SOFT LAW IN U.S. ICT SECTORS: FOUR CASE STUDIES

Adam Thierer*

ABSTRACT: Traditional hard law tools and processes are struggling to keep up with the rapid pace of innovation in many emerging technologies sectors. As a result, policymakers in the United States rely increasingly on less formal "soft law" governance mechanisms to address concerns surrounding many newer technologies. This Article explores four case studies from different information technology areas where soft law mechanisms have already been utilized to address governance concerns. These four sectoral case studies include domain name management, content oversight, privacy policy, and cybersecurity matters. After considering the various soft law mechanisms used to address those issues, the Article concludes with some general thoughts about the effectiveness of those approaches and what lessons those case studies might hold for the use of soft law in other emerging technology sectors and contexts.

CITATION: Adam Thierer, *Soft Law in U.S. ICT Sectors: Four Case Studies*, 61 JURIMETRICS J. 79–119 (2020).

Historical ages or eras are often defined by the technologies or technological processes that shaped them—from Stone to Iron Age, from agricultural to industrial era. The period we are living in today has already been referred to as the information age, the internet era, and the digital economy.[1] Regardless of which moniker future historians eventually affix to our current era, information and communications technology (ICT) will likely be at the center of it because of its importance to recent economic, social, and political developments. The impact of these technologies has made their governance a major concern for society over the past century. ICT governance has been undergoing a major metamorphosis, however, especially during the past quarter century. This Article explores how many of the traditional "hard law" mechanisms used to govern ICT have been giving way to a diverse array of "soft law" governance approaches. It also offers a few explanations for why this transition has been occurring.

That discussion leads into an exploration of several case studies from different ICT sectors, including domain name management, content oversight, privacy policy, and network security matters. The Article concludes with some general lessons about soft law governance tools and methods that are drawn from those experiences. The case studies and the corresponding lessons make it

*Senior Research Fellow at the Mercatus Center at George Mason University.

1. MANUEL CASTELLS, THE INFORMATION AGE: ECONOMY, SOCIETY AND CULTURE 20 (2d ed. 2000); DON TAPSCOTT, THE DIGITAL ECONOMY: PROMISE AND PERIL IN THE AGE OF NETWORKED INTELLIGENCE 6 (1996).

clear that soft law represents the new norm for ICT governance, at least within the United States, which is the primary focus of this brief history.[2]

I. SOFT LAW, BRIEFLY DEFINED

Hard law represents legal and regulatory governance mechanisms that are (1) formally promulgated, (2) in accordance with accepted procedures, and (3) binding in character. Importantly, hard law includes formal efforts both to impose new restrictions and to remove them. Deregulation and agency downsizing, for example, represent hard law enactments even though they remove previously enacted rules. However, most hard law takes the form of new laws, regulations, or treaties that impose some sort of formal limits on economic or social behavior and include clear penalties for noncompliance. Hard law rulemaking procedures are standardized and typically require hearings, a notice-and-comment process, cost-benefit analysis, and other formal requirements. These procedures are guided by the Administrative Procedure Act (APA) and other laws.

By contrast, soft law represents a more amorphous, less formal, and constantly evolving set of governance mechanisms that lack the same degree of enforceability or "bindingness" of hard law. Soft law scholars tend to agree that the term "has no precise technical meaning and its definition is contested."[3] It makes more sense to view soft law "as part of a continuum"[4] that includes a wide range of ever-changing governance options. Some of those soft law governance mechanisms or approaches include the following:

- agency guidance documents;
- agency workshops and workshop reports;
- informal consultations between government and nongovernmental actors;
- "sandboxes" or special trial-run approaches to alternative regulatory arrangements (which can also include geographically defined innovation zones[5]);
- multistakeholder processes;
- the formation of best practices and voluntary codes of conduct (either for organizations or individual practitioners), often formulated through multistakeholder processes;
- industry standards, certifications, and self-regulation; and

2. Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 129 (2018).

3. Kenneth W. Abbott et al., *Soft Law Oversight Mechanisms for Nanotechnology*, 52 JURIMETRICS J. 279, 285 (2012).

4. *Id.* at 286.

5. See, for example, the FCC's recently announced innovation zones for testing 5G wireless network test beds. News Release, Fed. Commc'n. Comm'n, FCC Establishes First Two Innovation Zones (Sept. 28, 2019), https://docs.fcc.gov/public/attachments/DOC-359737A1.pdf [https://perma.cc/D79G-EE2K] ("Under this initiative, parties have flexibility to conduct multiple non-related experiments under a single authorization within a defined geographic area to develop new technologies and services while protecting incumbent services against harmful interference. This initiative allows experimental program license holders which are licensed to operate elsewhere to also use the New York City and Salt Lake City Innovation Zones.").

