysis of the Geopriv Protocol*, INTERNET SOC'Y (Feb. 2004), https://tools.ietf.org/html/rfc3694 [https://perma.cc/3EDY-RMGQ].

70. John B. Morris, Jr. & Alan B. Davidson, *Public Policy Considerations for Internet Design Decisions* (Internet Eng'g Task Force, Internet-Draft, June 2003), http://tools.ietf.org/id/draft-morris-policy-considerations-00.txt [https://perma.cc/Y8JB-T4CZ].

71. See Doty & Mulligan, *supra* note 68, for a discussion of privacy activities; *see also* Alissa Cooper et al., *Privacy Considerations for Internet Protocols,* INTERNET ENGINEERING TASK FORCE (July 2013), https://tools/ietf.org/html/rfc6973 [https://perma.cc/G6QM-HHC4]; Niels ten Oever & Corinne Cath, *Research into Human Rights Protocol Considerations*, INTERNET ENGINEERING TASK

2. The Move Toward Embedding Values in Design

STS insights accelerated the academic movement to view technological artifacts as social actors. Scholars and practitioners recognized technology's capacity to affect and be affected by humans, institutions, other artifacts, or any other social actor,[72] and began to call more aggressively for the incorporation of human values into computer design. More significantly, this work took a practical turn when scholars moved away from critique and observation to develop models, processes, and strategies for analyzing values in the practice of design.[73]

Concurrent with this scholarly recognition, a trend has grown toward the conscious identification and incorporation of values into technology by designers, engineers, and managers.[74] The early "Socially Responsible Computing" movement focused on computer technology practitioners such as programmers, designers, and engineers.[75] Building on scholarship recognizing computing technology as a social phenomenon, computing professionals were urged to "work within society for responsible applications of computer technology" to bring about potential social benefits and prevent institutional pathologies.[76] Through socially responsible computing, computing professionals could take account critical social theories of computing and incorporate social activism into their work.[77] At the same time, theorists could challenge the assumptions of the technical tradition and still be responsive to the actual needs of practitioners.[78]

In practice, protecting values can be difficult.[79] Yet the movement among engineers and designers to be more conscious of the values embedded in the

---

FORCE (Feb. 2017), https://tools.ietf.org/html/draft-irtf-hrpc-research-11 [https://perma.cc/9QXT-8YYC] (discussing ongoing efforts to develop a framework for systematically attending to human rights considerations).

72. Latour, *supra* note 29.

73. Flanagan, Howe & Nissenbaum, *supra* note 29 (providing a methodological approach—discovery, translation, and verification—for values in design); Batya Friedman, David G. Hendry & Alan Borning, *A Survey of Value Sensitive Design Methods*, 11 Found. and Trends in Hum.–Computer Interaction 1, 63–125 (2017) (surveying 14 value sensitive design methods); Batya Friedman, Peter H. Kahn, Jr. & Alan Borning, *Value Sensitive Design and Information Systems*, *in* Human-Computer Interaction and Management Information Systems: Foundations 348, 349–50 (Ping Zhang & Dennis Galletta eds., 2006) (providing an iterative three part value sensitive design methodology of conceptual, empirical, and technical investigations).

74. Colin Allen, Wendell Wallach & Iva Smit, *Why Machine Ethics?*, 21 IEEE INTELLIGENT SYSTEMS 12 (2006).

75. Philip E. Agre, *Computing as a Social Practice*, *in* REINVENTING TECHNOLOGY, REDISCOVERING COMMUNITY: CRITICAL EXPLORATIONS OF COMPUTING AS A SOCIAL PRACTICE 1 (Philip E. Agre & Douglas Schuler eds., 1997).

76. *Id.*

77. *Id*

78. *Id.* at 3.

79. Flanagan, Howe & Nissenbaum, *supra* note 29; Noëmi Manders-Huits & Michael Zimmer, *Values and Pragmatic Action: The Challenges of Introducing Ethical Intelligence in Technical Design Communities*, 10 INT'L REV. INFO. ETHICS 37 (2009).

systems they design,[80] anticipate the ethical consequences of such values,[81] and elevate values to the level of design aspiration and excellence criteria,[82] is growing. Additionally, the professional community has developed techniques to address values more systematically in technical practice[83] that while not all widely used, are gaining traction. For instance, the National Science Foundation supported the Values-in-Design Council, which brought together sixteen members from law, humanities, and social sciences to work with researchers designing alternative next generation Internet architectures.[84] Both the development of new organizations to promote the protection of values in systems that rely on big data, machine learning, and artificial intelligence, and the increased focus on ethics by professional associations further attest to growing interest among practitioners.[85]

Designing for values is complicated as the implications for values occur—and can shift—at design, configuration, *and* run time.[86] Technology is appropriated by users in new and unexpected ways, altering its value implications. Technology interacts with business models, organizational structures, and other technologies in ways that can transform its effects, use, and impact on values. Additionally, there is the problem of teasing out and anticipating what Harry Surden has called the "latent structural constraints" that often work to protect values in addition to and in conjunction with legal measures.[87] These constraints may suddenly be removed through the introduction of a new technological system. As a result, the social shaping and

80. Allen, Wallach & Smit, *supra* note 74, at 13; David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM TRANSACTIONS NETWORKING 462, 466 (2005).

81. Katie Shilton, *Anticipatory Ethics for a Future Internet: Analyzing Values During the Design of an Internet Infrastructure*, 21 SCI. & ENGINEERING ETHICS 1 (2015).

82. Flanagan, Howe & Nissenbaum, *supra* note 29, at 322; Cory Knobel & Geoffrey C. Bowker, *Values in Design*, 54 COMM. ACM 26 (2011).

83. Doty & Mulligan, *supra* note 68, at 140-41; *see* Cooper et al., *supra* note 71; John Morris & Alan Davidson, *Policy Impact Assessments: Considering the Public Interest in Internet Standards Development*, TPRC 31ST RES. CONF. ON COMM., INFO. AND INTERNET POL'Y (2003); Fred Baker & Brian E. Carpenter, *IETF Policy on Wiretapping*, INTERNET ENGINEERING TASK FORCE (May 2000), https://tools.ietf.org/html/rfc2804 [https://perma.cc/8S5K-K6Z7]; Stephen Farrell & Hannes Tschofenig, *Pervasive Monitoring Is an Attack*, INTERNET ENGINEERING TASK FORCE (May 2014), https://tools.ietf.org/html/rfc7258 [https://perma.cc/8WCT-FXTZ]; Jon Postel & Joyce K. Reynolds, *Instructions to RFC Authors*, INTERNET ENGINEERING TASK FORCE (Oct. 1997), https://tools.ietf.org/html/rfc2223 [https://perma.cc/R6ZP-MP8R].

84. *Values-in-Design Council*, N.Y.U., http://www.nyu.edu/projects/nissenbaum/vid/vidcouncil.html [https://perma.cc/R9ZZ-E6M6].

85. *See* DATA & SOCIETY, https://datasociety.net [https://perma.cc/FNL2-SYFV]; PARTNERSHIP ON ARTIFICIAL INTELLIGENCE TO BENEFIT PEOPLE AND SOCIETY, https://www.partnershiponai.org [https://perma.cc/SZL4-WUP2]; AI NOW, https://ainowinstitute.org [https://perma.cc/MYX7-MLFX]; IEEE GLOBAL INITIATIVE ON ETHICS OF AUTONOMOUS & INTELLIGENT SYSTEMS, http://standards.ieee.org/news/2017/ieee_global_initiative.html [https://perma.cc/6D4F-M9D2]; and *Statement on Algorithmic Transparency and Accountability*, ASS'N FOR COMPUTING MACHINERY US PUB. POLICY COUNCIL (2017).

86. Clark, *supra* note 80, at 463.

87. Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1608 (2007).

appropriation of technology complicates engineering and design efforts to protect values during, and through, design.

The values-in-design movement has drawn attention to design choices and advocated "design of technology that accounts for human values in a principled and comprehensive manner throughout the design process."[88] It has also become a critical lens for viewing technological systems, such as identifying socio-political biases of search engines.[89] It has also been touted as a solution to a variety of values-protection and values-promotion problems, such as the protection of privacy in Digital Rights Management (DRM) solutions[90] and the promotion of "universal usability,"[91] social justice,[92] user autonomy,[93] and many others.[94] Most significantly, it has foregrounded questions about *which* moral, ethical, or legal code should be embedded in a technological system when there is not widespread agreement on key moral values.[95] And it has asked: who are the stakeholders included in that decision?[96]

B. The Fragmented Legal Literature on Regulating Through Technology

A small but growing body of legal scholarship addresses the use of technology to regulate behavior and guide decisionmaking. It considers a variety of individual cases, including copyright, automated regulatory compliance and decisionmaking systems, and technological nudging. It is diverse in terms of values considered, lenses of analysis, and prescriptions.

The largest body of scholarship involves the battles over technology intended to enforce copyrights.[97] Such "technological protection measures" are

88. Friedman, Kahn & Borning, *supra* note 73, at 349.

89. Introna, *supra* note 58.

90. Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003).

91. Ben Shneiderman, *Universal Usability*, 43 COMM. OF THE ACM 84 (2000).

92. Alan Borning, Batya Friedman & Peter H. Kahn, Jr., *Designing for Human Values in an Urban Simulation System: Value Sensitive Design and Participatory Design*, 2 PROCEEDINGS OF THE PARTICIPATORY DESIGN CONF. 68 (2004), http://ojs.ruc.dk/index.php/pdc/article/view/317/309 [https://perma.cc/UG7W-AD42].

93. Friedman & Nissenbaum, *supra* note 48.

94. See the more detailed review of this literature in Friedman, Kahn & Borning, *supra* note 73, at 348.

95. Allen, Wallach & Smit, *supra* note 74, at 15.

96. Alsheikh, Rode & Lindley, *supra* note 34, at 82; Clark, *supra* note 80; Jessica Miller, Batya Friedman, Gavin Jancke & Brian Gill, *Value Tensions in Design: The Value Sensitive Design, Development, and Appropriation of a Corporation's Groupware System*, PROCEEDINGS OF THE 2007 INTERNATIONAL ACM CONF. ON SUPPORTING GROUP WORK 281 (2007); Katie Shilton, *Values Levers: Building Ethics into Design*, 38 SCI., TECH. & HUM. VALUES 374 (2013).

97. *See, e.g.*, Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001); Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 GEO. L.J. 1 (2006); Deirdre K. Mulligan, *Digital Rights Management and Fair Use by Design*, 46 COMM. ACM 30 (2003); Molly Shaffer Van Houweling, *Communications' Copyright Policy*, 4 J. ON TELECOMM. & HIGH TECH. L. 97 (2005); Deirdre Mulligan & Aaron Burstein, *Implementing Copyright Limitations in Rights Expression Languages*, ACM WORKSHOP ON DIGITAL RTS. MGMT. 137 (2003); Deirdre K. Mulligan, John Han & Aaron J. Burstein, *How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use,"* PROCEEDING OF THE 3RD ACM

typified by DRM software created by private parties and embedded in digital-content files for sale or distribution.[98] This norm-enforcing technology governs the way those files can be used and shared. Specifically, DRM is used to protect—and often extend—the rights of copyright holders.[99]

Scholars have identified certain attributes of DRM's operation that undermine the contours of copyright law in ways that implicate other important values. As an initial matter, the capacities of systems purportedly designed with the singular purpose of protecting existing intellectual property rights often extend to other functions as well, including not only protection, but identification, description, trading, monitoring, and tracking of user rights.[100]

Even within the rights-protection function, critics point to the ways that these sorts of copyright compliance systems can privatize what was previously a public sphere,[101] potentially enabling parties with incentives to overprotect property rights to subvert public goals. They further describe how rule-based code potentially creates perfect use constraints in ways unanticipated and unparalleled by law. Notions such as "fair use," or the "idea-expression distinction," as well as limitations on copyright incorporated into statutes or carved into the common law over decades by judges, may all be pushed aside.[102] Because fair use "inherently requires a judgment about purpose, or intent," DRM's technological constraints crowd out subjective, human elements of legal enforcement that are "beyond the ken of even the best computers."[103]

Empirical work has also shown that DRM implementations sometimes fail to conform to users' expectations regarding their rights to "personal use" of protected content.[104] "Robustness rules" for design of DRM technology, which attempt to solve the problem of copyright circumvention through a technologically based solution, threaten fundamental principles of "user agency"

WORKSHOP ON DIGITAL RTS. MGMT. 77 (2003); Stefan Bechtold, *Value-Centered Design of Digital Rights Management*, INDICARE PROJECT (Sept. 9, 2004), http://www.indicare.org/tiki-read_article.php?articleId=39 [https://perma.cc/2SDL-SU3S].

98. Digital Millennium Copyright Act, 17 U.S.C. § 1201 (2006) (anti-circumvention provisions). *See generally* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 1 (1999) (discussing legal constraints on circumvention of such private-rights-enforcing controls) [hereinafter Samuelson, *Intellectual Property and the Digital Economy*].

99. Recently, Niva Elkin-Koren has argued that for fair use to survive, we must fight code with code and suggested that developments in Artificial Intelligence can support better reasoning about fair use. Niva Elkin-Koren, *Fair Use by Design*, 64 UCLA L. REV. 1082 (2017).

100. Mulligan & Burstein, *supra* note 97; Mulligan, Han & Burstein, *supra* note 97.

101. Margaret Jane Radin, *Regulation by Contract, Regulation by Machine*, 160 J. INST. & THEORETICAL ECON. 142 (2004).

102. *See* Bechtold, *supra* note 97; Burk & Cohen, *supra* note 97; Mulligan, *Digital Rights Management*, *supra* note 97. *See generally* 17 U.S.C. § 107 (2012) (providing for copyright's fair-use exception).

103. LESSIG, CODE: VERSION 2.0, *supra* note 56, at 187.

104. Mulligan, Han & Burstein, *supra* note 97.

over technological artifacts.[105] This concern is exacerbated by most consumers' lack of either the expertise to understand its "complex technical terminology," or the bargaining power necessary to negotiate a change.[106] These deficiencies disable market constraints on the development of technological standards consistent with free private ordering of rights allocation and protection.

Finally, DRM is one way in which the private sector has employed technology to accomplish a regulatory program formerly operated in a far more public manner—namely, the protection and enforcement of copyright through lawsuits, open court proceedings, and fines imposed by the state.[107] Tim Wu, in discussing the development of Napster and other P2P programs as governing standards, demonstrates more broadly the ways that code design can function as a tool of interest group behavior. He shows how specific private stakeholders can, without going through the costly process of traditional legal regulation, advance their interests in a "lopsided" fashion and reap profits accordingly.[108]

A second body of literature considers the design of technologies intended to "force" compliance with legal mandates, particularly those related to risk management. Automated regulatory compliance systems have been effective. However, they can, in a variety of intended and unintended ways, direct behavior so as to diverge from the values reflected in the regulatory charge they are intended to satisfy. Specifically, even when the compliance technology is intended to embed legal values with fidelity, they can suffer "distortions." Such distortions arise from the social and technical environment in which regulatory norms are "translated" into hardwired code[109] and include the cognitive biases of those who design and use the technologies.[110] "Systemic effects" also result when such distortions are introduced into large, complex systems.[111]

Compliance technologies are susceptible to "opportunities for gamesmanship" by actors who are cognizant of the rule-bound nature of the systems.[112] The recent Volkswagen scandal[113] underscores the extent to which compliance technologies—even those operated by government—can be gamed in ways that subvert regulatory aims and public governance. Volkswagen used

105. TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE 240–42 (2007).

106. Cohen, *supra* note 90, at 615; *see* Pamela Samuelson & Jason Schultz, *Should Copyright Owners Have to Give Notice of Their Use of Technical Protection Measures?*, 6 J. TELECOMM. & HIGH TECH. L. 41, 59–65 (2007) (discussing generally the lack of transparency of technology protection measures).

107. Tarleton Gillespie, *Designed to 'Effectively Frustrate': Copyright, Technology and the Agency of Users*, 8 NEW MEDIA & SOC'Y 651 (2006); Bechtold, *supra* note 97.

108. Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 688 (2003).

109. Bamberger, *Technologies of Compliance*, *supra* note 11, at 706–07.

110. *Id.* at 711–14.

111. *Id.* at 710.

112. *Id.* at 714; *see also* Pasquale, *supra* note 14, at 236.

113. Russell Hotten, *Volkswagen: The Scandal Explained*, BBC NEWS (Dec. 10, 2015), http://www.bbc.com/news/business-34324772 [https://perma.cc/3BU4-4S59].

software code to detect regulatory test conditions by interpreting their external environment and, when relevant, to conform emissions levels to regulatory requirements by altering engine behavior in real time. The scandal underscored the significant role software plays in compliance with regulatory obligations. It also highlighted the way that the "deep opacity" of technology—where "[e]mbedded values can remain hidden, and the forces that shape those choices, whether governmental, social or market, are shrouded"[114]—can mask intentional deviance from regulatory requirements.

A third strain of scholarship has noted the risks of automating administrative agency decisionmaking[115] and algorithmic rules in the private sector.[116] In the context of automated decisionmaking, critics have pointed out worrying consequences of an overreliance on programmatic solutions to regulatory decisionmaking problems. First, it may deprive individuals of constitutionally enshrined rights to due process by failing to provide them with any or adequate notice of decisions, a proper opportunity to be heard, or meaningful judicial review.[117] Particular concern is needed when using automated processes to assist with criminal investigations.[118] Second, regulators may be encouraged to craft legislative provisions that lend themselves more easily to their embodiment in code.[119] With such a process, not only is code law, it also *shapes* law. Third, critics charge that governance by way of automated processes is essentially tantamount to rulemaking by programmers. It is a "troubling" delegation of legislative power that fails to satisfy norms of administrative process including transparency, participation, and legitimacy.[120] Ironically, while automated governance systems were often initially justified to the public on the basis that they would be *more* transparent than other administrative processes (after all, anybody could look under the hood and determine how decisions were algorithmically made),[121] concerns later shifted to secrecy and protection from circumvention to prevent gamesmanship and protect economic and national interests. Transparency became a value of diminished importance or even actively opposed.[122]

114. Bamberger, *Technologies of Compliance*, *supra* note 11, at 723 (footnote omitted).

115. Citron, *supra* note 13, at 1260–67 (describing the design, implementation, and hurdles of automated-decision systems used for public-benefit programs such as Colorado's state benefits, the Food Stamp Act, and the National School Lunch Program); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014); Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1 (2005).

116. Introna, *supra* note 58; Pasquale, *supra* note 14.

117. Citron, *supra* note 13.

118. Steinbock, *supra* note 115.

119. Citron, *supra* note 13, at 1255.

120. *Id.* at 1288–98.

121. Pasquale, *supra* note 14, at 236.

122. *Id.* at 236–37.

Related concerns arise where technology is employed in the operation of government functions, such as voting[123] or recidivism-risk determinations.[124] Here, values such as efficacy, accuracy, reliability, security, privacy, and fairness are paramount, yet these systems have been found wanting along these dimensions—such as insecure voting systems[125] and biased recidivism predictions.[126] These particular malfunctions have been traced, in part, to a different variety of opacity, —one arising from privatization. Either because the system's software is proprietary[127] or shielded as a matter of public policy,[128] the source code is secret. Public functions become privately managed. Such closed-source code leaves outsiders "unable to discern how a system operates and protects itself"[129] and shields unintended errors that distort even clear legal and managerial goals.

---

123. Danielle Keats Citron, *Open Code Governance*, 2008 U. CHI. LEGAL F. 355, 365 (2008); Joseph Lorenzo Hall, Policy Mechanisms for Increasing Transparency in Electronic Voting (2008) (unpublished Ph.D. dissertation, University of California, Berkeley).

124. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias: There's Software Used Across the County to Predict Future Criminals. And it's Biased Against Blacks*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/WK73-BW9S].

125. *See* Cal. Sec'y of State, *Top-to-Bottom Review*, CAL. SECRETARY OF STATE (2007), http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ [https://perma.cc/4LVR-GWG8]; News Release, Debra Bowen, Cal. Sec'y of State, Secretary of State Debra Bowen Moves to Strengthen Voter Confidence in Election Security Following Top-to-Bottom Review of Voting Systems (Aug. 3, 2007), http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/db07-042-ttbr-system-decisions-release.pdf [https://perma.cc/8VVG-KGPU].

126. Angwin et al., *supra* note 124. *But see* Jon Kleinberg, Sendhil Mullainathan & Manish Raghavan, *Inherent Trade-Offs in the Fair Determination of Risk Scores*, PROCEEDINGS OF THE 8TH INNOVATIONS IN THEORETICAL COMPUTER SCI. CONF. (2016), https://arxiv.org/pdf/1609.05807v2.pdf [https://perma.cc/YTG8-M5CA] (explaining that alternate concepts of fairness cannot be met by the same scoring mechanism and showing that while the objections of Angwin et al. to the uneven distribution of false positive and false negative error rates were valid fairness concerns with the performance of the system, the system could not be both well calibrated and have equally distributed error rates across races because of the unequal distribution of the base rate in the data).

127. *See* Brauneis & Goodman, *supra* note 18, at 38–44 (reporting on cities' use of trade secrecy to limit responses to Public Record Act requests for information about algorithms); *id.* at 44–47 (reporting on cities' resisting Public Record Act requests about algorithms due to concerns about gaming or circumvention and other concerns); Citron, *supra* note 13, at 357 ("Because these systems' software is proprietary, the source code—the programmers' instructions to the computer—is secret."); Nicholas Diakopoulos*, We Need to Know the Algorithms the Government Uses to Make Important Decisions About Us*, CONVERSATION (May 23, 2016, 8:48 PM), https://theconversation.com/we-need-to-know-the-algorithms-the-government-uses-to-make-important-decisions-about-us-57869 [https://perma.cc/RCT4-6ZS7] (describing that open records requests about criminal justice algorithms were denied because of proprietary interests).

128. Katherine Fink, *Opening the Government's Black Boxes: Freedom of Information and Algorithmic Accountability*, INFO., COMM. & SOC'Y 1–19 (May 30, 2017), https://doi.org/10.1080/1369118X.2017.1330418 [https://perma.cc/ATP4-KRZ8] (reviewing current state of law and practice with respect to whether algorithms would be considered "records" under the Freedom of Information Act, and reviewing agency bases for withholding algorithms and source code under FOIA requests and finding exemptions claimed under national security, privacy, law enforcement investigations as well as trade secrecy exemptions).

129. Citron, *supra* note 13, at 357.

Most recently, a fourth vein of scholarship has begun to articulate the democratic deficits of regulating through nudging, by architectural or other means.[130] These scholars point to the particularly invidious way that design—technological or otherwise—can create the illusion of choice and autonomy by systematically exploiting cognitive biases that bypass rational decisionmaking processes and invoke intuitive, emotional processes.[131]

Regulation scholar Karen Yeung identifies a legitimacy deficit inherent in these methods of regulation, arising from "their lack of transparency, violating constitutional requirements that all governmental action should be transparent and open to public scrutiny, thereby ensuring that the government is legally and democratically accountable for its actions."[132] Because of this, Yeung explains, individuals regulated by traditional legal mandates on the one hand, and surreptitious "nudging" on the other, both act in a "nonvoluntary" manner. But the source of the nonvoluntariness in the second instance is a form of deception that hides the choices of the designer.