- education and awareness-building efforts.

Many of these soft law methods and processes are used in conjunction with hard law methods, or they gain their legitimacy from the fact that government authorities initiate or guide them in some fashion. Indeed, soft law frequently develops in the shadow of hard law and takes its cues from traditional statutory directives or regulatory priorities.

But soft law also can transcend hard law by tapping a broader and more flexible collection of governance approaches.[6] Whereas hard law tends to be top-down and technocratic in character, soft law is more bottom-up and multidimensional. "Soft law approaches provide key benefits in their adaptability and capacity to respond swiftly to new information about the regulated products or associated risks," argues Walter G. Johnson.[7] Furthermore, he states: "The extra degrees of freedom offered by nontraditional regulation further enables innovation in the governance tools selected, created, or combined."[8] As Johnson summarizes, most scholars studying soft law mechanisms repeatedly stress how *speed* and *flexibility* represent its primary advantages over hard law mechanisms.[9]

It is a mistake to believe hard law versus soft law represents an either-or choice. They are more symbiotic. For many soft law governance models, it is often said that "[g]overnment steers and industry rows."[10] Other phrases for this sort of coregulatory approach are "conditioned self-regulation" and "regulated self-regulation."[11] In this sense, governmental officials or bodies push for the development of governance mechanisms outside traditional legal channels and provide some guidelines for a process, but then leave it to industry and other stakeholders to flesh out the details through ongoing negotiations. This is particularly true for multistakeholder processes.

Indeed, among modern soft law tools and approaches, multistakeholderism has emerged as the most important and widely used governance mechanism for ICT over the past quarter century. Former U.S. Department of Commerce officials Lawrence E. Strickling and Jonah Force Hill, who were responsible for

---

6. Laurens Landeweerd et al., *Reflections on Different Governance Styles in Regulating Science: A Contribution to 'Responsible Research and Innovation*,' LIFE SCIS. SOC'Y & POL'Y, Aug. 2015, at 1, 17–18, https://doi.org/10.1186/s40504-015-0026-y (then follow hyperlink to download PDF) ("[S]ee the emergence of new, more hybrid styles of governance, in which the role of expert knowledge is explicitly acknowledged, but the range of relevant forms of expertise is broadened . . . .").

7. Walter G. Johnson, Comment, *Governance Tools for the Second Quantum Revolution*, 59 JURIMETRICS J. 487, 505 (2019).

8. *Id.* at 506.

9. *Id.* at 505.

10. Adam Thierer, *Reflections on Brussels Summit on Future of Free Expression / Child Protection*, TECH. LIBERATION FRONT (June 16, 2006), https://techliberation.com/2006/06/16/reflections-on-brussels-summit-on-future-of-free-expression-child-protection [https://perma.cc/8X24-8LUF]; Howard Fienberg, *New FTC Data Privacy Report Poses Challenges to Marketing Research*, INSIGHTS ASS'N BLOG (Mar. 26, 2012), https://www.insightsassociation.org/article/new-ftc-data-privacy-report-poses-challenges-marketing-research [https://perma.cc/DP4M-2893].

11. Thierer, *supra* note 10.

convening many multistakeholder processes during the Obama administration (some discussed below), have documented how these approaches are remarkably varied.

> They encompass a range of procedures, formats, resolution mechanisms, and outcomes. In the same way that democratic governments may follow a parliamentary or a presidential system of governance, so too do multi-stakeholder approaches vary and adapt to fit the particular governance question at hand. Some models lead to decisions whilst others are merely deliberative; some have established membership rules and criteria, whilst others allow anyone to participate; and some models are intended to last decades whilst others are one-off processes designed to address a specific challenge of the day.[12]

As with efforts to define soft law more generally, "there is no agreed-upon definition of 'multi-stakeholder governance,'" Strickland and Hill note.[13] Multistakeholderism is not a philosophy in and of itself. Rather, it represents a sort of governance disposition and range of governance alternatives, they observe.[14] It is meant to be an open, transparent, inclusive, stakeholder-driven process that seeks to build broad-based consensus.[15] As will be noted in the case studies that follow, a crucial feature of multistakeholderism and most other recent soft law processes is the effort to "bake in" important values and safeguards into technological design processes before or as innovations are introduced. For example, it is common to hear participants in soft law efforts stress the need for privacy by design, safety by design, and security by design.[16] This is often accomplished through ongoing meetings, conferences, negotiations, reports, and guidance documents, in which stakeholders negotiate and agree to a variety of best practices.

When formal, government-led multistakeholder efforts are also part of this process, these best practices can be formalized into agreements that industry representatives sign onto in some fashion. This represents an effort to introduce what some scholars refer to as "anticipatory ethics" in the early stages of technological development cycles, but without completely interrupting the innovative process in the same way precautionary hard law enactments might.[17]

In practice, things do not always work out as neatly as implied here. By its very nature, soft law lacks precision and formality. But, again, it is also more flexible and adaptive. While many tradeoffs are at work, the relative success of soft law in any context must always be judged against the alternative—which in many cases may be no governance scheme whatsoever. New marketplace and

---

12. Lawrence E. Strickling & Jonah Force Hill, *Multi-Stakeholder Internet Governance: Successes and Opportunities*, 2 J. CYBER POL'Y 296, 298–99 (2017).

13. *Id.* at 299.

14. *Id.* at 298–99.

15. *Id.* at 300; *see also* Jean-Jacques Sahel, *Multi-Stakeholder Governance: A Necessity and a Challenge for Global Governance in the Twenty-First Century*, 1 J. CYBER POL'Y 157, 162 (2016).

16. *See generally* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 (2011).

17. Deborah G. Johnson, *Software Agents, Anticipatory Ethics, and Accountability*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 61, 64 (Gary E. Marchant et al. eds., 2011) [hereinafter THE GROWING GAP].

social realities make traditional hard law governance efforts more difficult to formulate or less effective in practice. This has opened the door to soft law alternatives as second-best solutions that can at least produce *some* governance vision, tools, or guidelines for ICT.

II. WHY HARD LAW HAS FADED FOR ICT

As the internet and digital technologies began challenging social, economic, and technical norms a quarter century ago, hard law governance tools struggled to cope. This forced governments to reconsider their governance approaches for ICT.

Take a few steps back in time and consider how ICT sectors were governed prior to 1990. Before the rise of the internet, data networks, digitalization, and personal computing, ICT governance focused primarily on analog-based methods of communications (circuit-switched telephony, radio and television broadcasting, cable and satellite systems, etc.) and to a lesser extent, on consumer electronics and mainframe computing. ICT governance in the analog era was highly technocratic. ICT sectors tended to be fairly concentrated, often by design, as public policy sought to control outcomes for a handful of regulated monopolies at the national, regional, or municipal level.

Governance during this period typically took the form of formal statutes and administrative regulations that were top-down and quite rigid in character.[18] The dominant regulatory mechanisms of the past included operating licenses and line-of-business restrictions, price controls and rate-of-return regulation, technical device and equipment regulations, and various quality-of-service or access requirements. In a word, *centralization* was the norm for ICT sectors and the laws that governed them during the analog era.

The growth of the internet and digital technologies challenged these longstanding marketplace and legal realities. The new norm became technological *decentralization*.[19] Accordingly, ICT governance would also need to become more decentralized.

In some cases, regulators took steps that facilitated the move toward soft law for emerging sectors, often by simply creating a firewall between older (more regulated) sectors and newer ones. For example, in the late 1960s and early 1970s, the Federal Communications Commission (FCC) implemented three major proceedings that came to be known as the *Computer Inquiries*.[20] The FCC recognized that computer technologies were being integrated within traditional communications systems, but that those new technologies did not fall

18. Landeweerd et al., *supra* note 6, at 5.

19. *See* Chris Dixon, *Why Decentralization Matters*, MEDIUM: ONEZERO (Feb. 18, 2018), https://medium.com/s/story/why-decentralization-matters-5e3f79f7638e [https://perma.cc/WXL9-GYCZ].