Nudging, like regulation through design, can derive its operative force from a deceptiveness and invisibility at the moment of its operation that reduce citizen comprehension of political choices and undermine traditional mechanisms of political accountability. Cass Sunstein argues that invisibility in the moment that a "nudge" operates can be acceptable, so long as the initial political choice was conducted under "careful public scrutiny."[133] Yet new empirical research, like that conducted by Adam Hill, suggests that an accountability deficit is pronounced—and yields the same behavioral consequences—even when "nudging" is equally visible as traditional legal forms of regulation.[134] As his data in those cases reveals, "individuals blame regulators less for failed nudges than for failed laws."[135]

In sum, this scholarship identifies limits of, and regulatory flaws in, the technological implementations of policy and has begun to suggest remedies. But the legal literature has not yet used a broader lens to surface and connect the wholesale rise of governance-by-design, the range of value skirmishes it

130. *See* Ryan Calo, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773 (2014) (explaining the similarities of regulation that relies on "nudge," "code," and the provision of information).

131. *See* Karen Yeung, *The Forms and Limits of Choice Architecture as a Tool of Government*, 38 LAW & POL'Y 186, 195 (2016) (explaining that using architectures as a regulatory means to force human choices involves "a form of invidious manipulation, deliberately seeking to bypass the individual's rational decision-making processes. . . . they are *nonvoluntary*, analogous to decisions made on the basis of intentional deception that typically mitigate the individual's responsibility for the affected decision.").

132. *Id.*

133. Cass R. Sunstein, *The Storrs Lectures: Behavioral Economics and Paternalism*, 122 YALE L.J. 1826, 1893 (2013).

134. Adam Hill, *Why Nudges Coerce: Experimental Evidence on the Architecture of Regulation*, J. SCI. ENGINEERING ETHICS (published online July 4, 2017), https://doi.org/10.1007/s11948-017-9944-9 [https://perma.cc/MD7F-E7FJ].

135. *Id.*

surfaces, and the insufficiency of current decisionmaking structures and processes to resolve them in ways consistent with fundamental public norms.

We seek to remedy this analytic absence by providing a framework for saving governance-by-design. To that end, the following section explores five recent design battles across a range of substantive areas. These cases begin to illuminate specific ways that existing government and policymaking institutions are poorly designed to regulate through design, and how this threatens a fundamental governance dystopia. We then propose a set of rules of engagement for addressing these issues in ways consistent with public governance principles.

II.
CASE STUDIES: GOVERNANCE DYSFUNCTION IN FOUR TECHNOLOGY DESIGN BATTLES

Four recent high-profile battles exemplify the governance challenges and risks to public values in regulating through technology. Each case demonstrates one or more of the core and interrelated regulatory problems with governance-by-design. Together, these skirmishes point to a cycle by which opaque decisionmaking in ill-equipped forums uninformed by trusted expert analysis produces designs that undermine other key values and make recalibration among values difficult and costly. These compound challenges, over time, threaten to erode trust not only in the decisions made, but also in decisionmaking institutions and processes.

A. Case 1: Apple v. FBI and the Ongoing Cryptowars

The December 2015 terrorist attack in San Bernardino, California had one repercussion that was unexpected and potentially far-reaching: the subsequent criminal investigation sparked a fierce battle over technology design between the FBI and Apple. The resulting court case constituted the latest conflict in the ongoing "crypto wars" over efforts to build ways for law enforcement to access encrypted communications[136] and highlights a range of dysfunctions involved in setting policy through technical design.

After the San Bernardino attackers were killed in a shootout with police, the FBI discovered an Apple iPhone in their car. Agents tried unsuccessfully to reset the phone's password, inadvertently locking the phone's contents. To protect the privacy of its users, Apple had begun encrypting the data in iPhones

136. Steven Levy, *Why Are We Fighting the Crypto Wars Again?*, WIRED (Mar. 11, 2016, 12:00 AM), https://www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again [https://perma.cc/KB4J-J868]; Deirdre K. Mulligan & Kenneth A. Bamberger, *Apple v. FBI: Just One Battle in the 'Design Wars,'* LAW.COM (Mar. 21, 2016, 3:08 PM), *https://www.law.com/sites/lawcomcontrib/2016/03/18/apple-v-fbi-just-one-battle-in-the-design-wars* [https://perma.cc/2AES-HGFY].

so that no one, not even Apple, could access it without the user's consent.[137] When the FBI approached Apple for assistance, they gave the FBI relevant information on its servers but refused to write code to unlock the encrypted phone.

The Bureau then turned to the judiciary to resolve the matter. Citing the 1789 All Writs Act, the FBI presented a federal district court with an ex parte demand to force Apple to create software to help them defeat the phone's encryption by creating a technological "back door" that could allow the government access to the data stored on millions of Apple devices.[138] In essence, the FBI asked the court to confer an extraordinary power, the ability to require a company redesign of product features.

In normal circumstances, the ex parte demand would have deprived the court of Apple's perspective altogether. However, the FBI filed a procedurally unnecessary motion to compel Apple to comply with the assistance order,[139] which created an opportunity for Apple and numerous organizations raising diverse concerns about the FBI's request to weigh in. Human rights, civil liberties groups, and the UN Special Rapporteur for Freedom of Expression lodged their concerns about the implications for U.S. residents, dissidents, and especially individuals in countries with repressive governments in amicus curiae briefs.[140]

The FBI's request was particularly bold given that, over the years, Congress had repeatedly withheld broad law enforcement access by design requirements, despite pressure from law enforcement. For example, CALEA, which was

137. The phone's owner (the San Bernardino County Health Department) gave the government permission to break into the phone, but Syed Farook, the mass murderer who used the phone and encrypted its contents, , was deceased. Mulligan & Bamberger, *supra* note 136.

138. Ron Wyden, *This Isn't About One iPhone. It's About Millions of Them*, WIRED (Feb. 19, 2016, 12:00 AM), https://www.wired.com/2016/02/this-isnt-about-one-iphone-its-about-millions-of-them [https://perma.cc/GU9R-69M9].

139. Government's Motion to Compel Apple Inc. to Comply With This Court's February 16, 2016 Order Compelling Assistance in Search at 16–18, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

140. *See* Press Release, Apple, Amicus Briefs in Support of Apple (Mar. 2, 2016), https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple [https://perma.cc/L6HN-N3HG]; Brief of Amici Curiae American Civil Liberties Union, ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties, in support of Apple, Inc., In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016), ECF No. 57; Brief of Amici Curiae Privacy International and Human Rights Watch, In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016), ECF No. 72; Brief of the Center for Democracy & Technology as Amicus Curiae in support of Apple Inc.'s Motion to Vacate and in Opposition to Government's Motion to Compel Assistance, In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016), ECF No. 98; Letter from David Kaye, Special Rapporteur on the Promotion & Prot. of the Right to Freedom of Op. & Expression, United Nations Human Rights Council, to Hon. Sheri Pym (Mar. 2, 2016), https://freedex.org/wp-content/blogs.dir/2015/files/2017/08/Letter_from_David_Kaye_UN_Special_Rapporteur_on_the_promotion_and_protection_of_the_right_to_freedom_of_opinion_and_expression.pdf [https://perma.cc/556D-5X5F].

enacted in 1994,[141] details a limited set of responsibilities for telecommunication service providers to ensure that their "equipment, facilities, or services" allow the government to intercept communications pursuant to a court order or other lawful authorization.[142] CALEA prohibits law enforcement from requiring "any specific design of equipment, facilities, services, features."[143] CALEA specifies which kinds of companies must assist the government in its surveillance orders and what assistance those companies must provide.[144] Congress specifically excluded firms such as Apple from its regulatory ambit.[145] It also rejected decryption obligations (except in limited circumstances not present in the case) and, above all, design mandates.[146] Moreover, CALEA includes a procedure for addressing the evolution of technologies that might replace telecommunication services. It authorizes the Federal Communications Commission (FCC) to extend the obligations to support law enforcement access to services that are a "replacement for a substantial portion of the local telephone exchange service."[147] Under this provision, the FBI has obtained FCC authority to monitor Voice over Internet Protocol (VoIP) and other Internet-based communications. CALEA, together with the 1986 Electronic Communications Privacy Act (ECPA),[148] which governs law enforcement access to electronic communications held by service providers such as Apple, created a comprehensive statutory regime that did not support the FBI's request.

In addition, although denied by the FBI, the subsequent record demonstrated that such demands by law enforcement would not have stopped

141. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012)).

142. 47 U.S.C. § 1002(a)(1) (2012).

143. *Id.* § 1002(b)(1)(A).

144. *Id.* § 1002(a) (coverage of telecommunication carriers) and (b)(2) (explicit exclusion of information service providers and private networks).

145. CALEA defines a limited set of firms that must assist law enforcement in special ways. Specifically, "telecommunications carriers" would be obligated to make sure that their "equipment, facilities, or services" allow the government to intercept communications pursuant to a court order or other lawful authorization. 47 U.S.C. §§ 1001(8)(A), 1002(a)(1). CALEA defines "telecommunications carrier" as a "person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." *Id.* § 1001(8)(A). Apple is not a common carrier but would be classified under CALEA as an "information service," which is explicitly excluded from coverage.

146. Even covered entities, like telecommunication carriers, are not required to redesign their system configurations. In addition, except for where "the encryption was provided by the [telecommunications] carrier and the carrier possesses the information necessary to decrypt the communication," telecommunications carriers have no obligation to "decryp[t], or ensur[e] the government's ability to decrypt, any communication encrypted by a subscriber or customer." *Id.* § 1002(b)(3). And CALEA may not be used to force firms to maintain an "encryption service for which [a carrier] does not retain the ability to decrypt communications for law enforcement access." S. REP. NO. 103-402, at 24 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3504.

147. 47 U.S.C. § 1001(8)(B)(ii) (2012).

148. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986) (codified at 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3126).

with this single device.[149] Indeed, the FBI and other intelligence agencies continually press for restrictions on encryption in consumer products and special keys for de-encrypting information.[150]

For instance, former FBI Director James B. Comey had also lobbied the Obama Administration to press the Bureau's case in Congress. But the White House, unlike individual agencies, must think through the full range of equities at issue in policy changes and has formal mechanisms such as the National Economic Council and National Security Council to do so. During the Obama Administration, there was ongoing debate about how to address the competing interests at issue, but no clear resolution. As a result, Director Comey switched his focus to the private sector where he sought to negotiate privately with companies to address the agency's needs. However, these efforts further subverted the public processes that had declined to embed his priorities in the technical infrastructure.

Like previous crypto battles, the San Bernardino case was initially cast simply as a contest between privacy and law enforcement and national security. Apple and its many supporters, including public advocates, academics, and industry officials, contended that other important values were at play.[151] Apple argued that opening a so-called "back door" into their phones exposed national security networks to penetration by malicious hackers, including ones from other nations.[152] Human rights advocates, aware of the reach of Apple's products, expressed particular concern about the global implications of the requested technical redesign and the resulting legal precedent for freedom of expression.[153] Security experts alerted the court to the wide repercussions for collective safety and security of a ruling weakening cryptography through the creation of mandatory backdoors.[154] Former national intelligence officials weighed in on the

149. Declaration of Nicola T. Hanna in Support of Apple Inc.'s Motion to Vacate Order Compelling Apple, Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance ¶ 5 & Ex. C, In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Feb. 25, 2016), ECF Nos. 16-1 & 16-4.

150. *Perils of Back Door Encryption Mandates: 'Five Eyes' Nations Should Support, Not Threaten, Digital Security*, HUM. RTS. WATCH (June 26, 2017, 10:52 AM), https://www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates [https://perma.cc/MF73-9L5R] (discussing efforts in various "Five Eyes" countries to mandate or otherwise obtain encryption backdoors).

151. Wyden, *supra* note 138 ("[I]f the FBI can force Apple to build a key, you can be sure authoritarian regimes like China and Russia will turn around and force Apple to hand it over to them. They will use that key to oppress their own people and steal U.S. trade secrets.").

152. Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, In the Matter of the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Feb. 25, 2016).

153. Brief of Amici Curiae Privacy International and Human Rights Watch, In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016); Letter from David Kaye, *supra* note 140.

154. Brief of Amici Curiae Iphone Security and Applied Cryptography Experts, In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 2, 2016).

security concerns, stating that while access to encrypted data might promote national security, weakening systems to enable such access compromises overall system security and can thereby also threaten that same national security.[155] For these reasons, former NSA and CIA Director Michael Hayden concluded that, on balance, America is "more secure with end-to-end unbreakable encryption."[156] The remedy requested by the FBI, moreover, would have ramifications for broader issues like consumer security, intellectual property, and human rights.

The number of values and parties implicated in this design battle illustrates the limitations of bilateral court processes to adequately address them. A win for the FBI would have indicated that company engineers could be conscripted by law enforcement to create code to crack devices they had placed into the market.

Inevitably, at least some if not most companies would likely build back doors in from the get-go, creating a veritable slippery slope. These back doors, unlike a legal process that allows those in specific government roles (such as law enforcement) to go to court and gain lawful access to communications once a specific legal standard is met, could be used by anyone who finds them—no standard, no process, and no court involvement. Over time, the proliferation of back doors in response to the court action in this case would upend the balance of values chosen by the legislature.

The district court never had the chance to rule on this dispute. FBI Director Comey withdrew the motion after a private company assisted the agency in breaking into the phone.[157] This case reveals how the Bureau sought to relocate important debates over competing values from open, public participatory processes to closed processes—and ultimately to solutions behind closed doors.

B. Case 2: The Wholesale Regulatory Embrace of "Privacy-by-Design"

Governance-by-design has nowhere been embraced more publicly and unabashedly than in the context of "Privacy-by-Design"—in the words of the Conference of Privacy and Data Protection Commissioners from across the world: the project of "embedding privacy as the default into the design, operation and management of ICT and systems, across the entire information life cycle."[158]

---

155. Wall Street Journal, *Hayden: The Pros and Cons of Access to Encrypted Files*, YOUTUBE (Feb. 17, 2016), https://www.youtube.com/watch?time_continue=4&v=6HNnVcp6NYA [https://perma.cc/95SV-X6SM].

156. Rachael King, *WSJ CIO Network: Former Director of CIA, NSA Argues for End-to-End Encryption*, WALL ST. J. (Feb 2, 2016, 3:06 AM), http://blogs.wsj.com/cio/2016/02/02/wsj-cio-network-former-director-of-cia-nsa-argues-for-end-to-end-encryption [https://perma.cc/7EMP-9WAH].

157. Government's Status Report, In the Matter of the Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 28, 2016) (asking the court to vacate a motion to compel).

158. *Resolution on Privacy by Design*, 32ND INT'L CONF. OF DATA PROTECTION AND PRIVACY COMMISSIONERS (Oct. 27-29, 2010), https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf [https://perma.cc/Y6FL-7MGQ].

Yet while protecting and privileging one public value by embedding it technologically, well-organized privacy advocates and regulators promoting this project have, largely inadvertently, excluded important competing values.

Privacy and consumer protection regulators have long raised concerns about the use of personal and even de-identified data to classify individuals for the purpose of tailoring services and products. While some commentators recognized the negative implications for privacy and civil rights concerns about antidiscrimination and fairness,[159] the initial regulatory response was to push companies harder to provide privacy protection "by design."[160]

Beginning in the mid-1990s and escalating in recent years, privacy regulators and advocates have sought to protect privacy by minimizing the collection of data and the identifiability of collected data, among other methods.[161] For example, the Federal Trade Commission (FTC), members of Congress, and European privacy regulators encouraged the development of technical specifications to support individual control over online tracking.[162] Privacy design solutions initially dominated the landscape for two reasons. First, information privacy, or data protection, provides a well-developed set of substantive policies, practices, actors, and institutions that address an issue obviously at stake in the collection and use of data—particularly big data.[163] Privacy regulators and professionals are well-organized and have proven adept

159. Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35 (2013).

160. *See generally* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 (2011) (describing the Federal Trade Commission's (FTC) Proposed Framework on protecting consumer privacy as well as FTC enforcement actions).

161. *See Resolution on Privacy by Design*, *supra* note 158; Edith Ramirez, Commissioner, Fed. Trade Comm'n, Privacy by Design Conference Hong Kong: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission (June 13, 2012) (describing the FTC's policy and enforcement actions aimed at promoting privacy-by-design); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS iii, 22–34 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [https://perma.cc/U9AW-WM9P] (directing companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services and describing its encouragement and support for the development of browser-based tools for consumers to request that websites not track their online activities and the World Wide Web Consortium's Do Not Track specification, a universal web protocol to help consumers control online tracking).

162. Doty & Mulligan, *supra* note 68, at 149-53 (describing stakeholder, including regulatory and legislative, engagement with the Tracking Protection Working Group at W3C working on the specification commonly known as Do Not Track (DNT)).

163. *See* Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 435–40 (2011) (discussing the influence of privacy regulators in Northern European Union member states on the adoption of corporate compliance officers and industry codes of conduct and techniques, such as privacy seals and privacy impact statements, that are hallmarks of privacy-by-design); and more generally, see ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (2008) (documenting the formidable and indeed outsized role member state data protection authorities played in the creation of the structure and requirements of the EU Directive, which focused on data minimization among other things).

at moving the privacy protection agenda forward. Thus, the information privacy regime is both an easy and relatively profitable one to rally, and the actors and institutions associated with it are ready and able to address problems with big data. Second, protecting privacy has an intuitive connection to limiting discrimination—you can't misuse knowledge you don't have. Privacy-oriented design solutions were bolstered by an understandable if ill-founded assumption that privacy solutions—specifically, the ability to withhold or hide information—could protect against discriminatory or unfair uses of big data.

Unfortunately, the political and intellectual monopoly that information privacy initially held over the policy discourse about the design of big data systems and practices placed other values at risk. Information privacy solutions proved not just ill-equipped for protecting discrimination or fairness in the face of big data but also detrimental where structural or implicit discrimination was at issue.[164] Reducing the collection of data about protected class status can constrain its intentional use to discriminate. But it removes data that is useful if not essential for identifying the latent, redundant encoding of protected traits that algorithms are so adept at finding. Because protected traits that are predictive of relevant differences will be redundantly encoded in other data that is mined to produce classifications, recognizing and eliminating such classifications depend upon access to data about protected classes. For this reason, the practice of identifying and policing discriminatory practices requires data about the race and gender of, for example, job applicants and employees, so that it can be determined whether other kinds of classifications that are being used inappropriately correlate with protected traits. Rooting out this unintentional bias would require knowing that protected groups are arrayed differently along this set of dimensions and would require data about legally protected statuses. This form of unintentional statistical discrimination that can occur in automated decisionmaking systems "may also normalize the far more massive impacts of system-level biases and blind spots."[165] For example, journalists at ProPublica using data about the race of defendants in arrest records to document that a proprietary system for assessing the recidivism risk had a higher rate of false positives and lower rate of false negatives for black defendants.[166] Limiting the availability of attributes like race, gender, and nationality can limit blatantly intentional discrimination but confounds efforts such as this to root out more invidious forms of discriminatory profiling.

Unlike the FBI v. Apple crypto-battle, the privacy-by-design agenda was the product of accountable, participatory processes in government agencies.[167]

---

164. Dwork & Mulligan, *supra* note 159.

165. Dwork & Mulligan, *supra* note 159, at 37 (quoting Oscar H. Gandy Jr., *Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems*, 12 ETHICS & INF. TECH. 29, 37–39 (2010)).

166. Angwin et al., *supra* note 124.

167. Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Dir 95/46/EC

But those agency venues were oriented towards promoting a singular policy focus rather than the whole range of competing values. To be sure, privacy and consumer protection regulators are increasingly attentive to the need of thinking across multiple values. In the United States, the FTC has provided a forum for discussions regarding both privacy and fairness, while European data protection authorities, too, consider privacy and bias together.[168]

Yet despite recognition of the complicated interaction between privacy-by-design and fairness-by-design (now its own area of technical and legal research),[169] privacy-by-design was first out of the gate and has already had an impact on practice. To the extent privacy-by-design solutions foreclose architectures, algorithmic design, or the collection of data necessary to design, deploy, and oversee systems to ensure fairness, they may have already locked in one value at the expense of the other. Depending upon where privacy is built in, retooling designs to assist in protecting against and identifying discrimination after the fact may be prohibitively expensive or difficult because of dependencies across components or systems. How to prioritize technical designs that assist in policing or avoid discrimination, relative to those that protect privacy, is a policy conversation that extends and impacts numerous other regulatory agencies. Ensuring both values are discussed simultaneously during prioritization and building is essential.

C. Case 3: The SOPA Battle

The battle over the 2012 Stop Online Piracy Act (SOPA)[170] similarly involved an attempt to protect one value through design—here, intellectual property rights. In seeking to provide such protection, however, Congress sought a wide-reaching technological solution at the expense of a range of other values including security, access to information, and freedom of expression. In this case, Congress's committee structure, partisanship, and lack of trusted, independent technical expertise led to a design proposal that threatened to undermine the very

(General Data Protection Regulation), 2016 O.J. (L 119) 1 (adopting privacy-by-design as a regulatory requirement); FED. TRADE COMM'N, *supra* note 161 (recommending companies adopt privacy-by-design as a best practice).

168. The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251 16 (adopted on 3 October 2017) (calling for regular assessments of bias in data sets and systems and "procedures and measures to prevent . . . discrimination on the basis of special category data").

169. See FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY IN MACHINE LEARNING, https://www.fatml.org [https://perma.cc/AT5L-K2M7], and CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, https://fatconference.org/index.html [https://perma.cc/FC9V-H24D], for an overview of growing research and community around fairness, accountability, and transparency in machine learning.

170. Stop Online Piracy Act of 2011, H.R. 3261, 112th Cong. (2011).

infrastructure and security of the Internet before the bill was ultimately shelved.[171]

SOPA was introduced ostensibly to expand the ability of U.S. law enforcement to combat online copyright infringement and online trafficking of counterfeit goods occurring on foreign-owned-and-operated websites. To achieve this, the bill mandated Domain Name System (DNS) blocking of websites and web services known to host copyrighted material without authorization.[172]

The DNS is one of a few protocols central to the operation, usability, and scalability of the Internet. It provides a universal mapping from website names to Internet Protocol (IP) addresses, a sort of dynamic phone book for the Internet.[173] DNS "blocking" would interfere with this universal mapping, making it difficult for users to locate specific domains.[174] Further, DNS blocking is incompatible with Domain Name System Security Extensions (DNSSEC), the method that provides secure authentication of both ends of an Internet connection through the use of cryptography.[175] This mutual authentication thwarts man-in-the-middle attacks used to redirect traffic to fraudulent and otherwise illicit websites.[176]

SOPA's DNS-blocking provision would have required DNS operators to break a security feature of the web that had been embraced by the U.S. government as well as the technical community. Civil liberties and human rights groups also emphasized that using the DNS in this way would signal to other countries that manipulating the Internet infrastructure to control access to information and suppress speech (effectively Balkanizing the Internet) was acceptable.