20. Reg. and Pol'y Probs. Presented by the Interdependence of Comput. and Commc'n Servs., *Notice of Inquiry*, 7 F.C.C.2d 11 (1967); *see also* Reg. and Pol'y Probs. Presented by the Interdependence of Comput. Commc'n Services, *Tentative Decision*, 28 F.C.C.2d 291 (1970) [hereinafter Computer I Tentative Decision]; Reg. and Pol'y Probs. Presented by the Interdependence of Comput. Commc'n Servs., *Final Decision*, 28 F.C.C.2d 267 (1971) [hereinafter Computer I Final Decision].

under the agency's traditional regulatory authority. The FCC (and state regulatory bodies) exercised regulatory control over "basic" communications services (on the grounds that they were monopolistic), but not more "enhanced" computer services, which were viewed as more competitive. Generally speaking, through its three *Computer Inquiries*, the FCC decided to keep things that way. If services were enhanced—or built on interactive information technologies and computerized services— then the agency would generally avoid applying traditional regulations meant for the traditional telecommunications systems. This dichotomy was later extended through the Telecommunications Act of 1996 and the Clinton administration's *Framework for Global Electronic Commerce*, discussed at greater length below. These decisions left open the question of how these newer enhanced computer and digital technologies and networks would be governed. Soft law filled that vacuum. Before explaining how it did, the balance of this section explains how the old ICT governance toolkit came under strain because of a variety of other interrelated factors.

A. The Intensifying Pacing Problem

The "pacing problem" refers to the inability of legal or regulatory regimes to keep adjusting to the intensifying pace of technological change.[21] It is one of the most commonly cited reasons for using soft law processes and multistakeholder arrangements.

Today's ICTs work in a symbiotic fashion, and "concurrent technological revolutions"[22] are taking place in which the building blocks of one technological process can simultaneously act as a catalyst for developments in many other fields, including sectors well beyond traditional ICT fields. The underlying technological drivers of these "revolutions"—microchips, sensors, wireless networking and geolocation capabilities, digital code, cloud computing, cryptography and anonymization tools, and more—are becoming faster, cheaper, more powerful, and easier to find and use.

As these technologies work together and their development accelerates, it is giving rise to "seismic innovation[s]" that often catch policymakers by surprise and challenge long-held assumptions underlying traditional regulatory regimes.[23] Consulting firm Deloitte notes, "New technologies that used to have

21. *See* Adam Thierer, *The Pacing Problem and the Future of Technology Regulation*, MERCATUS CTR.: THE BRIDGE (Aug. 8, 2018), https://www.mercatus.org/bridge/commentary/pacing-problem-and-future-technology-regulation [https://perma.cc/UQ9F-WU8W].

22. Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, *in* THE GROWING GAP, *supra* note 17, at 19, 19.

23. CRISTIE FORD, INNOVATION AND THE STATE: FINANCE, REGULATION, AND JUSTICE 167 (2017); *see* Strickling & Hill, *supra* note 12, at 302 ("[T]raditional governance organisations and regulatory mechanisms often cannot keep pace with the rapid technological changes that characterise the internet, nor can they effectively incorporate the views of the diversity of stakeholders necessary to develop innovative or equitable answers for technology policy questions.").

two-year cycle times now can become obsolete in six months, and the pace of change is not slowing."[24]

This is the supply side of the pacing problem. Important demand-side factors are also at work. As the public gains access to various new technologies (and becomes more reliant upon them), they come to expect that even more (and better) technological capabilities will be forthcoming.[25] Innovators have to move faster to meet those societal expectations, which means governance regimes need to be nimble and able to adapt more quickly as they do. Putting the proverbial technological genie back in the bottle will not be easy once the public has gained access to those new goods and services.[26] With the pacing problem becoming a dominant and undeniable reality across so many sectors today (ICT and otherwise), more flexible soft law governance methods have become essential.

B. Technological Convergence and Blurring Governance Boundaries

ICT has always been a broad umbrella term covering an assortment of sectors and technologies with ever-changing boundaries. This has created classification challenges for lawmakers and regulators and led to debates of an almost metaphysical nature. For example, what is a "telephone," "television," or "radio"? These terms had widely accepted definitions in ICT's analog era. But in an age of widespread technological convergence and rapid-fire combinatorial innovation, with new technologies multiplying and building on top of one another in the symbiotic fashion discussed above, those concepts evolved and blurred rapidly.[27] As a result, almost as soon as new ICT laws or regulations are enacted, they are confronted with new marketplace realities and technological changes that call into question legal classifications or regulatory distinctions—especially those formulated decades ago.

Nothing has shattered traditional regulatory norms quite like the rise of the smartphone. One device now incorporates dozens of different functions or applications that were previously quite distinct, such as photography, mapping, retail shopping, gaming, live video, and voice telephony. Regulating telephony was a more straightforward affair when a single phone line came into each home to connect a rotary-dial telephone—which was used exclusively to make voice calls. With the rise of the internet, IP-enabled communications, and the spread

24. SHRUPTI SHAH ET AL., THE REGULATOR OF TOMORROW: RULEMAKING AND ENFORCEMENT IN AN ERA OF EXPONENTIAL CHANGE 3 (2015), https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/Regulator-of-tomorrow_vFINAL.pdf [https://perma.cc/B2TV-UBQJ].