---

171. Jonathan Weisman, *After an Online Firestorm Congress Shelves Antipiracy Bills*, N.Y. TIMES (Jan. 20, 2012), http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html [perma.cc/7G6J-BTX8] (describing House Judiciary Chairman Lamar Smith's statement that consideration of the bill was postponed and then Senate Majority Leader Harry Reid's tweet delaying consideration of the Senate bill).

172. Stop Online Piracy Act, H.R. 3261.

173. STEVE CROCKER ET AL., SECURITY AND OTHER TECHNICAL CONCERNS RAISED BY THE DNS FILTERING REQUIREMENTS IN THE PROTECT IP BILL 3–4 (2011), http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf [https://perma.cc/SAL4-CMEV].

174. *Id.*

175. *Id.* at 5–6; Pamela Samuelson, *Can Online Piracy Be Stopped by Laws?*, 55 COMM. ACM 25, 26 (2012) ("SOPA is fundamentally inconsistent with DNSSEC . . . ."). *See generally Overview of DNSSEC*, MICROSOFT DOCS (Feb. 11, 2014), https://technet.microsoft.com/en-us/library/jj200221(v=ws.11).aspx [http://perma.cc/9768-RRNM]; David Bruggeman, *USACM Statement on SOPA and PROTECT IP*, ASS'N FOR COMPUTING MACHINERY (Jan. 18, 2012), https://techpolicy.acm.org/2012/01/usacm-statement-on-sopa-and-protect-ip [https://perma.cc/Z477-W9XC] (referring to SOPA and explaining that "[t]he proposed legislation, including the manager's amendment in SOPA, will impose significant negative consequences on the proper functioning of DNS, and especially with the ongoing implementation of DNSSEC").

176. Crocker et al., *supra* note 173, at 5.

Ironically, the United States had championed and shepherded through the Organization for Cooperation and Economic Development (OECD) an important agreement—the Internet Policymaking Principles—designed to keep policy battles out of the core elements of the Internet infrastructure, such as the DNS, for fear of the fallout for human rights and Internet functionality.[177] While many of these concerns were raised early in the process, a set of structural and procedural factors limited the extent to which they were heard, vetted, and addressed by Congress.

1. Institutional Shortcomings in Decisionmaking: The Lack of Congressional Committee Input

Congressional committees are organized around subject-matter expertise relevant to specific national interests, industries, legal topics, or government activities. Normally, staying within the substantive lines of their jurisdiction and allowing for sequential and concurrent referrals where necessary ensure that each committee's work contributes to the development of reasonably coherent federal law. While statutes developed through different committees may interact oddly or even appear to conflict in some instances, they can coexist until there is a need to resolve their interaction through regulation or court proceeding.

Technology is far less forgiving. Choices must be made. Different committees may decide to use technology to support different values and fail to foresee the impact on values and interests outside their domain. Further, rules adopted under then-House Speaker Newt Gingrich in 1994 discourage sequential or joint referral, complicating efforts to identify cross-committee impacts of bills, particularly the potentially pernicious effects of regulating through technology.[178]

These structural issues led to a lack of attention to SOPA's DNS provisions. The Judiciary Committees in the House and Senate exercised exclusive jurisdiction over SOPA, yet neither had substantive expertise in cybersecurity. Committees with substantive responsibility for cybersecurity or national security were not part of the legislation process until late in the game.[179] It was only when

177. *See* OECD, OECD PRINCIPLES FOR INTERNET POLICY MAKING (2014), https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policymaking.pdf [https://perma.cc/WG9C-M3KQ]; *see also* Danny Weitzner & Karen Kornbluh, *Agreement Reached on Internet Policymaking Principles*, WHITE HOUSE BLOG (July 1, 2011, 11:30 AM), https://obamawhitehouse.archives.gov/blog/2011/07/01/agreement-reached-internet-policymaking-principles [https://perma.cc/T7W8-E4PH].

178. Adopting the Rules of the House of Representatives for the One Hundred Fourth Congress, H.R. Res. 6, 104th Cong. § 205 (1995) (enacted).

179. *See* EDWARD LEE, THE FIGHT FOR THE FUTURE: HOW PEOPLE DEFEATED HOLLYWOOD AND SAVED THE INTERNET—FOR NOW, 79–80 (2013) (discussing a hearing on cybersecurity issues in SOPA scheduled for January 12, 2012, by House Committee on Government Oversight and Reform, which was ultimately postponed as the bill died); Dan Lungren, *Issue Position: SOPA*, VOTE SMART FACTS MATTER (Jan. 1, 2012), https://votesmart.org/public-statement/671801/issue-position-sopa#.WqWfZxMbP4N [https://perma.cc/RQE4-3YAD] (objecting to the lack of "hearings in the

Republican national security experts and Republican grassroots began to voice concerns that relevant committee chairs became engaged.[180]

2. Skewed Stakeholder Involvement: Corporate Dominance

Structural issues, moreover, were compounded by the tilt of interests providing input into the governance decision. In the past, hearings had allowed for a diversity of views, often including nongovernmental organizations representing consumers and constitutional and environmental rights. But the Republican-controlled Congress has increasingly structured hearings along partisan lines and favoring corporate perspectives. This was the case with SOPA.[181] The House held only one hearing that included only two non-corporate witnesses: the Library of Congress's Master of Copyrights and the President of the Professional Department for Professional Employees at the AFL-CIO.[182]

As a result, the Committee was not exposed to the full range of values at issue. Proponents of SOPA viewed the DNS provision as a critical means of expanding the law's extraterritorial impact.[183] And the ability to practically disappear servers outside the country offered a way to stem infringement unparalleled by legal approaches.[184] Some companies were concerned with the DNS provisions and requested their removal.[185] But most of the service providers who would be required to implement it—and understood its security ramifications—did not actively oppose the DNS provisions.[186] In addition, at

---

Judiciary Committee on this issue" and that "none of the witnesses who testified at the one hearing we held were sufficiently knowledgeable on this issue to even discuss it"); Declan McCullagh, *New Flap Over SOPA Copyright Bill: Anti-Web Security?*, CNET (Nov. 16, 2011), https://www.cnet.com/news/new-flap-over-sopa-copyright-bill-anti-web-security [https://perma.cc/G89F-AUGR] (Rep. Dan Lungren, head of the Homeland Security subcommitteee on cybersecurity raising concerns about SOPA interfering with DNSSEC).

180. *See* Edward, *supra* note 179, at 99–101 (discussing importance of Heritage Foundation and Redstate to Republican members changing position on SOPA); Stewart Baker, *The SOPA War: Why the GOP Turned on Piracy*, HOLLYWOOD REP. (Feb. 2, 2012, 11:00 AM), https://www.hollywoodreporter.com/news/sopa-hollywood-gop-piracy-286648 [https://perma.cc/7C8A-DXM2] (discussing why Republicans abandoned SOPA).

181. Eva Galperin, *Who's Missing From Today's SOPA Hearing? A Short List*, ELECTRONIC FRONTIER FOUND. (Nov. 16, 2011), https://www.eff.org/deeplinks/2011/11/whos-missing-todays-sopa-hearing-short-list [https://perma.cc/USZ5-HPPV] (discussing lack of balance and public interest representation).

182. *Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. (2011).

183. *Id.* at 68–79 (testimony of Michael P. O'Leary, Senior Executive Vice President, Global Policy And External Affairs, on behalf of the Motion Picture Association of America, explaining that SOPA addresses "the rogue websites and cyberlockers. . . . [that] do not comply with DMCA requests, because their purpose is to traffic in stolen content. And when they are based overseas, they can simply thumb their noses at U.S. law").

184. *Id.*

185. *Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. 171–72 (2011).

186. *Id.*; *see also* Mike Masnick, *Comcast—Owner of NBC Universal—Admits that DNS Redirects are Incompatible with DNSSEC*, TECHDIRT (Jan. 11, 2012, 7:35 AM),

least one Internet Service Provider (ISP), AT&T, had expressed a willingness to engage in domain-name-level blocking of sites through a legal process, which would be easier and less costly to implement than other options.[187]

Despite being largely shut out of the formal legislative process, the technical community, advised and aided by a small group of policy insiders, alerted Congress to the cybersecurity implications of the provision.[188] Human rights and civil liberties organizations warned Congress of the provision's dire impact on international Internet policy and human rights and civil liberties globally.[189] For example, the Center for Democracy and Technology (CDT) and the Electronic Frontier Foundation (EFF), which had a long track record of working closely with technologists, raised technical concerns over DNS—including risks to speech from over-blocking, to cybersecurity from interference with DNSSEC, and to stability should the DNS be hijacked to meet policy goals.[190] Leading technical experts subsequently wrote a detailed whitepaper explaining the bill's threat to the stability and security of the Internet.[191]

The Committee failed to heed the experts. One reason, consistent with regulatory capture theory, may have been that the Committee was inclined to discount the concerns of entities they dealt with infrequently.[192] The Judiciary Committees in the Senate and House oversee important and high-profile issues (judicial appointments, civil rights, immigration, etc.), but their jurisdiction over intellectual property consistently brings in corporate interests.[193] Many of the

---

https://www.techdirt.com/articles/20120110/18081517371/comcast-owner-nbc-universal-admits-that-dns-redirects-are-incompatible-with-dnssec.shtml [https://perma.cc/2BX9-DX5L].

187. Nate Anderson, *AT&T Wants 3 Strikes Tribunal, Government Website Blacklist*, ARS TECHNICA (Apr. 30, 2010, 12:20 PM), https://arstechnica.com/tech-policy/2010/04/att-calls-for-us-3-strikes-tribunal-web-censorship [https://perma.cc/J2Z8-RZXL].

188. *Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. 42–43 (2011).

189. Letter from the International Civil and Human Rights Community to Chairman Lamar Smith and Rep. John Conyers on H.R. 3261 The Stop Online Piracy Act (Nov. 15, 2011), https://www.scribd.com/document/72833350/SOPA-Letter-From-Int-l-Human-Rights-Community [https://perma.cc/AUE3-DQVL].

190. *Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. 158–59 (2011).

191. Crocker et. al, *supra* note 173, at 5; *see also* An Open Letter from Internet Engineers to the United States Congress (Dec. 15, 2011), https://www.eff.org/files/internet-engineers-letter.pdf [https://perma.cc/5UCD-UDAL].

192. *See* DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION (1991); MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1980).

193. *See About the Committee*, HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE, https://judiciary.house.gov/about-the-committee [https://perma.cc/86ZE-FJ9N] (outlining the jurisdiction of the committee); *About the Committee: Jurisdiction*, U.S. SENATE COMMITTEE ON THE JUDICIARY, https://www.judiciary.senate.gov/about/jurisdiction [https://perma.cc/85HY-D5F6] (same). See also OpenSecrets discussing funding patterns for House and Senate Judiciary Committees noting that, while lawyers make hefty donations to committee members who have jurisdiction over their courtrooms, the business interests care about "bankruptcy, immigration, and copyright and antitrust law," *House Judiciary Committee*, OPENSECRETS.ORG, https://www.opensecrets.org/cong-

long-term members had developed relationships with the industries and agencies they regulate in that context, particularly the content community that was heavily invested in the bill.[194]

Second, the lack of trusted technical experts or independent expertise on staff may have led the Committee to discount these concerns. Prior to 1995, when the Office of Technology Assessment (OTA) was defunded during the so-called Gingrich revolution, OTA would have provided such nonpartisan advice on technical subjects.[195] OTA's role was to ensure that sound scientific insight from the sciences guided Congressional policy choices. OTA's reports, however, were technical and by design omitted policy recommendations.[196] The cross-cutting nature of technology made OTA's assessments a vehicle for identifying and considering the equities that spanned multiple committees. OTA expert panels included diverse stakeholders and because recommendations were not made, there was no need or expectation to reach consensus on policy choices.[197] Despite its efforts to provide balanced, non-partisan advice to Congress, OTA was defunded after twenty-three years in part due to the perception that it favored liberal policies.[198]

Finally, Congress's lack of initial receptivity to advice from technical experts may have resulted from the company those experts kept. The technical experts were initially brought into the policy debate by two advocacy

---

cmtes/overview?cmte=HJUD&cmtename=House+Judiciary+Committee&cong=115 [https://perma.cc/GZ22-PYSY], and on the Senate side noting that "financial, computer, telecommunications, and entertainment industries all give generously because of the committee's jurisdiction over issues like bankruptcy, immigration, copyright, and antitrust," *Senate Judiciary Committee*, OPENSECRETS.ORG, https://www.opensecrets.org/cong-cmtes/overview?cmte=SJUD&cmtename=Senate+Judiciary+Committee&cong=115 [https://perma.cc/W7DN-MDH4].

194. Zach Carter, *SOPA: Washington vs. the Web*, HUFFINGTON POST (Dec. 14, 2011), https://www.huffingtonpost.com/2011/12/14/sopa-protect-ip_n_1140180.html [https://perma.cc/CQ2B-E7SN] (discussing ties between Judiciary Committee members, staffers, and intellectual property rights holder organizations); *see also* T.C. Sottek, *Meet Lamar Smith: SOPA Author, Climate Change Skeptic, and Congress' Next Science Boss*, VERGE (Dec. 5, 2012), https://www.theverge.com/2012/12/5/3725768/meet-lamar-smith [https://perma.cc/M5YR-YUDK] (describing the revolving door between the entertainment industry and its lobbyists and the Judiciary Committees in the context of SOPA); Grant Gross, *Former Congressional Staffers Lobby for Copyright Bills*, CIO (Dec. 14, 2011, 7:00 AM), https://www.cio.com/article/2401258/internet/former-congressional-staffers-lobby-for-copyright-bills.html [https://perma.cc/H9WT-ZX9E] (same).

195. GENEVIEVE J. KNEZO, CONG. RESEARCH SERV., RS21586, TECHNOLOGY ASSESSMENT IN CONGRESS: HISTORY AND LEGISLATIVE OPTIONS 1 (2005), https://fas.org/sgp/crs/misc/RS21586.pdf [https://perma.cc/V52T-UJP6].

196. Jathan Sadowski, *Office of Technology Assessment: History, Implementation, and Participatory Critique*, 42 TECH. IN SOC'Y 9, 16 (2015) (describing OTA's habit of providing a "suite of different policy options decision-makers could take into account" and how this "annoyed members of Congress who wanted flat out answers, or at least straightforward advice").

197. *Id.* (discussing that the emphasis on "'just the facts' . . . was a deliberate choice that was intended to help OTA escape accusations of partisanship by relying on an aura of neutrality and scientific objectivity").

198. *Id.* at 15–16.

organizations, EFF and CDT. Those two organizations play an important role in legislative debates that pit expanded intellectual property protection against privacy, freedom of expression, and cybersecurity, among other values, routinely raising concerns about policies advocated by the content industries[199]—and are perceived as more typically aligned with Democratic policy priorities.[200]

Still, the DNS issue ultimately resurfaced and contributed to SOPA's defeat.[201] The values arguments remained largely the same, but a marked shift in messengers, along with growing and unprecedented grassroots activity, influenced Congress. Noted Republicans with credentials on national security, such as Stewart Baker and the conservative Heritage Foundation,[202] along with institutions like the national labs, spoke out against the DNS provisions, picking up the security and fragmentation concerns of the technologists. Tea Party Republican grassroots organizations added their own spin on the DNS provisions, painting them as a big government regulation grab by the Department of Justice and then-Attorney General Eric Holder.[203]

Finally, Republicans were attracted to opposing SOPA because it forced Democrats to choose between the technology sector and Hollywood, creating new fundraising inroads for the GOP in Silicon Valley.[204] When the Senate vote was scheduled, Judiciary Committee Republicans demanded that DNSSEC be dropped.[205]

D. Case 4: The Electronic Voting Debacle

Lacking the technical expertise to translate legislation into code, Congress, in our fourth illustration of governance-by-design dysfunction, delegated the

199. *See Annual Reports and Financial Information*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about/annual-reports-and-financials [https://perma.cc/C2EA-QQ5T] (documenting ongoing involvement in intellectual property policy related to the Internet); Andrew McDiarmid & David Sohn, *Bring in the Nerds: The Importance of Technical Experts in Defeating SOPA and PIPA*, *in* HACKING POLITICS: HOW GEEKS, PROGRESSIVES, THE TEA PARTY, GAMERS, ANARCHISTS AND SUITS TEAMED UP TO DEFEAT SOPA AND SAVE THE INTERNET (David Moon, Patrick Ruffini & David Segal eds., 2013) (describing CDT's role in debates around SOPA, PIPA, and precursors).

200. McDiarmid & Sohn, *supra* note 199 (describing CDT and EFF's role in bringing technologists into the debate).

201. *Id.*

202. Dan Kaminsky & Stewart Baker, *CISPA Isn't 'Son of SOPA,'* POLITICO (Apr. 24, 2012, 9:50 PM), https://www.politico.com/story/2012/04/cispa-isnt-son-of-sopa-075546 [https://perma.cc/T6VA-RLZM].

203. Erick Erickson, *Stopping SOPA*, REDSTATE (Dec. 22, 2011, 8:50 PM), https://www.redstate.com/erick/2011/12/22/stopping-sopa [https://perma.cc/AXH2-BVVW] ("The way the Act [SOPA] goes about doing this is, in large part, allowing Eric Holder to take control of the internet and shut down websites he does not like.").

204. *See* Baker, *supra* note 180 (explaining how opposition to intellectual property enforcement might be a "political winner" for Republicans since it "drives a wedge between two Democratic constituencies, Hollywood and Silicon Valley").

205. *See Smith to Remove DNS Blocking from SOPA*, HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE (Jan. 13, 2012), https://judiciary.house.gov/press-release/smithtoremovednsblockingfromsopa [https://perma.cc/9WM2-2372].

implementation of electronic voting systems to private vendors through the Help America Vote Act of 2002 (HAVA). Despite public input into the legislative process, a lack of public input and oversight of the technological translation of the statute subverted public values (and wasted money).

Congress passed HAVA[206] to accelerate the transition to electronic voting in response to the voting problems in the 2000 presidential election. HAVA established six requirements for electronic and other voting systems used in federal elections, including that the voter must be able to confirm their ballot is correct before casting their vote,[207] and the voting system must have a manual audit capability with a permanent paper record.[208] It also established the U.S. Election Assistance Commission to establish a testing and verification process for certifying voting equipment that complied with these new standards.[209]

The testing and certification process made vendors largely responsible for translating HAVA regulations into technical requirements, delegating them to private company engineers and certification labs.[210] This delegation reduced the ability of regulators and other stakeholders to participate and oversee the process of embedding these requirements into technical systems.

Yet, while statutory construction is a subject with a long history of jurisprudential and scholarly analysis,[211] the translation of legislative and regulatory text to technical requirements is an active field of research without settled practices.[212] When contracted engineers are forced to turn nuanced issues of law into machine logic and process, they often make decisions with implications for policy, not just implementation. This privatizes some of the public values choices that administrative and constitutional law seeks to keep in government's hands. For example, HAVA's manual auditing requirement does not list a set of criteria for or definition of what constitutes a "permanent paper record"[213] or "manual audit capacity."[214] One could reasonably conclude that the

206. Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (2002) (codified in scattered sections of 42 U.S.C.)

207. *Id.* § 301(a)(1)(A).

208. *Id.* § 301(a)(2).

209. 42 U.S.C. § 15321 (2012).

210. David L. Dill, Bruce Schneier & Barbara Simons, *Voting and Technology: Who Gets to Count Your Vote?*, 46 COMM. ACM 29 (2003); *Voting System Test Laboratories*, U.S. ELECTION ADMIN. COMMISSION, https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl [https://perma.cc/Q3JK-RATE].

211. *See, e.g.*, *Sutherland Statutes and Statutory Construction*, YALE L. SCH. LILLIAN GOLDMAN L. LIBR., https://library.law.yale.edu/sutherland-statutes-and-statutory-construction [https://perma.cc/K2H2-R9HC] (noting that the "definitive" Sutherland treatise still in use today (in updated form) was first published over one hundred years ago).

212. *See* Nadzeya Kiyavitskaya, Alžběta Krausová & Nicola Zannone, *Why Eliciting and Managing Legal Requirements Is Hard*, PROCEEDINGS OF THE 2008 REQUIREMENTS ENGINEERING AND LAW 26 (2008).

213. Help America Vote Act of 2002, Pub. L. No. 107-252, § 301(a)(2), 116 Stat. 1666 (2002) (codified in scattered sections of 42 U.S.C.).

214. *Id.*

terms "permanent" and "paper" indicate that the record must be fixed, durable, and not instantiated in a re-writable medium, such as common digital storage. Instead, the voting system manufacturers seemed to be designing the systems to eliminate paper records as much as possible. They attempted to satisfy the permanent paper record requirement by simply providing the ability to print out the vote tallies at the end of the day, effectively doing away with the connection between the fixed voter-verified ballot and auditing.[215] Since the printout was not what the voter cast, a specific voters ballot could be altered, creating opportunities for vote-buying and coercion.[216]

This breakdown is not surprising, given the lack of public involvement and oversight over the translation of requirements in technology design. The technological systems produced were subject to certification by third parties, but they were not opened up to the sort of wide public review that an administrative rulemaking would receive.[217] Both the translation process and the translations themselves became black boxes.[218]

The handoff from legal mandate to electronic systems proved to be a costly failure. The systems were not designed to allow easy redesign, so it was difficult to retrofit them to produce the Voter Verified Paper Record that became the standard for ensuring election auditability on electronic systems.[219] Many jurisdictions used their HAVA money to purchase machines that now sit in

215. Rebecca Mercuri, *A Better Ballot Box?*, 39 IEEE SPECTRUM 46, 46 (2002) (discussing the reliance on the system to audit itself and stating, "[t]here will simply be no way to ever know, because the new equipment does not make an independent recount possible.").

216. *Russian Interference in the 2016 U.S. Elections: Hearing Before the Select Comm. on Intelligence of the United States Senate*, 115th Cong. 72–80 (2017) (statement of J. Alex Halderman, Professor of Computer Science, University of Michigan, describing vulnerabilities created by lack of a voter-verified paper trail).

217. For an overview of the legislative process around HAVA and decision to withhold regulatory authority from the Election Administration Commission and rely on guidance and voluntary standards see, Candice Hoke, *Voting Technology and the Quest for Trustworthy Elections*, *in* AMERICA VOTES! A GUIDE TO MODERN ELECTIONS LAW AND VOTING RIGHTS 321, 328–33 (Benjamin E. Griffith ed., 2d ed. 2012).

218. *Id.* at 330.