25. *See* Adam Thierer, *The Pacing Problem, the Collingridge Dilemma & Technological Determinism*, TECH. LIBERATION FRONT (Aug. 16, 2018), https://techliberation.com/2018/08/16/the-pacing-problem-the-collingridge-dilemma-technological-determinism [https://perma.cc/4QEF-FUEP].

26. FORD, *supra* note 23, at 19–20 ("There is no putting the genie of innovation back into her bottle, and nor would most of us actually want to.").

27. Hal R. Varian, *Computer Mediated Transactions*, 100 AM. ECON. REV. PAPERS & PROC. 1, 1 (2010).

of wireless networks and mobile phones, the traditional governance realities and corresponding regulatory tools have been weakened as smartphones continue to evolve more rapidly than the old rules.

Change continues. With the rise of blockchain technologies and even more decentralized crypto-networks, some predict that "the core internet services will likely be almost entirely rearchitected in the coming decades,"[28] meaning that the pacing problem could grow to become an even bigger governance challenge. Meanwhile, the continued growth of the internet of things (IoT)—the growing universe of internet-connected appliances—is placing added strain on hide-bound regulatory distinctions.[29] "Smart" fitness devices and "connected" clothing that can track one's movement and even one's heartbeat are just two examples of ICT applications that were never envisioned under traditional communications laws and regulations.

Because soft law is not boxed in by rigid preconceptions of what a particular technology or technological process is or entails, it is often more equipped to address these new marketplace realities. Soft law can adapt as technologies do. Hard law, by contrast, struggles to adapt as rapidly for the reasons stated next.

C. Legislative Dysfunctionalism and Agency Resource Constraints

As digital technologies have multiplied, the universe of potential policy concerns has also expanded considerably. Lawmakers in Congress and state legislatures struggle to keep up, due to the pacing problem discussed above as well as larger problems inherent to modern legislative and regulatory processes.

Policy-making processes move slowly because of constitutional, bureaucratic, and other legal constraints as well as the more rigid nature of traditional regulatory systems. Cristie Ford notes that the problem with "old-style Welfare State regulation" is that it is "a clumsy, blunt instrument for achieving regulatory objectives" due to its reliance upon "one-size-fits-all mandates, prohibitions, and penalties."[30] "Formal rulemaking is simply too time-consuming," other scholars note.[31]

Twenty years ago, Jonathan Rauch coined the term "demosclerosis" to describe the "government's progressive loss of the ability to adapt."[32] If anything, legislative and regulatory processes have slowed down even more since then.[33] Inadequate resources are also part of the problem, with Congress facing a complex, rapidly evolving set of technical issues but devoting only limited resources

28. Dixon, *supra* note 19.

29. *See generally* Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1 (2015).

30. FORD, *supra* note 23, at 83.

31. Mark D. Fenwick et al., *Regulation Tomorrow: What Happens When Technology Is Faster than the Law*? 6 AM. U. BUS. L. REV. 561, 572 (2017).

32. JONATHAN RAUCH, GOVERNMENT'S END: WHY WASHINGTON STOPPED WORKING 125 (1999).

33. Marchant, *supra* note 22, at 23.

to technical staff or studies to better understand these developments.[34] A recent Deloitte survey of U.S. Code reveals that 67 percent of federal regulations have never been updated and that 17 percent have only been updated once.[35] An August 2017 survey by the Congressional Management Foundation "found overwhelming majorities of senior congressional aides believe Congress is not equipped to execute its basic functions."[36]

Meanwhile, as noted previously, innovators and technologies continue to arise quickly while policymakers are still coming to grips with previous developments—thus creating a "competency trap."[37] With these problems in mind, academic articles and media reports about modern tech policy-making efforts frequently note that the law is unable to adequately address emerging technologies and their associated concerns.

One solution to these problems would be to liberalize old regulatory regimes and deregulate sectors that are experiencing faster technological change and added competition. In recent decades, however, deregulatory outcomes have become just as rare as efforts to expand the horizons of the regulatory state to take on new challenges. Following a brief wave of deregulatory efforts in the 1970s and 1980s, comprehensive regulatory reforms have largely stalled. The Trump administration attempted to slow the growth of new regulation, and was successful to some extent. But no major agency downsizings or targeted deregulations occurred after he came into office. There may be many reasons for this, but what matters for purposes of this inquiry is that hard law of a *deregulatory* nature has become stifled by the same factors and forces that frustrate hard law enactments of a *regulatory* nature.

Thus, while they no doubt find it frustrating, soft law alternatives may become a second-best alternative for supporters of deregulation. Once deregulation supporters and proponents of greater government oversight realize that hopes of comprehensive reform are less likely in today's legislative environment, they may embrace the role of soft law governance.

D. Globalization and Innovation Arbitrage

Increasingly interconnected global markets have also placed strains on some elements of traditional domestic regulatory mechanisms. Modern ICT

34. Marci Harris, *Congress vs. the "Pacing Problem[s]*,*"* MEDIUM (Aug. 21, 2019), https://medium.com/g21c/congress-vs-the-pacing-problem-s-a887e3ca953f [https://perma.cc/G6MV-65K4].

35. DANIEL BYLER ET AL., USING ADVANCED ANALYTICS TO DRIVE REGULATORY REFORM: UNDERSTANDING PRESIDENTIAL ORDERS ON REGULATION REFORM 6, 9 (2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-ps-using-advanced-analytics-to-drive-regulatory-reform.pdf [https://perma.cc/AEC4-F4FF].

36. Jeff Stein, *A Staff Survey Shows Just How Broken Congress Is*, VOX (Aug. 8, 2017, 11:50 AM), https://www.vox.com/policy-and-politics/2017/8/8/16112362/congress-survey-broken-yikes.

37. David Rejeski, *Public Policy on the Technological Frontier*, *in* THE GROWING GAP, *supra* note 17, at 47, 57 ("By the time they catch up, competitive forces have created the next competency trap vis-à-vis a new set of actors and technological realities.").

technologies "are truly global and call out for policy approaches that do not respect traditional national borders," argue Strickling and Hill.[38] This is because, with the rise of the internet and the continued growth of digital computing, the potential for rapid cross-border data flows expanded considerably.

Innovation arbitrage has become more prevalent in this environment.[39] Government policies that limit innovative activities often encourage firms to "offshore" their operations to jurisdictions with less onerous regulations. Richard Baldwin, author of *The Great Convergence*, notes modern ICT has spurred a "new globalization," which has "denationalized comparative advantage by redrawing the international boundaries of competitiveness."[40] As jurisdictional shopping intensifies, geographically limited hard law regimes will be put under further strain, potentially opening the door for more soft law efforts—especially those of a multistakeholder variety.

To reiterate, all the new developments and realities discussed in this section are interrelated, and they have been ushering in a new era of ICT governance. Put simply, policymakers no longer have the breathing room they once enjoyed to craft proactive regulatory policies for ICT. This does not mean that traditional hard law regimes or regulatory procedures are completely irrelevant. Statutes, rules, and agencies have, and will continue to play, a major role in the future of technological governance. It will likely be a very different role compared with the past, however.

III. HOW THE U.S. GOVERNMENT EMBRACED SOFT LAW

As the new realities described above began to take hold, a major governance shift for ICT sectors occurred in the mid-1990s in the United States. The first major development was the Clinton administration's decision to open the internet for commercial activity, which was followed by passage of the Telecommunications Act of 1996 (Telecom Act). The Telecom Act was notable because it was a mostly bipartisan affair, gaining support from a Republican-led Congress with input from the Clinton administration.

Importantly, the Telecom Act's regulatory provisions were mostly backward-looking. The law was preoccupied with older sectors and regulatory questions surrounding regulatory distinctions between local versus long-distance telephone service, cable and satellite television, and licensed broadcasters versus other audio and video providers. The internet and interactive services were generally just too new to yet be considered important enough to deserve as much regulatory attention as more well-established sectors and "essential" services.

---

38. Strickling & Hill, *supra* note 12, at 310.

39. Adam Thierer, *Innovation Arbitrage, Technological Civil Disobedience & Spontaneous Deregulation*, MEDIUM (Dec. 7, 2016), https://medium.com/tech-liberation/innovation-arbitrage-technological-civil-disobedience-spontaneous-deregulation-eb90da50f1e2#.zpwzhifty [https://perma.cc/SE2H-APP4].