219. *See* LAWRENCE NORDEN, LAURA SEAGO, SUSANNAH GOODMAN, SEAN FLAHERTY & PAMELA SMITH, IS AMERICA READY TO VOTE? STATE PREPARATIONS FOR VOTING MACHINE PROBLEMS IN 2008, at 11 (2008), http://www.commoncause.org/research-reports/National_101708_Report_Voting_Machine_Preparedness.pdf [https://perma.cc/5LES-WBKK] ("Thirty-two states currently have either voter-verifiable paper ballots, or have added voter-verifiable paper record printers to voting machines statewide. Another four states (Maryland, New Jersey, New York and Tennessee) have passed laws to require voter-verifiable paper ballots or records, which take effect in 2009 or 2010. Three states—Arkansas, Colorado and Mississippi—have paper in most counties. The District of Columbia and Florida have paper ballot systems in all counties, along with paperless DREs, and Florida will eliminate paperless systems altogether by 2012."); Daniel Root & Liz Kennedy, *9 Solutions to Secure America's Elections*, CTR. FOR AM. PROGRESS (Aug. 16, 2017), https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections [https://perma.cc/38UP-XJCE] (discussing ways to address threats to elections, specifically, "[s]tates and counties using paperless touch-screen voting systems should replace them with paper ballots and optical scanners, or invest in electronic voting machines that produce voter-verified paper records").

warehouses and have had to buy new machines.[220] Allowing vendors to engage in the translation work without public oversight placed them in an uncomfortable position of being given inadequate guidance, and then being blamed for faulty machines and limited public oversight over the fitness of voting systems.[221]

Federal and state agencies failed to exert adequate influence over the design of the technology, and trade secrecy and vendor contracts further constrained the public participation, transparency, and publicness that is viewed as integral to legitimate governance.[222] The move to electronic voting systems also makes visible the ways in which traditional approaches to values decisions—by which public bodies without access to technological expertise deliberate ex ante over competing norms—can fail. When lawmakers unfamiliar with the technology-based statutes assigned the implementation of public value choices to private technology contractors, design choices prioritized efficiency over accountability, subverting public values. Although a range of democratic values were explicitly debated and articulated during the legislative process, that public process did not address the ways that those values were to be embedded into technological design. Instead, private vendors were left to make important decisions with policy implications and embedded those decisions in electronic voting machines, undermining other values, including the integrity of elections.

E. Learning From the Cases: The Threat of Governance-by-Design Dystopia

These four recent technology battles underscore how policy is increasingly made through design war—and the inadequacy of existing modes of public governance to address that trend. This accelerating development subverts fundamental norms of intentional, deliberative, participatory, and expert public

220. For example, after the *Top-to-Bottom Review of Voting Systems*, California decertified several direct record electronic voting systems and recertified them "solely for the purposes of conducting early voting and to allow counties to have one DRE machine in each polling place on Election Day for the purpose of complying with disability access requirements of the Help America Vote Act (HAVA)." Debra Bowen, *California Decertifies Voting Machines, Conditions Applied for Use*, GOV'T TECH. (Aug. 6, 2007), http://www.govtech.com/templates/gov_print_article?id=99379169 [https://perma.cc/8CPT-9LKR]. And see earlier decertification of "14,000 electronic voting machines made by Diebold Inc. in the November election because of security and reliability concerns" by then-Secretary of State Kevin Shelley. John Schwartz, *High-Tech Voting System Is Banned in California*, N.Y. TIMES (May 1, 2004), http://www.nytimes.com/2004/05/01/us/high-tech-voting-system-is-banned-in-california.html [https://perma.cc/77VC-W2GW].

221. *See* Joseph Lorenzo Hall, *Contractual Barriers to Transparency in Electronic Voting*, PROCEEDINGS OF THE 2007 USENIX/ACCURATE ELECTRONIC VOTING TECHNOLOGY WORKSHOP (2007), https://www.usenix.org/legacy/event/evt07/tech/full_papers/hall/hall_html/jhall_evt07_html.html [https://perma.cc/GUY2-HY4X] (discussing the use of contracts to limit public oversight); Doris Estelle Long, *Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?*, 23 J. COMPUTER & INFO. L. 533 (2005) (discussing one voting systems company's knowledge of faults in its system and attempt to suppress knowledge of them in discussing Online Policy Group (OPG) v. Diebold 337 F. Supp. 2d 1195 (N.D. Cal. 2004)).

222. Hall, *supra* note 221; Hoke, *supra* note 217.

decisionmaking that is free from capture or caprice. Specifically, these four battles underscore four fundamental dysfunctions that pose the threat of governance-by-design dystopia.

1. Governance-by-design overreaches by using overbroad technological fixes that lack the flexibility to balance equities and adapt to changing circumstances—with unintended, irrational, and long-term consequences

Governance-by-design is plagued by overconfidence, and its technological fixes—to borrow an image from First Amendment Law—by overbreadth. When using technology to regulate, the rule-of-law instinct is towards developing a comprehensive, defined, ex ante, body of regulatory mandates—an instinct that resonates in some ways with technology's deceptive promise of complete, unerring, perfectly-manipulated control. SOPA's drafters identified a bold way to "force" the worldwide protection of intellectual property rights at the risk of "break[ing] the Internet."[223] The FBI, meanwhile, sought access to a unique iPhone in a single investigation, yet in a wide-reaching fashion that would compromise the security of millions of devices across the globe.

This failure to "narrowly tailor" regulatory measures threatens enduring—and often opaque—dangers when using technological fixes, which often lack the flexibility to balance equities, to adapt to changing circumstances, and to enable democratic participation. As the voting machine debacle reveals, errors and unintended consequences result. And as the successful Privacy-by-Design movement demonstrates, the instinct to settle policy broadly and decisively through design produces unforeseen casualties, as the technology sweeps far wider than a text interpreted by substantive experts through deliberative or adversary processes might. Such distortions and irrational outcomes, in turn, are "sticky" and difficult to remedy.

2. Governance-by-design privileges singular values at the expense of all others, especially human rights

Second, governance-by-design often privileges one or a few values, excluding other important ones, particularly broad human rights. By its nature, governance-by-design involves competing values, and powerful parties will attempt to technologically embed their preferred values. The FBI argued law enforcement should trump all other values, SOPA was designed to value intellectual property rights above all others, and privacy-by-design reflected a similar singular substantive focus.

223. Joel Hruska, *How SOPA Could Actually Break the Internet*, EXTREMETECH (Dec. 19, 2011), https://www.extremetech.com/computing/109533-how-sopa-could-actually-break-the-internet [https://perma.cc/QG5H-LCFN].

These dysfunctional outcomes—overbroad solutions that privilege singular values, often disfavor human rights, and produce distortions and irrational effects that are hard to discern and sometimes even harder to remedy—further reflect two failures of decisionmaking processes, reflected in the third and fourth insights suggested by our four examples.

3. Regulators engaged in governance-by-design lack the proper tools

Administrative agencies, legislatures, and courts are poorly designed, in terms of structure, accountability mechanisms, and expertise, to take into account the implications of technology design. Their jurisdiction is intentionally circumscribed and their focus purposefully siloed, whether by limits on their substantive ambit, the specificity of their delegated authority, or by constitutional case-and-controversy requirements. Even when explicitly directed to take account of issues outside their substantive focus, these governance bodies often lack the ability and incentives to do so—a phenomenon heightened by lack of expertise about technology and the trans-substantive implications of its design.

The SOPA battles reveal these shortcomings of legislatures as venues for technology design debates. Legislative process may be skewed in favor of motivated and powerful interest groups. Committees may work at cross-purposes, and they often lack or exclude the technical expertise required to understand the implications of their decisions.

Administrative agencies called upon to translate values into design, moreover, are generally poor sites, practically and constitutionally, for the weighing of a broad range of norms. Their policymaking authority is often narrowly circumscribed by the substantive concerns assigned to them by statute. Even when they are empowered to address a range of competing values, they may lack the incentives and expertise to do so. They may suffer from regulatory capture that steers their policymaking in one direction. And, like Congress, agencies are also limited by the substantive limits of their professional staff, particularly their inexperience with technology.

Finally, the case-by-case approach of courts, exemplified by the Apple v. FBI litigation, severely handicaps their ability to deal with the wide range of competing values implicated by design tinkering. While amicus briefs afford nonparties an opportunity to broaden a court's understanding of a case, at the end of the day, a court must rule on the facts before it. And courts are neither designed nor equipped to make judgments on precise technological questions with broad policy implications.

The kinds of expertise present and absent in principals and professional staff at these institutions further limits regulatory competence. Except in agencies or courts with a technical focus (such as the National Highway Traffic Safety Administration, the U.S. Court of Appeals for the Federal Circuit, or legislative committees focused on science), the staff often lacks design and engineering expertise entirely. Lawyers are the dominant principals across all

three institutions, and lawyerly ways of constructing and remedying problems generally dominate. As we saw in the SOPA story, the absence of staff with engineering expertise and the lack of external, trusted technology advisors may have led Congress to downplay the risks of mucking with the Domain Name System. The encryption debates highlight how gaps in understanding and perspective that result from different forms of expertise can hinder sound approaches to regulating through technology. Law enforcement circles (dominated by lawyers) believe that encryption back doors can be designed to mimic law's specificity and control overuse, while the security community (dominated by engineers) asserts this is both theoretically wrong and, even if true in theory, practically impossible.[224]

4. Governance-by-design decisions are often made in private venues or in processes that make technological choices appear inevitable and apolitical.

Public power is too often exercised in private, by private parties, or without nonpartisan or nonpolitical sources of expertise. The substance and political nature of choices fixed by technology is thus obscured, which enfeebles citizen awareness and involvement, diminishes ex post accountability, and yields unintended outcomes.

All four cases cited showcase elements of this problem. Just as the FBI attempted to resolve the encryption issue in their favor through private negotiations with Apple, through a private ex parte court order, and through hacking the phone, Apple made a private decision to bake in privacy controls to protect customers and markets. In the SOPA example, copyright holders (through lobbyists and campaign contributions) influenced narrowly focused Congressional committees to consider fundamental changes to Internet architecture in ways, at least initially, that precluded broader public participation. With core democratic values at stake, implementation of electronic voting was nonetheless delegated to private contractors. Privacy-by-design advocates too have used their influence among legislators and administrative agencies to restrict broader public consideration of competing values.

Unfortunately, the traditional policymaking processes for safeguarding transparency, participation, and rational decisionmaking actually subvert those values when governing by design. Providing a veneer of public process, they mask the political and policymaking choices involved in exercising control through technical requirements, standards, and artifacts. They forfeit those

224. *See* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69 (2015); WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (2007); SUSAN LANDAU, LISTENING IN: CYBERSECURITY IN AN INSECURE AGE (2017); *see also* Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, 2 WORLD WIDE WEB J. 241 (1997) (noting an older but evergreen discussion).

decisions to companies, standard-setting bodies, and programmers, and surrender policy choices to private metrics.

As demonstrated in the case of electronic voting machines, leaving the design of technologies that play a role in public governance to private actors like regulated parties or programmers—those with the greatest combination of incentives and technical expertise—risks privileging those stakeholders and their values. Even if a regulatory agency has set goals at a high level through public processes, the private sector has the capacity and motivation to employ (often proprietary and nonpublic) technology to implement and enforce regulation in a way that obscures the specifics of design implementation, the choices made, and even the fact that policy choices are occurring. Regulatory oversight of translation from rule to code can be hampered by contracts[225] and intellectual property law,[226] in addition to lack of technological expertise. Even when public entities then try to regulate, the horse has often already left the stable: many of the key policy choices have already been made.

III.
SAVING "GOVERNANCE-BY-DESIGN": RULES OF ENGAGEMENT FOR PREVENTING GOVERNANCE DYSTOPIA

Saving governance-by-design requires new rules of engagement. The cases explored in Section III highlight four dysfunctions that undermine democratic processes and values and threaten governance dystopia. Continued reliance on the status quo without revisiting the process through which design decisions are used to make policy constitutes willful disengagement from this subversion of norms. To address this challenge, we propose a new institutional, technological, and conceptual framework for when and how we should use design to protect values.

This framework involves four proposed rules of engagement that address each of the dysfunctions highlighted by the design battles discussed in Section III. They also put forth concrete examples, where available, that begin to model the approaches we suggest.

1. Design with Modesty and Restraint to Preserve Flexibility
2. Privilege Human and Public Rights
3. Ensure Regulators Possess the Right Tools: Broad Authority and Competence, and Technical Expertise
4. Maintain the Publicness of Policymaking

---

225. Hall, *supra* note 221.

226. AARON BURSTEIN, STEPHEN DANG, GALEN HANCOCK & JACK LERNER, LEGAL ISSUES FACING ELECTION OFFICIALS IN AN ELECTRONIC-VOTING WORLD (2007), https://www.law.berkeley.edu/files/Legal_Issues_Facing_Election_Officials.pdf [https://perma.cc/7DKX-JPG8]; David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135 (2007).

A. First Rule of Engagement: Design with Modesty and Restraint to Preserve Flexibility

To prevent the sort of overreaching that has characterized efforts to regulate through technology, governance-by-design initiatives must be narrowly tailored. Applied to the design context, this means that such efforts must be guided by engineering and design principles that emphasize modesty, restraint, and extensibility in order to preserve flexibility. Approaching technological means of governance with modesty and restraint, and creating explicit mechanisms for reviewing and revising decisions, can preserve the flexibility to adapt to social and technological changes and fine-tune the alignment among competing values.

Designing with modesty and flexibility would have avoided numerous outcomes that characterized our case studies: SOPA's threatened change to fundamental rules guiding the global Internet; the unintended consequences of privacy-by-design for civil rights goals; and in the voting machine skirmish, inflexible technologies that failed to accommodate the changes required to protect the integrity and fairness of the voting process.

Indeed, because "choices tend to become strongly fixed in material equipment, economic investment, and social habit," technologist Langdon Winner explained, technology's original flexibility can "[vanish] for all practical purposes once the initial commitments are made."[227] In that sense, technological choices can be "similar to legislative acts or political foundings that establish a framework for public order that will endure over many generations."[228] While the plasticity of code is oft-touted, code in fact can be extremely difficult to alter once it becomes hardened into the technology infrastructure.[229] The technology often becomes embedded in organizations and social structures, and in the practices of a culture, community, or profession and then fades into the background.[230] Entrenchment can overrule plasticity.

Regulation through technology, then, should generally embody values only to the extent necessary, and in ways that maximize reconsideration, flexibility, and generativity. This avoids problems of spillovers, durability, and the need to retrofit or redesign wholesale. Regulation must be designed to accommodate other values and adapt as more information is learned. Such a mindset asks regulators to approach design as designers do. It must be "an iterative process whereby technologies are invented and then redesigned based on user

227. Winner, *supra* note 29, at 127–28.
228. *Id.* at 128.
229. *See* Clark, *supra* note 80, at 465–66.
230. *See* Susan Leigh Star & Karen Ruhleder, *Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces*, 7 INFO. SYSTEMS RES. 111 (1996).

interactions, which then are reintroduced to users, further interactions occur, and further redesigns implemented."[231]

This principle resonates with general jurisprudential caution when regulating in uncertain contexts.[232] It is supported by a growing body of empirical and analytical research in the literature on regulation, which demonstrates that "specific rules often cannot reflect the large number of variables involved in achieving multifaceted regulatory goals," and that "uniform, static, approaches to regulation are particularly inapt to contexts characterized by rapid changes in technology and market infrastructure."[233] A call to "leav[e] things undecided"[234] also reflects layers of doctrine suggesting restraint and flexibility in contexts where decisions are constitutive of background structure, as in constitutional jurisprudence.

The principle of modesty-in-design also reflects important trends in engineering. An extensive design literature, fully embracing Kranzberg's law that "[t]echnology is neither good nor bad; nor is it neutral,"[235] has articulated values to guide engineers, particularly those involved in technical standards work. Early examples of this literature emphasized, in Rawlsian fashion, a thin set of values. Those examples argued for engineers to exercise self-restraint with respect to values, in deference to questions of legitimacy. Scholars, reluctant to set rules and determine substantive outcomes, argued that designers should acknowledge and facilitate "tussle"—allowing stakeholders to battle over policy outcomes rather than settling them through technical design—within the technical landscape and seek to limit the externalities or spillovers from such value disputes. This perspective on where values disputes should be resolved—by legal and social processes, not technical choices—led engineers to argue for a set of principles that would support variation in values outcomes; compartmentalize values tussles to avoid disrupting other aspects of the technical system; and facilitate informed choices about values by different stakeholders

231. Batya Friedman & Alan Borning, *Value Sensitive Design as a Pattern: Examples from Informed Consent in Web Browsers and from Urban Simulation*, PROCEEDINGS OF THE DIRECTIONS & IMPLICATIONS OF ADVANCED COMPUTING SYMPOSIUM 109, 110 (2002) [hereinafter Friedman & Borning, *Value Sensitive Design as a Pattern*].

232. *See generally* STEPHEN BREYER, REGULATION AND ITS REFORM 184 (1982) ("[*M*]*odesty* is desirable in one's approach to regulation.").

233. Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477, 479–80 (2011); *see also* Bamberger, *Regulation as Delegation*, *supra* note 20, at 387–88 ("[W]hen regulators attempt to reflect the breadth of uncertain contextual factors in a regime of precise provisions, the proliferation of rules itself creates an unwieldy, confusing body of mandates and exceptions leading to uncertain and inconsistent application.").

234. Cass R. Sunstein, *The Supreme Court 1995 Term Foreword: Leaving Things Undecided*, 110 HARV. L. REV. 4 (1996).

235. Melvin Kranzberg, *Technology and History: "Kranzberg's Laws,"* 27 TECH. & CULTURE 544, 545 (1986).

through transparency about rules and data flows and mechanisms to handle end-user decisions.[236]

In the context of governance-by-design, these approaches call for three decisional principles:

> *First*, when a value remains fundamentally contested, or the implications of designing for one value on other important values appear uncertain, it weighs *against* a decision to regulate comprehensively by technological means. This bias does not preclude regulation by technology but suggests caution about where to position the intervention. In this respect, the failure of the SOPA legislation, which threatened the security of the backbone of the Internet, was a desirable outcome.
>
> *Second*, in a contested context, if the decision is made to enlist technology to regulate, efforts should be made to design systems that "enable" values—that is, systems with defaults that support alternate end states—rather than "baking them [in]" as part of the fundamental system architecture (i.e., forcing certain behaviors while making the choices invisible).[237] Technologies that support end user control over content on the Web are an example of such technology. While not mandated by government, two technologies have provided a less restrictive means for addressing indecent content on the Web and limited the government's ability to adopt more heavy-handed regulations: filtering software and the Platform for Internet Content Selection (PICS) mechanism.[238] The PICS mechanism allowed websites to communicate machine-readable information about site content, which permitted browsers to make access decisions on behalf of users. The PICS specification did not engage in content description or filtering itself, but instead, performed the "lighter" regulatory function of creating a mechanism that others—in competition and contest—could use to label, describe, and rate content on the Web. In the language of traditional governance, it performed "informational regulation," rather than "coercive regulation."[239] The specification allowed for ongoing debates about what was, or was not, appropriate for minors and also provided a technical system for actualizing the results of those

236. Clark, *supra* note 80.

237. *See* Corinne Cath & Luciano Floridi, *The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights*, 23 SCI. & ENGINEERING ETHICS 449, 461–65 (2017) (arguing that "IETF should opt for an approach that enables human rights *through* protocols over designing them *in* protocols").

238. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997) (holding unconstitutional two provisions of the Communications Decency Act of 1996 (CDA) that criminalized providing indecent materials to minors by on the internet on grounds that it violated the First Amendment because technical measures available to parents and families provided a less restrictive means).

239. *See* Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613 (1999).

> debates.[240] It thus provided "technical *hooks* for the expression of policies or requirements"[241] but did not embed value outcomes in the technological system itself.
>
> *Finally*, if the decision is made specifically to embed certain values, technology should be designed according to engineering principles that permit flexibility and facilitate evolution, including extensibility, abstraction, and modularity.

Extensibility refers to the ability to add new functionalities to a system with minimal effects on its internal structure and data flow. Recognizing that not everything can be designed in advance, an extensible application is not limited to the methods, protocols, or content considered at design time.[242] Extensible design "provides a light framework which can allow for changes" and additions "made in small, incremental steps."[243] A paradigmatic example is the design of the Standard Template Library (STL), a software library for the C++ programming language. STL separates what it calls "containers" from the algorithms it uses and provides a mechanism that allows new algorithms to be added later.[244]

---

240. Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, WORLD WIDE WEB CONSORTIUM (1996), https://www.w3.org/PICS/iacwc.htm [https://perma.cc/XUQ9-BKMD] (updated in 39 COMM. ACM 87). The authors explain how:

> [t]he separation of selection software from rating services will enable both markets to flourish. Software companies and on-line services that prefer to remain value-neutral can offer selection software without providing any rating labels; values-oriented organizations can offer labels, even if they lack the expertise to write selection software. Labels may come from many sources. . . . With multiple perspectives to choose from, parents and other supervisors can choose labeling sources that reflect their goals and values, and ignore all other labels.

Id.

241. Nick Doty & Deirdre K. Mulligan, *The Importance of Privacy Hooks for Advanced Web APIs*, W3C WORKSHOP ON PRIVACY FOR ADVANCED WEB APIS (2010), https://npdoty.name/papers/privacyhooks.txt [https://perma.cc/TS4A-VD2Z] (emphasis added). The authors also emphasize that:

> [t]hough not self-enforcing, expressions of policy transmitted via an API can fulfill a valuable forcing function in making web site developers consider, express and accept statements of privacy policy. While Web standards and privacy hooks cannot alone ensure user privacy on the Web, they can support privacy by enabling both legal enforcement and market competition.

Id.

242. *See* Niklas Johansson & Anton Löfgren, *Designing for Extensibility: An Action Research Study of Maximizing Extensibility by Means of Design Principles* 3 (Univ. of Gothenburg Dep't of Applied Info. Tech., Working Paper No. 053, 2009), https://gupea.ub.gu.se/bitstream/2077/20561/1/gupea_2077_20561_1.pdf [https://perma.cc/45FE-MFST].

243. Allan Kelly, *The Philosophy of Extensible Software*, ACCU PROFESSIONALISM IN PROGRAMMING (2002), http://accu.org/index.php/journals/391 [https://perma.cc/A5ZY-QJJS].

244. *Id.*

The STL example further reflects the design values of "abstraction" and "modularity" (or "componentization").[245] These approaches isolate subcomponents or layers within an architecture, allowing pieces of applications to be built independently of one another and to evolve with greater ease. A web server that collects user data, applies business rules, formats the results, and then returns them to a browser represents an example of such an approach. The server permits changes in business rules by abstracting the rules from the rest of the application. If it were not designed in this fashion, the rules could not be changed.[246]

The activities of the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) further provide examples of modesty and restraint in action and of the flexibility they produce. The WC3 is the international organization that sets standards for the World Wide Web,[247] and IETF is the "open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet."[248] Most of WC3's and IETF's standards are not directed toward regulating through technology. Yet when they build systems specifically to support values, those systems tend to enable the expression of values, assertions of values, and choices about values.[249] In short, they build technological venues that can accommodate "tussles."[250] While some core architectural choices seem well aligned with human values, the aim has been to provide a playing field rather than to join a team or pick a winner. Thus, packet agnosticism and user empowerment—principles that have support in the technical community as described above— tend to support the underdog: the new entrant, the competitor, the citizen, activist, or whistle blower. But in general, the goal of WC3's and IETF's standards has been to maintain a capacity to support wildly different applications and values configurations. This flexibility, supported by modesty, restraint, as well as modularity and extensibility, is considered essential to the ongoing generativity of the Internet and the Web.[251]

The decision to support different values outcomes, rather than more sharply define and protect rights, has drawn objection from different quarters in different

245. For a description of these terms and their importance in design, see David G. Messerschmitt, *Rethinking Components: From Hardware and Software to Systems*, 95 PROCEEDINGS OF THE IEEE 1473, 1474–76 (2007).

246. Chris Armbruster, *Design for Evolution*, http://chrisarmbruster.com/documents/design-for-evolution-white-paper.pdf [https://perma.cc/3FTG-UA2T].

247. *About W3C*, W3C, https://www.w3.org/Consortium [https://perma.cc/BY8S-V6PP].

248. *About the IETF*, INTERNET ENGINEERING TASK FORCE, https://www.ietf.org/about [https://perma.cc/PLP4-FT95].

249. See Doty & Mulligan, *supra* note 68.

250. Clark, *supra* note 80, at 465.

251. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 67–101 (2008).

instances.[252] Yet, the standard-setting bodies have mostly held fast to playing an enabling role by providing language in which to articulate, negotiate, assert and agree about rights, while not determining those rights' exact contours, or taking full responsibility for their protection.[253]

Building on standards, products can and do offer clearer value propositions. They generally make additional choices that clarify how values interact and the extent to which they are protected. For example, P3P[254] is a W3C protocol that allows websites to declare the intended use of information they collect about web browser users. The protocol was employed by several browsers, but implemented in different ways. Some browsers protected privacy more than others due to the specifics of the implementation, including configuration, defaults, and controls offered to end users.[255]

Similarly, Apple's encryption standards are only one component of the overall cryptographic implementation that protects data. These standards determined the level of debate in the Apple v. FBI case; the government's strategy was accordingly directed towards defeating a password feature, not breaking the cryptography itself.[256] Other companies implement cryptography differently to protect communication, but they generally use a shared set of common standards.[257]

Finally, where Congress adopts a regulation employing a technological approach, it should be carefully and narrowly prescribed. In CALEA, for example, Congress decided that only "telecommunications carriers" would be obligated to make sure that their "equipment, facilities, or services" allow the government to intercept communications pursuant to a court order or other lawful authorization.[258] It did not mandate a particular design and precluded law enforcement from doing so.[259] While CALEA creates a process for the FCC to

252. *See, e.g.*, Doty & Mulligan, *supra* note 68, at 149–54.

253. *See* Cath & Floridi, *supra* note 237, at 453, 458 ("IETF has developed a strategy of responding to value-sensitive and human rights-by-design questions in technical terms" and describing how the IETF's work on privacy enables "a social value through protocols" but "do not instantiate" it, rather the technology enables "the actualisation of the right to privacy.").

254. *Platform for Privacy Preferences (P3P) Project*, W3C, https://www.w3.org/P3P [https://perma.cc/ZX6T-WVVU].

255. *P3P 1.0 Implementation Report*, WORLD WIDE WEB CONSORTIUM (Mar. 4, 2002), https://www.w3.org/P3P/implementation-report.html [https://perma.cc/HP5Q-26NR] (providing some sense of the divergent implementations supported by the specification and their implications for individual's ability to control the flow of personal information).

256. Mulligan & Bamberger, *supra* note 136.

257. Jason Cipriani, *What You Need to Know About Encryption on Your Phone*, CNET, (Mar. 10, 2016, 5:00 PM), https://www.cnet.com/news/iphone-android-encryption-fbi [https://perma.cc/YT83-ZHKL] (describing encryption as implemented on iPhone and Android devices).

258. 47 U.S.C. § 1002(a)(1) (2012).

259. *See id.* § 1002(b)(1).

This subchapter does not authorize any law enforcement agency or officer . . . to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by . . . any manufacturer of telecommunications equipment, or . . . to prohibit the adoption of any equipment, facility, service, or feature by . . . any manufacturer of telecommunications equipment . . . ."

extend the law's requirements to services that replace a substantial portion of local telephone exchange,[260] doing so requires a detailed public process.[261] This has not safeguarded competing values, but has ensured that the impact of techno-regulation on other substantive values is publicly recognized and debated.

Research on human factors in technology underscores the need to design for flexibility. Human interaction with technology is unpredictable,[262] suggesting that system designers should maintain ambiguity, rather than trying to get rid of it. Rather than forcing people to interact with systems in only one way, design should allow flexibility in how information is presented; recognize that design might have different meanings or uses in different contexts; and reflect ambiguity in what values the design may hold and how people would then relate to it.[263]

These approaches comport with Julie Cohen's articulation of a broad goal to design networks and information policies to support human flourishing—specifically, to "preserve room for play" in interactions with cultural resources, the formation and performance of identity, and the ongoing adaptation of networked places and artifacts.[264] To support this "room for play," Cohen calls for network architectures and policies that support access to knowledge, operational transparency through technical standards and artifacts and the processes of their production, and approaches with "semantic discontinuity."[265] Her call to design for semantic discontinuity is radical, intriguing, and important. She calls on us to resist the allure "toward seamless continuity" in pursuit of the "bad man" and argues that "the good person and . . . good society" only flourish in "conditions of (partial) unpredictability."[266]

Those seeking to regulate through technology should heed these insights. They should not simply replace wholesale one regulator—the law—with a second—technology. The properties of the two are distinct. Law provides for semantic discontinuity. It allows contradictory laws to exist and maintains the possibility for action inconsistent with both. Technology can preserve these traits

---

Id.

260. *Id.* §§ 1001(8)(B)(ii), 1002(a).

261. *See, e.g.*, In the Matter of Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 20 FCC Rcd. 14989 (2005), on reconsideration in part, 21 FCC Rcd. 5360 (2006) (showing how the government has used this procedure to obtain FCC authority to monitor VoIP and other internet-based communications).

262. Jennie Carroll, *Completing Design in Use: Closing the Appropriation Cycle*, ECIS 2004 PROCEEDINGS 44 (2004) (discussing user appropriation of information and communication technology "configuring or personalising it for their needs and using it for novel purposes" not imagined by designers).

263. William W. Gaver, Jacob Beaver & Steve Benford, *Ambiguity as a Resource for Design*, 5 PROCEEDINGS OF THE 2003 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 233 (2003).

264. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 224 (2012).

265. *Id.* at 266.

266. *Id.* at 241.

to some extent if care is taken in choosing how and where to regulate through technology. Technology, like law, comes in multiple forms (expressive, prescriptive, nudge-y, or controlling), and those forms provide different opportunities for negotiation, deviance, coexistence with other values, and evolution. Where technology is chosen as the modality of regulation, we must be keenly aware of its form and location in the ecosystem. Choosing carefully can avoid spillovers, maintain room for debate and dissent, allow for useful variation, and support generativity.

B. Second Rule of Engagement: Privilege Human and Public Rights

The second rule of engagement requires that governance-by-design must be guided by frameworks that prioritize among rights. Specifically, it requires decisions to design-in values to consider all the values at stake, and, reflecting the approach of most international institutions, insists that human and public rights come first.

As discussed below, this prioritization of rights is reflected in two ways. First, because of the strength and durability of a decision to govern by design, we should be more sanguine about "baking" human and public rights values into technology systems. Second, reflecting the norms of modesty in design prescribed by the first rule of engagement, policy makers should seek to steer the protection of rights and values to the least intrusive point of technical intervention. This involves designing systems that enable the promotion of values rather than fixing them in determinatively, by designing technological hooks that permit different value choices in different contexts.

Such a rule would have prevented the FBI (or Apple or the courts) from failing to consider the competing values at stake and cautions against broadly and decisively fixing law enforcement access to information through technology design at the expense of personal privacy. At the same time, it would prohibit privacy regulators from requiring technological fixes that preclude competing values, including nondiscrimination. Nor would legislators be able to alter the Internet's core architecture to eliminate challenges to copyright holders while failing to consider freedom of expression and other human rights, as Congress attempted to do in SOPA.

1. What to Prioritize: A Consensus Hierarchy of Individual Rights, Public Goods, and Economic Rights

The Internet design experience offers a starting point for thinking about how to prioritize different values. Despite ongoing disagreement around values, a consensus reflecting longstanding democratic judgment and ethical frameworks has arisen among and within individual countries. The consensus prioritizes individual human rights and establishes principles for interference with those that are derogable. It is reflected in both governmental commitments regarding technology use and scholarship on values in design—particularly, the

work of engineers wrestling with the inescapable values implications of their work.

More specifically, both of these "top down" and "bottom up" sources have approached consensus on a hierarchy, or typology, of values that can guide the prioritization of values when considering regulation through technology. They have distinguished, in order of priority, between individual rights, public goods, and economic rights. This typology provides a firm departure point for thinking about embedding values in technology.

Where governments have addressed the prioritization of legal rights in technical design and Internet architecture, they have expressed an ongoing commitment to the prioritization of human rights over economic interests. The OECD Principles for Internet Policymaking underscore the importance of human rights in Internet governance.[267] The Communiqué, which preceded the adoption of the principles, set the stage by "recogniz[ing] that the Internet allows people to give voice to their democratic aspirations, and any policymaking associated with it must promote openness and be grounded in respect for human rights and the rule of law."[268] The principles, adopted by the thirty-five OECD member countries[269] and Egypt as well as the OECD Business and Industry Advisory Committee and its Internet Technical Advisory Committee, tie the rights of individuals to broader societal interests. They emphasize the relationship between supporting the fundamental openness of the Internet and freedom of expression. The document highlights freedom of expression,[270] privacy,[271] and due process,[272] as well as the need to foster cooperation to promote Internet security.[273] It asks members to "[m]aximi[z]e individual empowerment,"

267. ORG. FOR ECON. CO-OPERATION & DEV., OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY MAKING 6 (2011), http://www.oecd.org/internet/ieconomy/49258588.pdf [https://perma.cc/X3TT-VGQU] (noting that Internet governance must be "designed to help preserve the fundamental openness of the Internet while concomitantly meeting certain public policy objectives").

268. ORG. FOR ECON. CO-OPERATION & DEV., COMMUNIQUÉ ON PRINCIPLES FOR INTERNET POLICY-MAKING 2 (2011), http://www.oecd.org/dataoecd/33/12/48387430.pdf [https://perma.cc/4AWH-UKSF].

269. The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. *List of OECD Member Countries—Ratification of the Convention on the OECD*, OECD, http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm [https://perma.cc/GN6Z-2XKK]. The Commission of the European Communities also participates in the work of the OECD. ORG. FOR ECON. CO-OPERATION & DEV., EUROPEAN COMMUNITY DEVELOPMENT ASSISTANCE COMMITTEE (DAC) PEER REVIEW 2 (2007), https://www.oecd.org/dac/peer-reviews/38965119.pdf [https://perma.cc/25MN-57VV].

270. OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY MAKING, *supra* note 267.

271. *Id.* at 8 ("Strengthen consistency and effectiveness in privacy protection at a global level.").

272. *Id.* ("[P]olicies that ensure transparency, fair process, and accountability.").

273. *Id.* at 9.

"[p]romote creativity and innovation," "[l]imit Internet intermediary liability," and "[g]ive appropriate priority to enforcement efforts."[274]

By contrast, OECD Principles directly mention public goods such as security and law enforcement as substantive norms to be protected, yet frames them primarily as instrumental. For example, innovations to protect security "should not disrupt the framework conditions that enable the Internet to operate as a global open platform for innovation, economic growth, and social progress and should not be used as preten[s]e for protectionism."[275] Such needs, then, are again positioned as instrumental to a functioning society and market.[276] Under the OECD Principles, members may review current regulations and legislation to ensure that such instruments "can be effectively enforced and are consistent with fundamental rights."[277] With respect to security, the Principles call for policies that "enhance individual and collective efforts for self-protection and promote trust and confidence" and for careful assessment through multi-stakeholder processes to ensure "consistency with, and potential impact on, other economic and social dimensions of the Internet."[278] Nowhere do the OECD Principles affirmatively call for renewed efforts to build law enforcement needs into technical design.[279]

Finally, in juxtaposition to both individual rights and public goods, the OECD Principles discuss intellectual property (IP) as an instrumental means of supporting other goals, such as innovation and creativity. IP does not receive independent protection as a right or objective.[280] The document calls on members to "ensure protection of legitimate competition and fundamental principles such as freedom of expression, access to lawful content and Internet services and technologies, fair process, and privacy,"[281] while allowing for new and complementary approaches to protecting IP where necessary.

As with IP, limitations on intermediary liability are discussed because of the role they play in enabling other rights. Liability limits for intermediaries are not held out as an unalloyed good but as an instrumental one.[282] Again, while the

---

274. *Id.* at 8–10.
275. *Id.* at 10.
276. *Id.*
277. *Id.*
278. *Id.*
279. *See id.*
280. *Id.* at 6. Discussing how:

> Effective protection of intellectual property rights plays a vital role in spurring innovation and furthers the development of the Internet economy. . . . It is clear that the open and accessible nature of the Internet needs to be supported for the benefit of freedom of expression, and to facilitate the legitimate sharing of information, knowledge and exchange of views by users, including research and development, that has brought about widespread innovation to our economies.

Id.
281. *Id.* at 9.
282. *Id.* at 9 ("Limitations play an important role in promoting innovation and creativity, the free flow of information, and in providing the incentives for co-operation between stakeholders.").

document allows for members to consider that intermediaries can assist through multi-stakeholder processes, it says that such approaches should assess "the social and economic costs and benefits, including impacts on Internet access, use, security and development of the policy options," as well as "their compatibility with the protection of all relevant fundamental rights and freedoms and their proportionality in view of the seriousness of the concerns at stake."[283]

These Internet policymaking documents are aligned with global efforts to support the primacy of human rights.[284] They support the rights of freedom of expression, privacy and related associational freedoms, and self-development—rights that have been identified as particularly relevant to the development of the Internet and Information and Communication Technology (ICT) more broadly.[285] Scholars and practitioners have argued that these rights can be promoted by architectural choices such as decentralization, user empowerment, transparency, and open interfaces.[286] Conversely, they can be undermined through architectural choices that create bottlenecks, control points, preferences for open access,[287] and increased capacity for identification and surveillance.

Two recent reports from the UN Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression lend support for the prioritization of freedom of expression and freedom of privacy. The reports find that "[e]ncryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[288] They also note that the rights to "[p]rivacy and freedom of expression are interlinked" and that encryption and anonymity are protected because of the critical role they can play in securing

283. *Id.*

284. Universal Declaration of Human Rights G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171; S. Exec. Doc. E, 95-2 (1978), S. Treaty Doc. 95-20, 6 I.L.M. 368 (1967).

285. *See, e.g.*, David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/71/373 (Sep. 6, 2016), http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373 [https://perma.cc/H644-27T5] (discussing shutdowns and other governmental efforts to undermine freedom of expression on the Internet); David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/29/32, at 9 (May 22, 2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement [https://perma.cc/S4JW-XYPM].

286. *See, e.g.*, Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619 (1995); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1975 (2006).

287. *See, e.g.*, Cohen, *Pervasively Distributed Copyright*, *supra* note 97; Morris & Davidson, *supra* note 83; Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 574 (1998) (noting that "networks, like the Internet, have architectural designs and standards that implement the default rule of open information access" thus undermining privacy by default).

288. Kaye, *Report of the Special Rapporteur*, *supra* note 285, at 7.

those rights.[289] Private sector efforts to address human rights in the ICT sector have also focused on the rights to privacy and freedom of expression.[290]

Advisors and regulators focused on the responsibilities of the private sector provide a final source of values prioritization. First, the UN adopted the *Protect, Respect and Remedy Framework* (the Ruggie Report), which addresses risks to human rights in business activities and responsibilities for companies.[291] The UN Human Rights Council adopted a resolution unanimously welcoming the Ruggie Report, adding "that transnational corporations and other business enterprises have a responsibility to respect human rights."[292] Building upon this, the Global Network Initiative, a multi-stakeholder organization, found that "Information and Communications Technology (ICT) companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users."[293] Data protection and privacy regulators have also pushed the private sector to consider private protection during technical design.[294] In response, companies have moved to protect users affirmatively by deploying https encryption to protect communications and device encryption to protect data

289. Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/23/40, at 20 (Apr. 17, 2013), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement [https://perma.cc/UGJ6-XLPV].

290. *See, e.g.*, GLOBAL NETWORK INITIATIVE, GNI PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY (2008), http://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf [https://perma.cc/B3BH-R9B3].

291. John Ruggie (Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011), http://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf [https://perma.cc/295Q-9NMZ].

292. Human Rights Council Res. 8/7, U.N. Doc. A/HRC/RES/17/4, at 2 (Jun. 18, 2008), http://ap.ohchr.org/documents/E/HRC/resolutions/A_HRC_RES_8_7.pdf [https://perma.cc/AV8D-NFUQ].

293. GLOBAL NETWORK INITIATIVE, PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY 1 (2008), http://globalnetworkinitiative.org/sites/default/files/GNI-Principles-2008.pdf [https://perma.cc/D959-F9FX].

294. *See, e.g.*, FED. TRADE COMM'N, *supra* note 161; *Resolution on Privacy by Design*, *supra* note 158; *Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, at 27, COM (2012) 11 (Nov. 21, 2013), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN [https://perma.cc/X8Dx-J4ZP] (Draft EU Data Protection Regulation, Amendment 37).

stored on user devices.[295] They also issue transparency reports to alert users to requests for consumer data.[296]

The aforementioned documents and activities prioritize freedom of expression, privacy, security, individual empowerment (choice and control), and substantive fairness and nondiscrimination. This prioritization is consistent with the Universal Declaration of Human Rights (UDHR),[297] a set of values that is internationally recognized by the majority of societies. Values-in-design scholars have suggested that the adoption of constitutions can be viewed as a more abstract and representative version of the participatory design process, while dealing with "narrowly conceived self interests and hostile prejudices."[298] The UDHR, while not a formal constitution, is the product of a robust and representative process.[299] The Internet-specific documents flow from the foundational rights-protective frameworks of the UDHR.[300] They focus on threats from the lack of attention to values during design, as well as from the intentional desire to address privacy or other societal values at the level of architecture.[301]

The engineering and standards community has begun to emphasize the importance of this values prioritization in overcoming flaws in designing technology that regulates. Traditionally, design has sought to maximize engineering values such as interoperability, efficiency, elegance, and innovation.[302] While these remain relevant, they are a woefully incomplete set of priorities given the rights at stake in design, and more pointedly, in regulation through technology. Their continued emphasis—without additions—exacerbates the crowding-out problem noted above.

---

295. Adrienne Porter Felt et al., *Measuring HTTPS Adoption on the Web*, PROCEEDINGS OF THE 26TH USENIX SECURITY SYMP. 1334 (2017), https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-felt.pdf [https://perma.cc/5F3C-6ULE] (documenting "tremendous growth in HTTPS adoption"); Pablo Valerio, *Data Encryption on the Rise*, NETWORKCOMPUTING (Jan. 23, 2015, 8:00 AM), https://www.networkcomputing.com/applications/data-encryption-rise/840595896 [https://perma.cc/35RA-JCEV] (discussing data encryption by Blackberry, Apple, and Google).

296. Jillian York, *Tech Companies' Transparency Efforts May Be Inadvertently Causing More Censorship*, MOTHERBOARD (Dec. 8, 2017, 8:30 AM), https://motherboard.vice.com/en_us/article/8xmg3z/tech-companies-transparency-efforts-may-be-inadvertently-causing-more-censorship [https://perma.cc/V8R2-W6P8] (discussing rise of transparency reports from U.S. companies and potential downsides for dissidents).

297. Universal Declaration of Human Rights G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

298. BATYA FRIEDMAN, PETER H. KAHN, JR. & ALAN BORNING, UNIV. OF WASH., DEP'T OF COMP. SCI. & ENGINEERING, TECH. REPORT 02-12-01, VALUE SENSITIVE DESIGN: THEORY AND METHODS 2 (2002), http://faculty.washington.edu/pkahn/articles/vsd-theory-methods-tr.pdf [https://perma.cc/66E7-F3YL].

299. *Universal Declaration of Human Rights: History of the Document*, UNITED NATIONS, http://www.un.org/en/sections/universal-declaration/history-document/index.html [https://perma.cc/BNU4-2ECD].

300. *See* Kaye, *supra* note 285.

301. *Id.*

302. *See* Doty & Mulligan, *supra* note 68.

These engineering values have emerged from the bottom up through technical development processes and iterative engagement in international standard-setting bodies. Moving beyond them to create sets of capabilities that can be configured to support different policy objectives[303] requires a renegotiation of the rules of engagement as to how deeply values are absorbed. New rules must acknowledge the broad range of values always at play in technical design choices and, at least tacitly, the values contests that are increasingly afoot as regulatory aims become more central to technology choices.

This renegotiation is already underway in technical standard-setting bodies that have broadened their values-related work.[304] In some instances, this is more accurately construed as a grab rather than a negotiation, as engineers, disillusioned by revelations of illegal and indiscriminate government surveillance, seek to harden infrastructure to protect individual privacy without consultation or the consent of other stakeholders.[305] The renegotiation is also evident in the increasing focus on the extent to which governments should play a larger role in decisionmaking about technical standards and allocation of key Internet resources, such as domain names.[306] The values that have garnered attention and activity within technology standard-setting bodies include accessibility, privacy, security, freedom of expression, and, more recently, nascent human rights.[307]

The values at work at the W3C and IETF reflect the information-centric focus of the Web and Internet. Given the current role of ICT in society, privacy, security, freedom of expression, access to information, and accessibility are logical rights to have emerged as potentially worthy of protection or consideration through this bottom up process. Unsurprisingly, early

303. "*Separation of mechanism and policy*. Among the major causes of our inability to experiment with and adapt existing operating systems is their failure to properly separate mechanisms from policies. (Hansen has presented cogent arguments for this separation.) Such separation contributes to the flexibility of the system, for it leaves the complex decisions in the hands of the person who should make them—the higher-level system designer." W. Wulf et al., *HYDRA: The Kernel of a Multiprocessor Operating System*, 17 COMM. ACM 337, 338 (1974) (construing Per Brinch Hansen, *The Nucleus of a Multiprogramming System*, 13 COMM. OF THE ACM 238, 238-41 (1970) (arguing for the rejection of systems designed to embed particular security models)).

304. *Id.*; *see also, e.g.*, Cooper et al., *supra* note 71.

305. *See, e.g.*, Farrell & Tschofenig, *supra* note 83; Cindy Morgan, *IAB Statement on Internet Confidentiality*, INTERNET ARCHITECTURE BOARD, (Nov. 14, 2014), https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality [https://perma.cc/47WW-HYPX].

306. LENNARD G. KRUGER, CONG. RESEARCH SERV., R42351, INTERNET GOVERNANCE AND THE DOMAIN NAME SYSTEM: ISSUES FOR CONGRESS 6-20 (2013) (describing debates over Internet governance).