40. RICHARD BALDWIN, THE GREAT CONVERGENCE: INFORMATION TECHNOLOGY AND THE NEW GLOBALIZATION 175 (2016).

However, the Telecom Act did include one particularly important new provision known as Section 230, which immunized online intermediaries from liability for the content and communications that traveled over their networks. The immunities granted by Section 230 left most online content determinations to digital platforms, who would not face punishing legal liability for third-party contributions posted to their sites.[41] Congress hoped that by granting platforms legal immunity, the platforms could take steps to self-moderate potentially objectionable content without fear of legal repercussions. Section 230 helped spawn today's diverse internet ecosystem,[42] but it also gave rise to a new form of governance for a great many forms of content. This is relevant for the case study below on content moderation, but it is also important because it represented a hard law enactment that generated greater reliance on soft law governance approaches. Incidentally, Section 230 has come under fire from Republicans and Democrats in recent years, and calls for reform to curb the law's sweeping scope are growing from both parties.[43] But, consistent with the themes running throughout this paper, most of these hard law reforms are not being finalized—at least not yet.

Regardless, the Telecom Act is the last truly comprehensive hard law enactment for ICT, at least to date. In 1997, the Clinton administration released its *Framework for Global Electronic Commerce*, which articulated the U.S. government's approach toward the internet and the digital economy.[44] For governance of the new ICT world, the *Framework* generally recommended reliance on civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experimentation.[45] Specifically, it said: "The private sector should lead.

---

41. Adam Thierer, *The Greatest of All Internet Laws Turns 15*, FORBES (May 8, 2011), http://www.forbes.com/sites/adamthierer/2011/05/08/the-greatest-of-all-internet-laws-turns-15 [https://perma.cc/839Q-LGSG].

42. David Post, *A Bit of Internet History, or How Two Members of Congress Helped Create a Trillion or So Dollars of Value*, WASH. POST: VOLOKH CONSPIRACY (Aug. 27, 2015, 10:05 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/27/a-bit-of-internet-history-or-how-two-members-of-congress-helped-create-a-trillion-or-so-dollars-of-value [https://perma.cc/9QUJ-QRPE] ("Yet it is impossible to imagine what the Internet ecosystem would look like today without it. Virtually every successful online venture that emerged after 1996—including all the usual suspects, viz. Google, Facebook, Tumblr, Twitter, Reddit, Craigslist, YouTube, Instagram, eBay, Amazon—relies in large part (or entirely) on content provided by their users, who number in the hundreds of millions, or billions.").

43. Matt Laslo, *The Fight Over Section 230—and the Internet as We Know It*, WIRED (Aug. 13, 2019), https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it [https://perma.cc/7NFH-ADVN]; Bobby Allyn, *As Trump Targets Twitter's Legal Shield, Experts Have a Warning*, NPR (May 30, 2020), https://www.npr.org/2020/05/30/865813960/as-trump-targets-twitters-legal-shield-experts-have-a-warning [https://perma.cc/56DK-QZJX]; Adam Thierer & Neil Chilson, *FCC's O'Rielly on First Amendment & Fairness Doctrine Dangers*, FED. SOC'Y BLOG (Aug. 6, 2020), https://fedsoc.org/commentary/fedsoc-blog/fcc-s-o-rielly-on-first-amendment-fairness-doctrine-dangers?linkId=96486156 [https://perma.cc/5DNB-D8UH].

44. *A Framework for Global Electronic Commerce*, CLINTONWHITEHOUSE4.ARCHIVES.GOV, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html [https://perma.cc/FT3K-XUT8].

45. Adam Thierer, *15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm*, FORBES (Feb. 12, 2012, 1:16 PM), http://www.forbes.com/sites/adamthierer/2012/

[And the] Internet should develop as a market driven arena, not a regulated industry."[46]

More importantly, the *Framework* signaled that soft law mechanisms would take on greater importance, asserting that "governments should encourage industry self-regulation and private sector leadership where possible" while "avoid[ing] undue restrictions on electronic commerce."[47] The document added that "parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention."[48] Furthermore, it stated: "Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."[49]

This represented a sea change in approach for the governance of ICT sectors, and the *Framework's* collaborative governance vision has been indicative of ICT policy in the United States ever since. These same principles have infused other governance frameworks, both domestically and abroad. In late 2011, the Organization for Economic Cooperation and Development (OECD) released a report, *Principles for Internet Policy Making*.[50] Three of the fourteen recommendations were to encourage multistakeholder cooperation in policy development processes, foster voluntarily developed codes of conduct, and encourage cooperation to promote internet security. The OECD's statement of principles reflected policy in the spirit of the modern internet era, which had become heavily focused on the facilitation of soft law solutions and multistakeholder processes. As noted in the case studies that follow, this commitment to multistakeholderism would be reinforced in the United States throughout the Obama administration and most recently during the Trump administration.