307. *See, e.g.*, *Web Accessibility Initiative*, W3C, https://www.w3.org/WAI [https://perma.cc/EVJ9-FESQ]; *Platform for Privacy Preferences (P3P) Project*, *supra* note 254; *Tracking Protection Working Group*, W3C, https://www.w3.org/2011/tracking-protection [https://perma.cc/58ZV-DNFR]; *Platform for Internet Content Selection (PICS)*, W3C, https://www.w3.org/PICS [https://perma.cc/U3VR-HJ3D]; Cooper et al., *supra* note 71.

consideration of the value impacts of the Internet also focused on this set of rights.[308]

Values work in other standard-setting bodies has centered on these rights as well,[309] although an emerging effort—harkening back to earlier interventions—seeks to protect human rights more broadly.[310] Recent specifications include RFC 7258,[311] which frames pervasive monitoring as an attack, reaffirms the IETF treatment of security as a privileged value,[312] and rejects built-in support for wiretapping.[313] The wiretapping provision lies in stark contrast to the telephony world, which has cooperated with government wiretapping, in some instances because telecommunications carriers are bound by law, including building networks that enable it.[314]

This consensus suggests a starting point for prioritizing which substantive values we might accept as part of technological architectures, and which should be promoted in ways less central to system design.

2. How to Prioritize: Exploiting Flexibility in Design

The typology of rights offers suggestions about how to actualize the flexibility in design discussed above. The design principles of modesty and restraint underscore the importance of recognizing that there are layers of technology within systems. These provide different points at which a technological intervention to promote a certain value can take place. In the Internet context, regulating through the core protocols or resources is different

---

308. *See, e.g.*, *Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet*, GLOBAL INTERNET LIBERTY CAMPAIGN, http://gilc.org/speech/report [https://perma.cc/37U7-HAAV] (focusing on freedom of expression and user control); Doty & Mulligan, *supra* note 68 (discussing W3C work on privacy, security, and accessibility).

309. *See, e.g.*, *Tracking Protection Working Group*, *supra* note 307; Cooper et al., *supra* note 71; Farrell & Tschofenig, *supra* note 83; Morgan, *supra* note 305 ("The IAB urges protocol designers to design for confidential operation by default.").

310. *See, e.g.*, Avri Doria, Niels ten Oever & Joana Varon, *Proposal for Research on Human Rights Protocol Considerations*, INTERNET ENGINEERING TASK FORCE (Mar. 2015), https://tools.ietf.org/html/draft-doria-hrpc-proposal-01 [https://perma.cc/Y4ND-NZZY].

311. Farrell & Tschofenig, *supra* note 83.

312. *Id.* at 4; *see also* Cooper et al., *supra* note 71.

313. Farrell & Tschofenig, *supra* note 83, at 2; Baker & Carpenter, *supra* note 83, at 1–2 (rejecting wiretappability because "operation of the Internet and the needs of its users are best served by making sure the security properties of connections across the Internet are as well known as possible. . . . making them as free from security loopholes as possible," "wiretapping will make affected protocol designs considerably more complex. . . . [and] jeopardizes the security of communications," and "[as stated in IETF RFC 1984,] commercial development of the Internet and adequate privacy for its users . . . requires the wide availability of strong cryptographic technology.").

314. *See* 47 U.S.C. § 1002(b)(1) (2012). Describing how the subchapter:

does not authorize any law enforcement agency or officer . . . to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by . . . any manufacturer of telecommunications equipment, or . . . to prohibit the adoption of any equipment, facility, service, or feature by . . . any manufacturer of telecommunications equipment . . . .

Id. (emphasis added) (setting capability requirements to be met by covered entities and *explicitly prohibits* the government from compelling them to change the design of their products).

from regulating the design of specific products that rely on or implement those protocols. Similarly, products can be regulated, and used to regulate, at the level of design, configuration, or defaults. To protect a public good like cybersecurity, regulators might be right to use all three levels to control behavior. However, doing so will come at the cost of reduced functionality and flexibility, generally, and of addressing competing values, specifically.

Similarly, distinguishing between facilitating and baking in—or prescribing values versus providing hooks for those at the upper levels to do so—provides an important vehicle for supporting consensus rights, supporting and forging ethical convergence, and allowing for evolution and generativity. The W3C work on privacy has often attempted to build mechanisms that protect rights but respect different implementations (i.e., acknowledging but not forcing ethical convergence) by supporting mechanisms and languages that act as a bridge. This work facilitates and provides hooks for values but does not determine them.

The consensus hierarchy of values, then, can guide policy makers and designers in choosing among sites of intervention (layers, design, deployment, defaults) and forms (hooks versus constraints) of technology as regulation.

David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has made comments on the treatment of encryption that provide a helpful, early description for how our four rules of engagement can interact to provide a useful structure for governance-by-design. As an initial matter, he confirmed that "encryption and anonymity are protected because of the critical role they can play in securing those rights."[315] He then concluded that, to be consistent with human rights law, restrictions on encryption "should be subject to public comment and only be adopted, *if at all*, according to regular legislative process" and, that "where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high."[316]

Kaye's emphasis on deliberative public processes aligns with our goal of achieving procedural and substantive legitimacy and proposes a venue and style of decisionmaking consistent with public governance norms. Kaye further emphasizes the government's need to avoid spillover effects, particularly given the role encryption plays in supporting the rights of privacy, freedom of expression, and association. This approach to regulating through technology on

315. Kaye, *Report of the Special Rapporteur*, *supra* note 285, at 7 (citing Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013); Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Corrigendum*, U.N. Doc. A/HRC/23/40/Corr.1 (Aug. 7, 2013)).

316. *See* Kaye, *Report of the Special Rapporteur*, *supra* note 285, at 12–13 (emphasis added).

behalf of law enforcement interests aligns with our principles of modesty and restraint to preserve flexibility.

Finally, Kaye's framing prioritizes a focus on the protection of human rights. It highlights the consensus that corporate economic interests take a back seat to human rights in technical design because "[t]he responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations."[317] And the report takes a hard look at the extent to which technological regulation to afford law enforcement access places other values, and other individuals, at risk.[318]

Kaye's report suggests that we should be more comfortable about building in, and even baking in, protections for human rights, while being mindful that doing so may not be the optimal vehicle of protection. It therefore points to the importance of the intervention point when thinking about technical design. Our first two rules, together, provide guidance about how to begin doing just that.

C. Third Rule of Engagement: Ensure regulators possess the right tools—broad authority and competence, and technical expertise

The third rule of engagement focuses on the institutional design and knowledge necessary to actualize the design and values norms reflected in the prior two rules. Governance-by-design should only occur in venues that can and do consider a wide scope of public values, and when government and other stakeholder groups have deep access to technical expertise.

Such a rule would have prevented the FBI from seeking an *ex parte* decision against Apple in a court ill-prepared to consider the political or technical issues at stake. In the SOPA case, it would require the legislature to have structures for considering broad value questions, not ones driven only by particular interest groups, and to have access to independent technical expertise, such as that formerly provided by OTA. Implementing electronic voting machines would have been overseen by a public authority capable of successfully (and democratically) translating public policy into code.

Existing governance institutions often lack these tools, and substantive regulatory capacity—breadth of authority, competence, and vision on the one hand, and expertise on the other—must be built to support the rational use of technology to govern. Reforms must address both the structure of institutions involved in technological decisionmaking and their internal decisionmaking processes. Existing mechanisms, such as joint referrals, consultation, multi-stakeholder processes, and collaboration with other agencies, can be used—and

317. Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HR/27/37, at 15 (June 30, 2014), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf [https://perma.cc/2FRD-WECY].

318. *Id.*

novel ones built—to avoid the natural myopia and foster the consideration of competing values. Expertise can be bolstered through the acquisition of new staff and processes or by leveraging external experts in other agencies, academia, professional associations, and stakeholder organizations.

1. Addressing Limits of Authority and Competence

The first challenge in addressing the "tunnel vision" and lack of competence that resulted in dystopic governance-by-design outcomes in our case studies is to broaden the set of values that decision makers must consider, decision makers' capacity to address relevant values, and the range of stakeholders who must participate in the decisionmaking process. To this end, we prescribe below a series of institutional reforms:

- Changing the design of legislative efforts;
- Expanding the scope of the regulatory charge;
- Changing internal decisionmaking by requiring human rights impact assessments;
- Leveraging coordination and input from a range of government actors; and
- Conditioning governance-by-design on multi-stakeholder involvement.

The fact that judicial decisionmaking processes are not subject to such external direction indicates that they, to the extent possible, should avoid direct involvement in governance-by-design efforts. By contrast, both legislative and regulatory efforts are susceptible to such efforts at structural design.

a. Change the Design of Legislative Efforts

Where regulation through technology is part of a legislative package, at least that component of the legislation should be referred to multiple committees. At the Congressional level, good governance-by-design requires procedures that enable multiple committees to review and shape a bill. Concurrent and sequential review is designed for bills that exceed the expertise of a single committee. This provides a way to navigate areas of overlapping responsibility and to coordinate policy in related areas. It also serves as a check on the myopia bred by the substantive agendas and technical expertise of a single committee, which may have close interactions with regulated parties and have members who have received campaign contributions from them.

b. Expand the Scope of the Regulatory Charge

In areas that anticipate regulation by design, Congress should expand the goals administrative agencies are required to consider to include a full range of human rights and public values. This is similar to what Congress already does when including requirements that agencies weigh issues of cost when

promulgating a regulation.[319] Recognizing the dynamic ways that the design decisions interact with values as technology advances, human interaction with technology systems develop, and contexts change, Congress should include in their regulatory charge processes for revisiting and updating governance-by-design decisions.

These efforts would thwart claims that agencies do not have jurisdiction to address values other than the core regulatory aims of the statute charged to their administration. They would also permit judicial review of the agency decisionmaking processes underlying governance-by-design efforts and reject as "arbitrary [and] capricious" processes that failed to give considered attention to, and then address, broader effects of such endeavors.[320]

Congress has, in fact, nodded (albeit in a limited manner) to the question of regulatory charge in two important pieces of legislation involving governance-by-design—the Digital Millennium Copyright Act (DMCA)[321] and CALEA[322]—creating at least a theoretical possibility for agencies to take a fuller range of values into account when pursuing techno-regulation.

The first example, the DMCA, involves once again a Congressional attempt to support the use of technology in order to strengthen the intellectual property rights protection in the face of digital-age challenges. As copyrighted works were increasingly distributed over the Internet, copyright holders in turn began using technological protection measures and DRM systems to exercise unprecedented control over their content.[323] Pressure from various stakeholders and rights holders in turn prompted Congress to enact the DMCA to prevent hacking of such measures. The law prohibits the circumvention and bypass of "technological measure[s] that effectively control[] access to a [protected] work"[324] and bans the trafficking of tools that are designed to enable such circumvention.[325]

---

319. MAEVE P. CAREY, CONG. RESEARCH SERV., R41974, COST-BENEFIT AND OTHER ANALYSIS REQUIREMENTS IN THE RULEMAKING PROCESS (2014) ("Regulatory analytical requirements (e.g., cost-benefit and cost-effectiveness analysis) have been established incrementally during the last 40 to 50 years through a series of presidential and congressional initiatives."), https://fas.org/sgp/crs/misc/R41974.pdf [https://perma.cc/65G6-X5VR].

320. *See* Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mutual Auto. Ins. Co., 463 U.S. 29, 41–45 (1983) (holding that it would be arbitrary and capricious for an agency to consider factors different than those on which Congress intended it to rely); Citizens to Preserve Overton Park, Inc. v. Volpe, 401 U.S. 402, 416 (1971) (holding that relevant factors must be considered).

321. 17 U.S.C. § 1201(a)(1)(A) (2012).

322. *See supra* notes 141–145 and accompanying text.

323. While DRM is often referred to as systems that seek to regulate copyrights, they are capable of reaching beyond copyright contours and regulating unprotected content that should be left in the public domain. *See, e.g.*, Pamela Samuelson, *DRM {and, or, vs.} the Law*, 46 COMM. ACM 41, 42 (2003).

324. 17 U.S.C. § 1201(a)(1)(A) (2012).

325. The DMCA also prohibits circumvention of a technological measure "that effectively protects a right of a copyright owner" (meaning exclusive rights under 17 U.S.C. § 106). 17 U.S.C. § 1201(b)(1)(A) (2012).

Recognizing the potentially vast and harmful implications of these provisions,[326] Congress enacted a number of statutory exceptions to the DMCA.

Most relevant, it created a unique, triennial rulemaking procedure that confers upon the Copyright Office the responsibility to create a regularized process for reviewing the impact of technical protection measures (TPMs) on noninfringing uses. This process allows any stakeholder to petition for an exemption for a particular class of content and gives the Copyright Office the authority to establish temporary (three-year) exemptions from the law to protect such noninfringing uses. [327] This rulemaking authority creates a "fail-safe mechanism"[328] to monitor the impact of TPMs on the values reflected in copyright law and facilitates ongoing consideration of competing values within the techno-regulation.

The DMCA has been subject to significant criticism,[329] as has its TRM procedure.[330] Indeed, this mammoth governance-by-design initiative runs afoul of several of our rules of engagement for its sweeping invitation to use technology to regulate overbroadly, and its delegation of the technical means of doing so to the private sector.

At the same time, the triennial rulemaking authority illustrates how a technology-focused law can be designed to allow room for flexibility, adaptations, reexaminations, monitoring and "fail-safe mechanisms,"[331] as well as consideration of competing values within its boundaries. According to legislative history, the rulemaking proceeding's primary goal is to balance

---

326. While this motivation for enacting the rulemaking procedure is implied from the legislative history, Herman & Gandy claim that the public interest was n'ot the reason behind the exemptions:

> [t]o some, the recurring procedure to determine exemptions may appear to be intended as an equitable solution to the harms to noninfringing uses created by TPMs. We strongly disagree. The appearance and evolution of the statutory provision for the hearings, as well as the reasoning behind each maneuver, help illustrate that most members of Congress were far more concerned with protecting the interests of copyright holders than with protecting fair use in the digital millennium.

Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121, 141 (2006).

327. *See* 17 U.S.C. § 1201(a)(1)(B)–(D) (2000).

328. *See* REPORT OF THE HOUSE COMMITTEE ON COMMERCE ON THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, H.R. REP. NO. 105-551, pt. 2, at 36 (1998) (Commerce Comm. Rep.) (stating, when referring to the DMCA exceptions, that "[g]iven the threat of a diminution of otherwise lawful access to works and information, the Committee on Commerce believes that a 'fail-safe' mechanism is required").

329. *See, e.g.*, Samuelson, *Intellectual Property and the Digital Economy*, *supra* note 98; Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001).

330. Woodrow Neal Hartzog, *Falling on Deaf Ears: Is the "Fail-Safe" Triennial Exemption Provision in the Digital Millennium Copyright Act Effective in Protecting Fair Use?*, 12 J. INTELL. PROP. L. 309 (2005); *see also* Herman & Gandy, *supra* note 326; Samuelson, *Intellectual Property and the Digital Economy*, *supra* note 98.

331. H.R. REP. NO. 105-551, pt. 2, at 36 (stating, when referring to the DMCA exceptions, that "[g]iven the threat of a diminution of otherwise lawful access to works and information, the Committee on Commerce believes that a 'fail-safe' mechanism is required").

values: specifically, to "assess whether the prevalence of these technological protections, with respect to particular categories of copyrighted materials, is diminishing the ability of individuals to use these works in ways that are otherwise lawful."[332]

As the use of TPMs has proliferated, they have surfaced a range of new values not anticipated in the statutory exceptions, such as competition and rights to repair.[333] For example, a recently concluded rulemaking provides a sense of the competition issues arising as automakers have embedded cars with code. Petitioners documented the ways in which software-based lock-out codes, authentication sequences, and encryption were being used to constrain consumers' and third-party service providers' interactions with lawfully purchased automobiles.[334] Petitioners reported that technical protection measures interfered with the ability of owners and independent repair shops to modify and repair vehicles, including agricultural vehicles.[335]

Unfortunately, the Copyright Office has declared itself incompetent to address the competition between intellectual property values and the other wide-ranging values brought up in its rulemaking process, reflecting the dysfunctions arising from limited authority (or the perception of limited authority) that we have identified as prevalent in governance-by-design efforts. It has, accordingly, limited its interventions to internal copyright-balancing issues.

Yet the agency has alerted Congress to the problems revealed through the TRM process and the need for reforms. For these purposes, the rulemaking procedure provided a venue for diverse stakeholders to at least object to the impact of evolving marketplace uses of TPMs on competing values, which has alerted other agencies to the risks that TPMs pose to their substantive agendas—be they security, competition, or human rights. Stakeholders have used the record created by the triennial review proceedings to support recommendations for law

---

332. *Id.* at 36–37.

333. For a thorough overview of the misuse of § 1201 of the DMCA to thwart competition see ELECTRONIC FRONTIER FOUND., UNINTENDED CONSEQUENCES: SIXTEEN YEARS UNDER THE DMCA 17–27 (2014), https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf [https://perma.cc/2S7F-LCPB] (examining cases where the DMCA is used to deter legitimate competition instead of to prevent piracy).

334. Petitions for exemption can be viewed here: *Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Petitions*, COPYRIGHT.GOV (2014), http://copyright.gov/1201/2014/petitions [https://perma.cc/R8SN-H29G]. Petitions 12, 14, 23, 24 are specifically about automotive vehicles.

335. *See* Electronic Frontier Found., Petition In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07, U.S. Copyright Office, https://www.copyright.gov/1201/2014/petitions/Electronic_Frontier_Foundation_1201_Initial_Submission_2014.pdf [https://perma.cc/GB74-85U4]; Intellectual Property & Tech. Law Clinic, Univ. of S. Cal., Petition for Proposed Exemption Under 17 U.S.C. § 1201, U.S. Copyright Office, https://www.copyright.gov/1201/2014/petitions/USC_IP_and_Technology_Law_Clinic_2_1201_Initial_Submission_2014.pdf [https://perma.cc/AB63-6FTZ].

reform to address the overreach of the techno-regulation.[336] And while Congress has not taken additional action to address the impact of DRM on security, competition, and rights to repair, the rulemaking has created some degree of ongoing visibility into conflict of values involved.

A second example is found in CALEA—one of the few laws requiring that technical capabilities be supported in the design of private sector equipment. CALEA requires "telecommunications carriers" to ensure that their "equipment, facilities, or services" allow the government to intercept communications pursuant to a court order or other lawful authorization.[337] On the one hand, the statute limited the requirement to provide wiretap capability to that category of actors—and purposefully excluded other Internet information services providers. At the same time, however, CALEA included a delegation of power to the FCC, pursuant to which they conduct public hearings to determine whether, as technology changes, the scope the category of telecommunications carriers should be altered to include other services that are "replacement[s] for a substantial portion of the local telephone exchange service" under the law.[338] While this process has not safeguarded competing values in practice, CALEA in theory offers at least a rudimentary schema for narrowly tailored techno-regulation, plus a future-proofing mechanism that enables adjustment to technical and marketplace change.

Together, DMCA and CALEA suggest that capacity for legislative recognition of values-myopia that can lead to errors and unintended consequences when regulating through technology over time. They offer the beginnings of an acknowledgment that agencies must be more permeable to interests outside their core substantive agenda, must provide opportunities for stakeholders representing other values to enter the discussion, and must enable iterative reviews of techno-regulation when governing by design.

c. Change Internal Decisionmaking: Require Human Rights Impact Assessments (HRIAs)

Congress (through legislation) should further mandate that any agency contemplating regulating through technology conduct a Human Rights Impact Assessment (HRIA). Until that time, the executive branch (either by executive order or by individual agency decision) should condition its own efforts on the use of such tools for assessing the ethical and political impact of techno-

336. *See* BERKELEY CTR. FOR LAW & TECH. ET AL., CYBERSECURITY RESEARCH: ADDRESSING THE LEGAL BARRIERS AND DISINCENTIVES 22–25 (2015), https://www.ischool.berkeley.edu/sites/default/files/cybersec-research-nsf-workshop.pdf [https://perma.cc/DJV6-JUFM].

337. 47 U.S.C. § 1002(a)(1) (2012).

338. *See id.* § 1001(8)(B)(ii). The government has used this procedure to obtain FCC authority to monitor VoIP and other Internet-based communications. In the Matter of Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 20 F.C.C. Rcd. 14989, 14989 (2005), on reconsideration in part, 21 F.C.C. Rcd. 5360 (2006).

regulation. These assessments can be modeled on privacy impact assessments (PIAs), which are required by federal administrative agencies developing or procuring information technology systems that include personally identifiable information under the E-Government Act of 2002.[339] HRIAs, which are nascent but becoming more common in the private sector, would focus agencies on the competing values and unintended consequences of technological regulatory tools. Beyond assessing risk, HRIAs would help organizations identify and discuss alternatives and mitigations, and explain the rationale for the final choice of technology design.

Ongoing work focuses on assessing the human rights and ethical impacts of technology[340] more broadly, but the intentional, governmental use of technology to regulate raises unique questions that make HRIAs more urgent.[341] As Karen Yeung forcefully states, "when employed as regulatory policy instruments, choice architecture [including technologies that shape and nudge human behavior] must be justified and subject to institutional safeguards."[342] Justification must include consideration of "the extent to which the technique undermines liberal democratic principles (including any interference with fundamental rights) and the extent to which they distort or undermine individual freedom."[343]

HRIAs will increase the likelihood that human rights will be identified and addressed during design. As we have identified in the context of privacy decisionmaking by government agencies, the success of such decisional tools is highest where it is used by an expert with inside access to the development process and a mix of embeddedness and independence.[344] Similar to other impact assessments (such as cost-benefit analysis and environmental impact assessments), HRIAs would create different frameworks and bring new considerations to bear in agency actions. They would facilitate participation by issue experts and by stakeholders who might otherwise be unaware of relevant risks and technological alternatives that might better accommodate human rights. By engaging other expert communities, HRIAs can bridge the gulf between the domain expertise of the regulatory agency and the frameworks, language, and risks familiar to human rights and consumer protection organizations when considering the details of a techno-regulation. They will serve a signaling function by alerting relevant organizations to the stakes of a techno-regulation,

339. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2921–22 (codified at 44 U.S.C. § 3501 note (2000 & Supp. 2002) (requiring agencies to conduct a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form").

340. *See* Oever & Cath, *supra* note 71; *see also* Cath & Floridi, *supra* note 237.

341. *See* Yeung, *supra* note 131.

342. *Id.* at 199.

343. *Id.*

344. Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-making in U.S. Government Agencies*, *in* PRIVACY IMPACT ASSESSMENT 225, 244 (David Wright & Paul De Hert eds., 2012); Bamberger & Mulligan, *Privacy Decisionmaking*, *supra* note 36.

and will bolster the legitimacy of stakeholders who may otherwise be perceived as raising issues that are out of scope.

d. Leverage Coordination and Input from a Range of Government Actors

Furthermore, efforts at governance-by-design must be conditioned on the leveraging of mechanisms that facilitate agency coordination around policy to address the risks of techno-regulation. Coordination tools come in many forms. Congress can require coordination, as they did pursuant to the Gramm–Leach–Bliley Act of 1999[345] regulating financial services, which originally charged eight federal agencies jointly with working together to implement regulations and enforcement policies to carry out the Act's *financial privacy* provisions.

Agencies may furthermore agree to coordinate their actions and collaborate on policy development. Scholars have clustered these collaborative efforts along degrees of voluntariness and integration. These include "collaboration," "coordination," "merger," "integration,"[346] and "consultation provisions, interagency agreements, joint policymaking, and centralized White House review."[347] Reviews of agency action have found that coordination can have a positive effect on policy outcomes, increase agency expertise and require agencies to jointly consider the impacts of technical choices.[348] This sort of coordination can broaden agency perspective and help mitigate systemic risks that may otherwise be overlooked.[349] Importantly, coordination, as compared to more integrated actions, maintains the healthy tension among agencies with different missions while diversifying inputs, improving and expanding information, and increasing and diversifying expertise.[350] For these reasons, coordination, rather than integrated policy action, may be the preferred method for regulating through technology.

The White House in particular can play a particularly important coordinating role with respect to governance-by-design. Technology can make policies sticky and pervasive, yet hard to see, and standard Office of Management and Budget (OMB) regulatory review processes of may miss them given the staff involved. The White House's Office of Science and Technology

345. Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338, 1342–43 (codified in scattered sections in 12 U.S.C. and 15 U.S.C. (1999)).

346. FREDERICK M. KAISER, CONG. RESEARCH SERV., R41803, INTERAGENCY COLLABORATIVE ARRANGEMENTS AND ACTIVITIES: TYPES, RATIONALES, CONSIDERATIONS 2–5 (2011) (analyzing how different types of collaborative arrangements ensure cooperation among agencies).

347. Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1155 (2012).

348. *Id.* at 1184 (describing how EPA-NHTSA joint rulemaking, in which they "formed joint technical teams, pooled data and information, and closely scrutinized their respective modeling techniques," improved the data and expertise available to both agencies and "required the agencies to think carefully through every element of program design and implementation together").

349. *Id.*

350. *Id.* at 1185.

Policy (OSTP), however, is a unique resource, providing the administration with access to expert advice from multiple technical domains.[351] During the Obama Administration OSTP played an important role in both coordinating agency action around issues such as encryption policy, as well as setting high level goals and coordinating technical design goals across multiple agencies in the areas of big data and artificial intelligence.[352] Additionally, the White House possesses the capacity to apply to governance-by design efforts requirements currently governing the promulgation of "major rules" pursuant to Office of Information and Regulatory Affairs' regulatory review process, which explicitly provide for input and comment by the breadth of administrative agencies.[353]

e. Condition Governance-by-Design on Multi-Stakeholder Involvement

Public agencies can shape the values expressed in governance-by-design in different ways. They can intervene "as public policy advocates promoting policy objectives,"[354] or as an enforcer and "activist privacy regulator,"[355] or as participants or vocal outside observer.[356]

Yet government must also create incentives for the technologists and regulated entities to bring in a broad range of other stakeholders—such as consumers, industry, civil liberties, and civil rights groups—that represent values that may impact their deliberations. In this way, the conscious or unconscious biases reflected in industry and engineering practices are in conversation with competing metrics, including those of good design, civil liberties, civil rights, and consumer protection. The unique, triennial rulemaking procedure set out in the DMCA, discussed above, [357] similarly institutionalized opportunities for a range of stakeholder input. Moreover, the multi-stakeholder processes convened by the National Telecommunications and Information Administration (NTIA)—an agency in the United States Department of Commerce that serves as the

351. *See generally* Jeffrey Mervis, *Internal Logs Show White House Interviewed Science Adviser Candidates. But Who?*, SCIENCE, http://www.sciencemag.org/news/2018/02/internal-logs-show-white-house-interviewed-science-adviser-candidates-who [https://perma.cc/J2ZT-7DL5] (noting that the Trump Administration has yet to appoint a person to head OSTP).

352. *See, e.g.*, Ed Felten & Terah Lyons, *The Administration's Report on the Future of Artificial Intelligence*, WHITE HOUSE BLOG (Oct. 12, 2016, 6:02 AM), https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence [https://perma.cc/X4EQ-CFWT]; *see also* John P. Holdren & Megan Smith, Office of Sci. & Tech. Policy, Exec. Office of the President, Cabinet Exit Memo (Jan. 5, 2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_exit_memo_final.pdf [https://perma.cc/FN5W-7S6B].

353. Exec. Order No. 12,866, § 6, 58 Fed. Reg. 51,735 (Sept. 30, 1993).

354. Reidenberg, *supra* note 287, at 587.

355. BAMBERGER & MULLIGAN, *supra* note 15, at 69; *see* Bamberger, *Technologies of Compliance*, *supra* note 11, at 729 (advocating for "more intense regulator involvement in oversight and accountability" of technologies of compliance).

356. *See* Doty & Mulligan, *supra* note 68 (discussing government engagement, including participation, feedback, and critiques of W3C technical standard-setting processes around privacy).

357. *See infra* notes 321–333 and accompanying text.

President's principal advisor on telecommunications policies,[358] around privacy issues raised by a range of technologies including facial recognition,[359] drones,[360] and the Internet of Things—provide early models for inclusive venues and processes that foster decisional legitimacy.

Technical standard-setting activities can offer further models for broadening input regarding governance through technology. Standard-setting processes can have a profound effect on human rights and civil liberties, and civil society organizations focusing on Internet policy issues have participated in important standard setting activities over the years.[361] And as we have described elsewhere in examining the W3C's privacy activities, technical standard-setting processes have some procedural features that make them particularly rich sites of engagement.[362]

2. Addressing Deficits in Expertise

Regulators must, moreover, use a range of approaches to address gaps in technological knowledge. These include developing internal expertise, drawing on the knowledge of other agencies and directly soliciting technological expertise from stakeholders.

---

358. Multistakeholder Process to Develop Best Practices for Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems, 81 Fed. Reg. 26,527 (May 3, 2016).

359. *Privacy Multistakeholder Process: Facial Recognition Technology*, NAT'L TELECOMM. & INFO. ADMIN. (June 17, 2016), https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology [https://perma.cc/T7VR-6GPQ].

360. *Multistakeholder Process: Unmanned Aircraft Systems*, NAT'L TELECOMM. & INFO. ADMIN. (June 21, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems [https://perma.cc/H32U-F5UT].

361. Arne Hintz, *Challenging the Digital Gatekeepers: International Policy Initiatives for Free Expression*, 2 J. INFO. POL'Y 128, 134–36 (2012) (describing how civil society organizations have increasingly become involved in policy processes because of their expertise and ability to help develop new forms of accountability). For an overview of the importance of Internet and Web technical standards for human rights and values, see Morris & Davidson, *supra* note 83; for a discussion of privacy standards at W3C in particular, see Doty & Mulligan, *supra* note 68; and for some additional standards where public interest organizations have participated, see Sally Floyd & Leslie Daigle, *IAB Architectural and Policy Considerations for Open Pluggable Edge Services*, INTERNET ENGINEERING TASK FORCE (Jan. 2002), https://tools.ietf.org/html/rfc3238 [https://perma.cc/6VPE-CXJM] (discussing recommendations by the Internet Architecture Board (IAB) on policy related to the Open Pluggable Edge Services (OPES)). *See also* Bray, *supra* note 46 (specifying a Hypertext Transfer Protocol (HTTP) status code to promote transparency); Danley et al., *supra* note 69.

362. Doty & Mulligan, *supra* note 68. Other features, such as meeting locations that rotate around the world, are more problematic. Though it increases participation by geographically diverse stakeholders, rotating the locus of activity may exclude civil society organizations, which often situate in national capitals and sites of international policy-making. Additionally, participation has been limited by a dearth of funding and technical expertise as smaller corporate players and subgroups with stakes in techno-regulation debates may also lack expertise and the resources to procure it. *See* Joe Waz & Phil Weiser, *Internet Governance: The Role of Multistakeholder Organizations*, 10 J. TELECOMM. & HIGH TECH. L. 331, 337 (2012) (discussing "openness" and how it is relative, since participation is contingent upon access to resources).

Some agencies, such as the FTC, now have technologists on staff. FTC technologists' knowledge and background directly aid the agency and also create new receptors for other forms of expertise.[363] They signal to the broader technical research community that their research and perspectives have a role in agency activity.

Those engaging in governance-by-design can also call on the technological expertise of other agencies, such as the National Institute of Standards and Technology (NIST), a research-only agency within the Department of Commerce. NIST brings together technical experts around a wide range of issues, including privacy, identity management, cybersecurity, usability, and many others.[364] NIST activities and publications provide a rich source of technical expertise and guidance to other federal agencies.[365]

Perhaps most importantly, agencies may solicit technological expertise directly from stakeholders. For example, the Federal Election Commission (FEC) used the "notice-of-inquiry" process to request information and feedback prior to proposing rules related to activity on the Internet.[366] Agencies may use their soft powers to convene workshops to learn about specific technology from experts in the field[367] and invite broader engagement with relevant research communities through workshops and conferences.[368] These interactions increase

363. David C. Vladeck, *Charting the Course: The Federal Trade Commission's Second Hundred Years*, 83 GEO. WASH. L. REV. 2101, 2106 (2014) (discussing appointment of first chief technologist, Professor Edward Felten, in 2010 and the ongoing acquisition of technological staff).

364. For examples of NIST's activities related to information and communication technologies, see *What ITL Does*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/itl/about-itl [https://perma.cc/Y8VF-H2WY].

365. *See, e.g.*, SEAN BROOKS ET AL., NAT'L INST. OF STANDARDS & TECH., NO. 8062, AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS (2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf [https://perma.cc/UE87-Y43N]; RONALD S. ROSS, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBL'N NO. 800-53 REV. 4, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [https://perma.cc/HVC6-YZV2].

366. Use of the Internet for Campaign Activity, 64 Fed. Reg. 60,360, 60,361 (Nov. 5, 1999) (Notice of Inquiry and Request for Comments); *see also* Comments of the Center for Democracy et al. to the Federal Election Commission, Notice of Inquiry, 1999-24**,** **(**Jan. 6, 2000), https://cdt.org/files/speech/political/000106fec.shtml [https://perma.cc/DVL5-LQT3] (responding to the Notice of Inquiry and Request for Comments, *supra*).

367. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 287–89 (2011) (discussing regulatory tools outside the enforcement context such as FTC workshops that help agencies understand technology); BAMBERGER & MULLIGAN, *supra* note 15, at 189–92 (discussing the FTC's use of "[n]onenforcement [r]egulatory [t]ools, [p]ublic [v]isibility, and [t]ransparency" in governing privacy).

368. The FTC regularly holds workshops at academic venues, began a yearly conference in 2016 called PrivacyCon, to explore the latest research and trends related to consumer privacy and data security that attracts researchers from diverse disciplines. *See PrivacyCon*, FED. TRADE COMM'N (Jan. 14, 2016, 9:00 AM), https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon [https://perma.cc/7Y4N-BSCS].

an agency's technical knowledge and ability to contemplate the risks and opportunities of innovation.

Furthermore, agencies can contract with experts to review technology, as then-Secretary of State Debra Bowen did when she commissioned an academic review to ensure her agency had independent advice on California's electronic voting systems.[369] Similarly, the Justice Department hired researchers to conduct an independent review of the FBI's Carnivore Internet wiretap system—a software-based tool to examine Internet Protocol packets—to explore its support and compliance with various legal requirements and policies.[370]

Agencies, as well, can and do combine these approaches. In their Autonomous Vehicle Policy, NHTSA combines a proposed network of external experts with new tools for acquiring necessary technical staff.[371]

The ideal approach for a given agency will vary based on the anticipated frequency and extent of techno-regulation related to the agency's mission. The increasing ubiquity of technology and the interest in governing by design suggests that many agencies—ranging as far afield as public utilities with demand control energy systems that regulate consumption, and police departments using surveillance tools—will require additional, dedicated expert staff.

D. Fourth Rule of Engagement: Maintain the Publicness of Policymaking

Our fourth rule of engagement requires that governance-by-design be conducted only subject to mechanisms that translate traditional commitments to participation and transparency to the technology context, in ways that address the intricate way in which policy is embedded in technical design and implementation choices.

Mechanisms for ensuring regulatory accountability, including transparent processes, stakeholder participation, and after-the-fact public scrutiny, guarantee public oversight and participation in traditional government policymaking. The opacity of code, the lack of general technological expertise, the characterization of design decisions as implementation rather than policy, and the difficulty in revisiting technology choices after the fact, however, thwart these guarantors of public involvement in governance-by-design. Diminished citizen awareness of techno-regulation, moreover, undermines the viability of traditional political checks. In the absence of governance-by-design constraints, the FBI pursued

369. Bowen, *supra* note 125.

370. STEPHEN P. SMITH ET AL., IIT RESEARCH INST., INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM, FINAL REPORT (2000), https://www.justice.gov/archive/jmd/carniv_final.pdf [https://perma.cc/G8KH-RMLX].

371. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY 81–82 (2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV policy guidance PDF.pdf [https://perma.cc/QFE6-3YE7].

their goals through private courts and third-party hackers; private companies set the design of voting machines without public oversight; and SOPA was drafted without oversight from a broader group of public stakeholders, and privacy-by-design imperiled fairness.

The wave of past multi-stakeholder processes around the use of technology design to serve policy objectives have consistently focused on totems of "participation" (generally understood as open access to a broad range of stakeholder input) and "transparency," satisfied by public documentation and open meetings and by requiring articulation of reasons for decisions as essential for procedural legitimacy.[372]

Though these procedural protections offer an important first set of guideposts for regulating through technology, they are little more than extensions of existing procedures that guide agency rulemaking. They fail to offer details on how to translate general governance principles of participation and transparency in ways that address the specific challenges the technology design process presents. The discussion below explores those details.

372. The 2012 Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13,098, 13,099–101 (Mar. 5, 2012), http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf [https://perma.cc/AN7S-STZD] (requesting public comments), for example, engaged the public in a high-level conversation about issues of procedural fairness—participation, transparency, and accountability. In response, a coalition of civil society organizations set out *Principles for Multi-Stakeholder Process*, WORLD PRIVACY FORUM (Feb. 23, 2012), http://www.worldprivacyforum.org/pdf/MultiStakeholderPrinciples2012fs.pdf [https://perma.cc/7N2B-C83A]. The Principles called for the following: "robust and reasonably balanced" consumer representation; "public sessions," "public documents" and "substantial decisions . . . made in open sessions"; equal opportunity to present proposals and equal treatment of items proposed; transparency about participants' affiliations; freedom to communicate about the process to nonparticipants; inclusion of dissenting views with published consensus documents; decisions based on "fair and broad consensus" not majority vote; open discussions, balance, mutual respect and consensus as guiding principles; electronic meetings unless adequate resources are provided to facilitate in person participation by civil society; civil society input on meeting locations; advanced access to documents to be considered; and the right to revisit and amend rules at the end of twelve months. *Id.* These principles are similar to those set forth in other areas by practitioner groups that emphasize inclusiveness, openness, transparency, participatory decision-making processes, and respect. *See, e.g.*, *IAP2 Core Values*, INT'L ASS'N FOR PUB. PARTICIPATION (2007), http://www.iap2.org/displaycommon.cfm?an=4 [https://perma.cc/VV9B-3F6G]; *Core Principles for Public Engagement*, NAT'L COALITION FOR DIALOGUE & DELIBERATION (Aug. 1, 2010), http://ncdd.org/rc/item/3643 [https://perma.cc/Y3BF-PHCT]. Scholars have underscored the importance of such "Input Legitimacy" when using "code as law." Marco Goldoni, *The Normativity of Code as Law: Toward Input Legitimacy* 1–3 (Sept. 7, 2011), http://ssrn.com/abstract=1923628 [https://perma.cc/5DAN-NQNE]. Under such a rubric, the legitimacy of technological production "should be assessed according to two intertwined principles: . . . transparency and publicness." *Id.* at 11. Accordingly, decisions "should be known and also the procedure that brought to that decision should be disclosed. . . . [and] the 'writing' of code [should involve an] equal chance of participation to the process, which also entails the idea that the writing process should be as inclusive as possible." *Id.*; *see id.* at 1 (arguing that "it is important to look not only at how new technologies shape democratic politics, but also how democratic action can shape the same technologies").

Specifically, translating participation to be meaningful for the design context requires input and oversight by stakeholders with both substantive and technological capacity at multiple points over the design and implementation timeline. The traditional sequential perspective of "policymaking" (during which there is an opportunity for input) followed by "implementation" is inconsistent with design. Rather, a stakeholder community with technical expertise must be developed that is accorded both the forum to wrestle with the question of which technical choices must be made in public processes and which can be left to private development, and given meaningful opportunities for insight and input throughout the processes that develop and implement technical standards, products, and systems. Building on the values-prioritization commitments and institutional suggestions of our second and third rules of engagement, greater participation would be coupled with regularized *ex post* reviews that create episodic opportunities for careful public scrutiny of how governance-by-design affects human rights and public values.

Moreover, for transparency to be meaningful in the design context, the process must not only include formal openness about the code itself, but also involve "political visibility"—publicity about the very existence and political nature of questions being resolved by design choices. Once resolved with technology, political choices may be viewed differently than legal rules—as less coercive or as products of the market or technical limitations—if seen at all. Governance-by-design processes must make the politics of design and implementation visible to stakeholders and the broader public, and more amenable to their participation.

1. Making "Participation" Meaningful for the Design Context

a. Meaningful Participation Must Reflect the Timing of Design

Operative differences between the regulatory levers of technology and those of law require public participation at different times to achieve the same democratic ideals. Traditionally, when a regulation is being promulgated, meaningful participation is satisfied by providing the opportunity to comment ex ante. The task of writing, implementing, and enforcing the final legal mandate is then handed off to the regulator. If displeased with the results on the ground, parties can then, ex post, return to the agency to advocate for change or challenge the result in court.

The development of technology as a regulatory tool works differently and requires different opportunities for meaningful participation. Limiting participation to ex ante policy decisions through the "notice-and-comment" process misses the action when regulators delegate or hand off the design and crafting of regulatory technology to standard-setting bodies, engineers, designers, and program managers. Tracking the notice-and-comment process may also reduce regulators' access to expert information that could help shape

their understanding of the technology, the appropriate rules, and the interaction among values.

In contrast to traditional legal regulation, values in technical infrastructure play out in a continuum—at design time, configuration time, and run time.[373] Technology is quite plastic during each stage. This presents unique risks for values, but it also provides opportunities to protect flexibility and generativity while enabling stakeholders to address ongoing disputes about the exact contours and balance within and across values. This "developer" perspective on the ability and need to address values at every stage of the process is captured in the security adage, "Secure by Design, Secure by Default, Secure in Deployment."[374]

This continuum between goals and implementation choices is also reflected in the work of standard-setting bodies. A formal specification or standard may be accompanied by implementation and deployment guidelines that provide information and advice but do not require conformance.[375] These documents allow designers to address technical and other issues that, while outside the formal specification, are important to achieving the goal of the standard. They allow the developers to convey the standard's intention without constraining more of the design space than is necessary. And they recognize that achieving an outcome requires attention through the whole process, although the role of the standard-setting organization moves from more to less directive as other goals—localization, cost, and business strategy—are allowed to compete in implementation and product.

The fact that values in technology play out across a time continuum requires government agencies to exercise greater influence and oversight, and to provide greater public participation during the translation of policy into specific standards and technical artifacts. The skirmish around voting machines illustrates this point. The translation of federally established design requirements into voting machines was performed by private companies and validated by private testing labs. The public was locked out of the design process and unable to ensure that federal requirements were faithfully translated into the machinery of democracy. Afterwards, trade secrecy, copyright, and contracts limited regulators' ability to test and study the machines. Regulators lost insight into the processes and outputs of the technical artifacts, impeding oversight and accountability in these vital systems. Finally, as these new electronic voting

373. Clark, *supra* note 80, at 463 (discussing how value tussles play out at design, redesign, configuration, and run time).

374. Steve Lipner, *The Trustworthy Computing Security Development Lifecycle*, PROCEEDINGS OF THE 20TH ANNUAL IEEE COMPUTER SECURITY APPLICATIONS CONF. (2004).

375. For example, the W3C Platform for Privacy Preferences specification is accompanied by a set of non-normative P3P Guiding Principles, Lorrie Cranor et al., *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C (Apr. 16, 2002), https://www.w3.org/TR/2002/REC-P3P-20020416 [https://perma.cc/7BFC-8XYY], and a Deployment Guide, Martin Presler-Marshall, *The Platform for Privacy Preferences 1.0 Deployment Guide*, W3C (Feb. 11, 2002), https://www.w3.org/TR/2002/NOTE-p3pdeployment-20020211 [https://perma.cc/4RGQ-Z7AP].

systems were unleashed on elections, there was no systematic effort to collect information about performance. Information about problems experienced in the field, however, yields important insight into whether and how values are protected. This is particularly true where software interacts with other software and human processes in unpredictable ways. A rich feedback loop is necessary to understand the values implications of the system as a whole in the wild.

Thus, meaningful participation requires stakeholder participation throughout all stages of the policy and design process. Technology that regulates will be filtered through designers and users, and its impact on values can often change over time through changes in human interaction. Just as institutional processes and practices can be more or less aligned with the substantive goals motivating a law's adoption, so too can standards and products. Effective regulation through technology requires continued participation and oversight at—and after—the implementation stage.[376] As a means of both mitigating unintended consequences and addressing technological and social change, then, venues for values-in-design debates must include procedural opportunities for both public input into regulations through design (whether designed by the government or the private sector) and after-the-fact oversight of design implementation, including redesign.[377]

NHTSA's newly issued Autonomous Vehicle Policy (AVP) (governing "connected cars") offers an early model to address issues of timing in two ways.[378] First, rather than calling for after-the-fact review of the code, it calls for stakeholder engagement in the development of the algorithms that control the decisionmaking of autonomous cars.[379] The policy calls for ethical judgments and decisions to be made "consciously and intentionally" and determined through a transparent process that involves all stakeholders in the design of algorithms that address conflicts between safety, mobility, and legality.[380] This is the first time the federal government has called for a transparent and inclusive public process to inform the *initial development* of algorithms that will resolve these ethical dilemmas, creating opportunities for the public to participate in the technical design.

Second, NHTSA identified the need for additional regulatory tools and rules to regulate the certification and compliance verification of post-sale

376. Designing for values "entails an iterative process whereby technologies are invented and then redesigned based on user interactions, which then are reintroduced to users, further interactions occur, and further redesigns implemented." Friedman & Borning, *Value Sensitive Design as a Pattern*, *supra* note 231, at 110.

377. *See* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 696–99 (2017) (emphasizing the importance of after-the-fact technological accountability).

378. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 371, at 7–8.

379. *Id.* at 26.

380. *Id.*

software updates.[381] This provision recognizes that redesign time presents another opportunity for values to be expressed and altered.

The NHTSA proposal is an important step forward in building robust public processes to shape initial design choices. Where other efforts have focused on opening up the "black box"—exposing the innards of already created algorithms to public scrutiny[382]—NHTSA has called for public input into code creation. In addition, recognizing that software updates will be an important method for addressing evolving safety and performance issues, and that such updates can alter the vehicle subsequent to vehicle certification, NHTSA identifies the need for additional regulatory tools and rules to regulate the certification and compliance verification of such post-sale software updates.[383]

b. Meaningful Participation Requires Developing Technical Expertise Among Stakeholders

Meaningful participation in design debates further requires resources and strategies to bolster the uneven technological expertise among stakeholders. Governance through design should occur in venues where government and civil society organizations that represent human rights, consumer interests, and other public goods have in-house technical capacity or external trustworthy technical advisors. These groups frequently lack the expertise to participate in complex technological and scientific agency processes. Without that expertise, they may miss risks posed by techno-regulation or be unable to formulate appropriate solutions.

Charitable foundations have recognized the need for human rights and civil liberties organizations to increase their technological expertise.[384] In response, they have funded fellowships,[385] supported technological consultants,[386] and invested in university-based centers to help cultivate publicly minded technologists and produce research at the intersection of technology and human rights.[387] Though important, foundation activity is not a long-term remedy for the expertise gap.

---

381. *Id.* at 76–77.

382. *See, e.g.*, PASQUALE, *supra* note 37 (describing the growing importance of secrecy in large financial and Internet companies). *But see* Kroll et al., *supra* note 377, at 633 (arguing that disclosure of code is neither necessary nor sufficient to demonstrate the fairness of an algorithmic process).

383. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 371, at 76–77.

384. FREEDMAN CONSULTING, A PIVOTAL MOMENT: DEVELOPING A NEW GENERATION OF TECHNOLOGISTS FOR THE PUBLIC INTEREST 1–4 (2016), https://netgainpartnership.org/wp-content/uploads/2016/02/pivotalmoment.pdf [https://perma.cc/M5AJ-9MTJ] (noting the creation of Netgain, a partnership between several foundations to respond to technological transformations).

385. *See id.* at 45 (describing Ford-Mozilla Open Web Fellowships).

386. *See id.* at 54–55 (describing Citizen Engagement Laboratory and DataKind).

387. *See, e.g.*, *About the Citizen Lab*, U. TORONTO, https://citizenlab.ca/about [https://perma.cc/P2PZ-2U9A] (describing an interdisciplinary laboratory focusing on research and development at the intersection of information and communication technologies, human rights, and global security); *Tech Policy Lab*, U. WASH., http://techpolicylab.org [https://perma.cc/8SYZ-TWD9]

Rather, to promote meaningful participation, agencies themselves must also fund consultant experts or help develop internal expertise in stakeholder groups. In some contexts, regulators have developed models for assisting stakeholder groups by funding their participation and acquisition of expertise or by directly providing expert assistance.[388] The California Public Utilities Commission (CPUC), for example, has an Intervenor Compensation Program and Public Advisor for hiring technical experts and providing funding to assist members of the public wishing to participate in proceedings.[389] The European Commission funds the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC), which enables nonprofit consumer organizations to participate in standard setting, policymaking, and legislation that affect European consumers.[390] Several U.S. environmental statutes provide for grants to nonprofit citizen groups to acquire independent technical assistance and to distribute their analyses to other stakeholders.[391] These efforts must be expanded in any context in which regulators contemplate governing by design.

2. Making "Transparency" Meaningful for the Design Context

a. Meaningful Transparency Must Involve "Political Visibility": Publicity About the Existence and Political Nature of Questions Being Resolved by Design Choices

To be meaningful in the governance-by-design context, decisional transparency must involve not only openness about design but also "political visibility"—that is, publicity about the very existence and political nature of values questions being resolved by design choices.

Debates about what values to reflect in traditional law and regulation, and how, render visible the political nature of the deliberations. While there may exist a jurisprudential hierarchy of values that distinguishes, for example, between values characterized as "constitutional"—and therefore more durable—

(describing interdisciplinary collaboration to enhance technology policy); *Center on Privacy & Technology*, GEO. L. CTR., https://www.law.georgetown.edu/academics/centers-institutes/privacy-technology [https://perma.cc/DDT4-A545] (describing a think tank focused on privacy and surveillance law and policy).

388. *See* Doty & Mulligan, *supra* note 68, at 163 (describing methods of addressing uneven participation by different stakeholders in the privacy context).

389. *CPUC Public Advisor's Office*, CAL. PUB. UTIL. COMM'N, http://www.cpuc.ca.gov/pao [https://perma.cc/J4RZ-MS2C] (last updated May 24, 2012). Funding under the Intervenor Compensation program is limited to organizations or individuals that represent the interest of customers. *The Intervenor Compensation Program*, CAL. PUB. UTIL. COMM'N (Apr. 2017), http://www.cpuc.ca.gov/icomp [https://perma.cc/2RJQ-DHP4].

390. Decision No 1926/2006/EC of the European Parliament and of the Council Establishing a Programme of Community Action in the Field of Consumer Policy, 2006 O.J. (L 404) 39, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006D1926&from=EN [https://perma.cc/QN9S-ZMHM].

391. *See, e.g.*, National Environmental Policy Act, 42 U.S.C. § 4368 (1994); Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. § 9613(a) (1994).

and those more open to political contest, policymaking discourse renders visible the fact that decisions are being made, what those decisions are, and why they are being made. This discursive visibility comprises a foundation for governance legitimacy; as regulation scholar Roger Brownsword describes:

> [W]hatever our particular conceptual understanding of law, it is a normative phenomenon that we are trying to frame. As formal high law shades into regulation and governance, even into ethics and morals, it remains normative. The enterprise is still one, as Lon Fuller famously expressed it, of seeking to subject human conduct to the governance of rules.[392]

Indeed, our system of public governance is structured along the principle that administrative legitimacy is predicated on the explicit public articulation of values choices that are being considered and deliberation about their resolution.[393]

By contrast, Brownsword continues, "[o]ne of the concepts that seems to be lost in the translation from a traditional legal order to a technologically managed order, is normativity."[394] While law explicitly discusses ought and ought not, the choices that technology permits, or does not permit, are experienced as can and cannot.[395] Regulative, or normative, features of technology design can appear "constitutive"—nonnormative and part of the natural state of things.[396] Embedding values in the technological architecture is "less visible as law, not only because it can be surreptitiously embedded into settings or equipment but also because its enforcement is less public."[397]

Thus, the very fact that technology embodies normative choices can escape notice. The perfect constraints that code places on behavioral possibility can seem as natural, immutable, and invisible as the laws of physics. The "moral register"—the fact that value choices are the core of regulation—is lost. This loss obscures the moral implications of default design practices[398] and conceals the

392. Roger Brownsword, *Lost in Translation: Legality, Regulatory Margins, and Technological Management*, 26 BERKELEY TECH. L.J. 1321, 1322 (2011) (citing LON L. FULLER, THE MORALITY OF LAW 96 (1969)).

393. *See, e.g.*, Auto. Parts & Accessories Ass'n v. Boyd, 407 F.2d 330, 338 (D.C. Cir. 1968) (noting that an agency rulemaking record must make visible "what major issues of policy were ventilated" and "why the agency reacted to them as it did").

394. Brownsword, *supra* note 392, at 1324.

395. *See id.* at 1322, 1324.

396. Mireille Hildebrandt, *Legal and Technological Normativity: More (and Less) Than Twin Sisters*, 12 TECHNÉ 169, 179 (2008).

397. Lee Tien, *Architectural Regulation and the Evolution of Social Norms*, 7 YALE J.L. & TECH. 1, 22 (2004).

398. *See* Philip Brey, *Disclosive Computer Ethics*, 30 COMPUTERS & SOC'Y 10, 11 (2000) (explaining that design practices can be morally "opaque," in that they have implications for values but are not recognized as controversial, because "[t]he hardware, software, techniques and procedures used in computing practice often has the appearance of *moral neutrality* when in fact they are not morally neutral").

role of powerful institutions and stakeholders, public or private, that shape those choices.[399]

An example from automobile-safety regulation demonstrates the complicated way in which the invisibility or visibility of a technical intervention can alter whether or not it is perceived as a political choice. Attempts to require automobile manufacturers to install ignition interlocks, which disable cars unless seats belts are enabled, were met with criticism and faced both marketplace and political rejection.[400] The literal visibility of the technological decision revealed the political decision underlying it: drivers did not like being disciplined by their car or the "nanny state." They found ways to disable ignition locks and Congress eventually prohibited, as one member called them "[o]ne of the most offensive invasions of the personal right of privacy to be dictated by the federal bureaucracy in recent years."[401] By contrast, the requirement that automobiles and lightweight-vehicle manufacturers include airbags, a technology that is literally invisible to drivers, met with less public resistance.[402] Although both technologies built safety into cars and overrode a driver's desires if they were inconsistent with governmental goals, airbags, unlike ignition locks, did not make their politics legible—a particularly ironic outcome, as the technology would later be taken to task for favoring the safety of men at the expense of children and smaller women.

Given technology's ability to fade into the background and hide the political nature of its design, relying on ex post oversight diminishes the likelihood that value impositions and value trade-offs will be recognized and assessed as governance. Furthermore, even where techno-regulation is visible and produces an outcome equivalent to traditional legal measures, a recent study found that individuals were less likely to hold regulators responsible for failed nudges than failed laws, because they perceive nudges as less coercive.[403] This suggests that even where the politics of techno-regulation are formally visible, the public may be less likely to hold government accountable, because it perceives such regulation as less heavy handed. Whether techno-regulations

399. *See* GERALD SUSSMAN, COMMUNICATION, TECHNOLOGY, AND POLITICS IN THE INFORMATION AGE 27 (1997) ("The grammar of technological determinism [is employed] precisely to disguise the political economic and repressive aspects and identities of empowered institutions and qinterests acting through their technocratic instruments.").

400. Jameson M. Wetmore, *Delegating to the Automobile: Experimenting with Automotive Restraints in the 1970s*, 56 TECH. & CULTURE 440, 453–55 (2015).

401. 120 CONG. REC. 11790 (1974), https://www.govinfo.gov/content/pkg/GPO-CRECB-1974-pt9/pdf/GPO-CRECB-1974-pt9-3-3.pdf [https://perma.cc/3KDD-3957].

402. *See* Wetmore, *supra* note 400, at 456–57 (discussing political resistance to safety technology that "disciplined drivers"). Airbags did meet some public resistance due to deaths of children and smaller statured women who were crushed by them; however, the resistance led to modifications in the airbags, not the massive public resistance observed with ignition locks. *See* Jameson M. Wetmore, *Redefining Risks and Redistributing Responsibilities: Building Networks to Increase Automobile Safety*, 29 SCI., TECH., & HUM. VALUES 377, 396–97 (2004).

403. Hill, *supra* note 134.

operate seamlessly and avoid notice, or operate in plain sight, there is a fundamental disconnect between retrospective oversight and political accountability.

This invisibility risks both intentional and unintentional subversion of public values. It decreases awareness of collateral losses by making values contests appear impossible or irrelevant and reduces system users' understanding of about the value choices and assumptions embedded in the logic. This lack of visibility can promote private ordering in place of decisions made according to public law ideals. Moreover, pulling activities out of courts and other sites of contestation reduces the process of choosing among competing values to an automatic, private act—rather than a public act involving judgment and community. This further undermines understanding of the political nature of decisions.

A combination of both policy and design expertise is essential to assure political visibility. Such deliberations require a deep understanding of whether and how "control points" can be implemented within a design. Control points can determine the ability "to implement particular value sets of various stakeholders, define[] the business models that economic actors can base their business on and outline[] the spectrum for regulatory intervention that can (and needs to) be imposed on the system."[404]

Governance-by-design, therefore, must, in philosopher Julie Cohen's words, "target the qualities of seamlessness and opacity."[405] Processes must be exhaustively explicit, transparent, and public about the choices that exist, the range of values implicated, the nature of agreement and disagreement about them. Likewise, these processes should publicly clarify what choices command broad enough agreement—or are otherwise substantively legitimate—to embed in technology, while also helping to determine when technology should instead "accommodate a variable set of social values to be configured at run-time in different contexts."[406] In turn, they must be purposive about what choices are being made, what is understood about them, and what is not,[407] and must further address these choices visibly from design and implementation through "values in repair" decisions after a system is in use."[408]

---

404. Ian Brown, David D. Clark & Dirk Trossen, *Should Specific Values Be Embedded in the Internet Architecture?*, PROCEEDINGS OF THE RE-ARCHITECTING THE INTERNET WORKSHOP 4 (2010).

405. Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1928 (2013).

406. Brown et al., *supra* note 404, at 10.

407. *See EIFFEL Report: Starting the Discussion*, FUTURE INTERNET 4 (July 13, 2009), http://www.future-internet.eu/uploads/media/Report_TT2008.pdf [https://perma.cc/HR7Z-4656] ("The nature and impact of this choice . . . need to be made explicit as well as understood.").

408. Lara Houston, Steven J. Jackson, Daniela K. Rosner, Syed Ishtiaque Ahmed, Meg Young & Laewoo Kang, *Values in Repair*, PROCEEDINGS OF THE 2016 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1403 (2016) (noting that because moments of maintenance and repair are also moments when values can be contested, re-evaluated, and redesigned, values in design can be seen as an ongoing process, not just something done at the design stage).

b. Tools for Promoting Political Visibility

The governance-by-design process must use tools explicitly intended to surface values, since it is difficult to understand the value implications of a system from the outside. On the one hand, such a process must employ "Values-Impact-Assessment" tools that enhance deliberation and make it public, such as the Human Rights Impact Assessments mentioned earlier.[409] The process must further use values-surfacing tools in technical design, drawing on a range of approaches that provide clarity over the properties embedded in code, as well as its performance. Such tools include the use of formal methods during development and the use of various forms of testing such as black box and usability testing.

Yet even with access to the guts of a system (the code, the architecture), the policies and procedures that govern its use, and information about the context of use (demographics, physical environment), the values implications of design decisions may nonetheless remain obscured. Despite the promise of developments like the NTHSA's Autonomous Vehicle Policy discussed above, we have not adequately tackled the complicated issue of how to expose code and technical design to promote public participation in its development. The early and insistent calls for open code belie a naive belief that access to code itself will lay values bare. Access can support reviews and analysis by experts—including values impact assessments, security reviews, and various automated analyses—but sobering research suggests that relying on manual code reviews to address problems related to values would be folly.[410] The scholarly literature has, to be sure, reflected a more nuanced appreciation of the ways that public participation and oversight are hindered by the complexity of technical systems and the lack of expertise, as well as by legal protections and corporate practices. But the question of what to do when government uses or procures such technical systems to govern remains unresolved.

Opening up the code is insufficient to meet democratic norms of transparency and participation. The question of what should be opened up, and in what ways, remains a hotly disputed topic across a range of disciplines. While a robust answer to this question requires attention to the specifics of a given technology of regulation as well as more research and experimentation, there are some promising directions in both policymaking and scholarship.

Researchers have suggested renewed focus on computer science methods that provide greater assurance that code is functioning in accordance with public goals through the use of audit logs, various forms of software verification, and

409. *See supra* Part IV(C)(1)(c) and accompanying text.

410. Anne Edmundson et al., *An Empirical Study on the Effectiveness of Security Code Review*, *in* ENGINEERING SECURE SOFTWARE AND SYSTEMS: 5TH INTERNATIONAL SYMPOSIUM 197 (Jan Jürjens, Benjamin Livshits & Riccardo Scandariato eds., 2013) (describing an experiment where none of thirty developers manually reviewing code containing seven known vulnerabilities found all the vulnerabilities, regardless of experience).

formal models that support computationally expressible definitions of privacy, fairness, and other desired properties.[411] As calls for transparent or interpretable code are often instrumental in nature, scholars have begun to parse the motivations behind such calls more carefully and to consider what other tools might be available to serve the underlying objectives.[412]

As researchers search for ideal solutions for building algorithmic systems that adhere to policy goals and can be audited to assure it, regulators are articulating guidance about what users need to interact with such systems safely and fairly. For example, the SEC has issued advice aimed at helping consumers interact safely with robo-advisors, online algorithmic-based programs that provide discretionary asset management services to clients. Much of the guidance document is devoted to recommending disclosures about how the computational system and data behind the robo-advisor work. The disclosures are aimed not at creating transparency during the design process but rather at imparting knowledge during use. The SEC rules are provocative and facilitate thinking through the complicated question of what forms of information about algorithmic systems are required to keep techno-regulation in line with democratic ideals.

Machine learning algorithms, however, pose a different challenge. These algorithms are not designed on the front end like traditional expert systems, but rather designed and redesigned by the data itself. For this reason, democratic norms require information about the data used to train the algorithm, including how the data was cleaned and information about the data sets on which the algorithm will be used.

Additionally, the growing set of practices and data repositories aimed at supporting reproducible research—that is, research that can be cross-validated, or at least carefully interrogated—provides additional insight into what might be required to fully empower public participation. Victoria Stodden, a leader in this field, articulates three categories of reproducibility that relate to specific components of the scientific pipeline: empirical, statistical, and computational.[413]

Empirical reproducibility is concerned with the data. It not only requires disclosure about how data was gathered, acquired, and cleaned, but also typically includes releasing the data used in a research study.[414] (Exceptions are made when the release of data would violate privacy.) These practices are becoming increasingly standardized and provide useful models for the regulatory process.

411. Kroll, *supra* note 377, at 656–94.

412. *See, e.g.*, *Investor Bulletin: Robo-Advisers*, SEC (Feb. 23, 2017), https://www.sec.gov/oiea/investor-alerts-bulletins/ib_robo-advisers.html [https://perma.cc/3PC5-YLLS] (providing users with information on using robo-advisors rather than simply releasing the code).

413. *See* Victoria Stodden, *2014: What Scientific Idea is Ready for Retirement?*, EDGE (Oct. 21, 2017), https://www.edge.org/response-detail/25340 [https://perma.cc/U4UT-TUXF].

414. *Modern Challenges of Reproducibility: Introduction*, GITHUB, ropensci.github.io/reproducibility-guide/sections/introduction [https://perma.cc/LMS3-LUKP].

Statistical reproducibility is focused on insight into the process of the experiment. It requires researchers to disclose specifics about the procedures used and the salient decisions about research design made, such as the choice of statistical techniques and tests, modeling parameters, and threshold values. Here, too, guidelines and approaches from reproducible research may be quite helpful in forming approaches to address transparency and participation. The disclosure guidelines focused on statistical reproducibility provide interesting templates for the sorts of information that could be shared to root out biases and assumptions in techno-regulation design.

Lastly, computational reproducibility focuses on the consistency of the methodology. It requires researchers to disclose all relevant ingredients to reproduce the computation in question, including actual code (or implementation details), software and hardware specifications, and environment settings, used in the scientific discovery. While code disclosure is surely insufficient on its own and raises complicated policy questions in its own right, the overall approach fits well with the needs of regulatory processes by ensuring that the context of a system is understood.

While rich and insightful, literature on algorithmic interpretability and reproducible research is generally aimed at expert audiences. Fully surmounting the technological barriers to democratic processes, then, will require meaningful ways of providing this information to nonexpert audiences, because those parties best able to identify and reason about values often are not adept at reviewing code and architecture, while those best able to understand and reshape the system are often not adept at identifying its values implications.

Policy reforms may need to look to approaches developed by "critical design" research, which offers interesting tools and methods for engaging people in forward-looking thinking about values in the design of technical systems. "Values Sensitive Design" can invite thinking about how a technology's use may evolve over time, be used by other populations, or be used in unexpected or troubling ways.[415] Considering misuse and abuse naturally leads to considering how the range of values that technologies support relates to moral responsibility and culpability of those who design, own, and use the technology. Speculative design and design fiction may help stakeholders imagine and reckon with future and problematic developments through intentional provocation or subversion of values and expectations.[416] Other tools, such as simulations, prototypes, storyboards, and other visual representations, can assist stakeholders. Scenario planning may be particularly useful when there is a need to think about possible

415. *See* Lisa P. Nathan, Batya Friedman, Predrag Klasnja, Shaun K. Kane & Jessica K. Miller, *Envisioning Systemic Effects on Persons and Society Throughout Interactive System Design*, PROCEEDINGS OF THE 7TH ACM CONFERENCE ON DESIGNING INTERACTIVE SYSTEMS 1 (2008).

416. Richmond Y. Wong & Deirdre K. Mulligan, *When a Product Is Still Fictional: Anticipating and Speculating Futures Through Concept Videos*, PROCEEDINGS OF THE 2016 ACM CONFERENCE ON DESIGNING INTERACTIVE SYSTEMS 121 (2016).

futures in a collaborative and explicit manner. Design tools and methods show promise as profitable avenues for bolstering stakeholders' capacity to identify risks to values and to iterate on solutions that could span technology, policy, and norm development.[417] Deep commitment and significant research will be required to imagine the ways that important and complex technical systems can be exposed to the public in ways that foster democratic regulation.

CONCLUSION

The rules of engagement for governance-by-design create an architecture for avoiding the dysfunction that has accompanied the move towards regulating through technology. With every battle over which values should be embedded in the coercive and enduring command of code, policymaking is unmoored from its traditional grounding in processes and institutions governed by public norms of rationality, deliberation, expertise, accountability, transparency, and participation. Governance-by-design war has resulted instead in tunnel vision, overbroad fixes, and unintended consequences—including the eclipsing of rights and the privatization of political decisionmaking.

Together, the rules of engagement offer a means for saving governance-by-design. Specifically, they offer a framework for reviving important governance norms in an age where technology functions as an increasingly important regulatory modality. In their insistence on modesty and flexibility in design, priority for human and public rights, and the development of institutions and processes that embrace participation, transparency, and publicness, these rules draw on tools and insights developed within engineering itself and use those insights to translate core normative commitments to the digital age.

The resulting framework thus addresses the challenge of regulating with technology framed by Laurence Tribe in a prescient analysis from forty-five years ago, the power of which we can only now broadly comprehend.

> [T]he very fact that law may more and more often be confronted with a widely-felt need on the part of legislators to control what people wish to do themselves will mean that the central legal role of such concepts as intelligent consent, voluntary choice and individual freedom may diminish as contemporary technology comes increasingly to operate directly on man himself. . . . To the extent that a kind of Faustian temptation beckons twentieth century man toward this Huxleyan dystopia, he may find it necessary to turn for protection to the increasingly authoritarian use of governmental regulation. Perhaps his hardest task will then be to avoid the trap of Big Brother as he resists the call of Brave New World. [418]

417. *Id.*

418. Laurence H. Tribe, *Legal Frameworks for the Assessment and Control of Technology*, 9 MINERVA 243, 255 (1971).

The proposed new rules of engagement seek to avoid that trap by ensuring that core governance values are preserved. We must use the newest tool in the chest to protect the values we cherish. Attractive as it may be to leverage technologies in values work, policy makers and stakeholders should proceed with caution and restraint, aided by a framework that helps them make better choices. Our rules of engagement are constructed to best support democratic "flourishing"[419] in the technological age through updated democratic processes that appreciate the opportunities and risks of governing through technology.

419. COHEN, *supra* note 264, at 6.