While soft law has always been with us, its moment in the spotlight has truly arrived. It has grown to be the first option instead of the last for many ICT governance matters, particularly in the United States, which is the focus of this review. An exploration of several case studies will help make this clear.

IV. CASE STUDY: DOMAIN NAME GOVERNANCE

During the heyday of over-the-air broadcasting and analog telephony, technical matters involving electromagnetic spectrum allocations or even the assignment of phone numbers involved rigid hard law processes that were administered by federal and state regulatory agencies in the United States, and by nationalized telecom monopolies in many foreign nations. Network access, interconnection, and pricing policies were particularly convoluted and contentious in this environment. Regulatory bodies opened proceedings, held many

---

02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm [https://perma.cc/JJ6T-5MWS].

46. *A Framework for Global Electronic Commerce*, *supra* note 44.

47. *Id.*

48. *Id.*

49. *Id.*

50. ORG. FOR ECON. COOP. & DEV., OECD RECOMMENDATION OF THE COUNCIL ON PRINCIPLES FOR INTERNET POLICY MAKING (2011), http://www.oecd.org/dataoecd/11/58/49258588.pdf [https://perma.cc/3CYU-P4CY].

hearings, received comments, and then, eventually, promulgated and enforced a set of rules. Court battles sometimes followed. Change came slowly if it came at all. Regulators had the luxury of taking their time when making these decisions because technological change was incremental and the major industry players did not change much from year to year.

That traditional regulatory approach was ill-suited for the internet and globally interconnected digital networks. As the world moved out of an age of information scarcity and into an era of information abundance, and as technologies and companies were evolving at a much more rapid clip, the way that technical networking standards were formulated and enforced also needed to evolve.

This became evident in the mid-1990s as management of the Domain Name System (DNS) became a pressing governance concern. The DNS is often conceptualized as the internet's phonebook, but it is actually more sophisticated than that analogy suggests. The DNS "provides a way of associating alphanumeric names, which are easier for humans to use, with the numerical addresses that designate every location on the Internet."[51] The DNS was created in the early 1980s when the internet was still a very limited, noncommercial community. It was meant to be "a simple and stable way for users and applications to identify computers on the Internet."[52] The DNS evolved rapidly in ensuing decades and continued to satisfy that original goal remarkably well.

Part of the reason it worked so well was that a broad community of individuals and organizations worked together to keep the system functioning while also constantly improving it. The sheer number of individuals and entities that have contributed to that goal is far too lengthy to itemize here, but some of the most important organizations included the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the Internet Governance Forum (IGF), the Internet Architecture Board (IAB), and the World Wide Web Consortium (W3C). These groups worked with governments, industry, civil society groups, university centers, and other interested parties to create technical standards for the internet in an iterative, collaborative fashion.

Day-to-day management of the DNS fell principally to the Internet Assigned Numbers Authority (IANA), which was managed originally by a handful of university-based computer scientists.[53] As the DNS grew, IANA's responsibilities grew alongside it, and eventually, IANA would receive U.S. government support.

In the late 1990s, following increased scrutiny of the internet and the DNS from the White House, the National Telecommunications and Information Administration (NTIA) helped chart a new process to transfer IANA functions to the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization headquartered in California. ICANN would become responsible for managing domain names, both globally and on an independent basis.

---

51. NAT'L RSCH. COUNCIL, SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEMS AND INTERNET NAVIGATION, at vii (2005).

52. *Id.* at 24.

53. KATIE HAFNER, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996); *see also* IANA, https://www.iana.org [https://perma.cc/A5D6-STRU].

But there was one important hitch: ICANN would continue to exercise ultimate control over the DNS "root zone," or the top-level domains like *.com* and *.org*, and it would do so with ongoing contractual oversight by the NTIA.

Importantly, however, the NTIA and the Clinton administration also envisioned a process whereby the U.S. government would completely hand off governance of the IANA functions to ICANN, as stated in a 1998 memorandum:

> The U.S. government recognizes that its unique role in the Internet domain name system should end as soon as is practical. We also recognize an obligation to end this involvement in a responsible manner that preserves the stability of the Internet. We cannot cede authority to any particular commercial interest or any specific coalition of interest groups. We also have a responsibility to oppose any efforts to fragment the Internet, as this would destroy one of the key factors—interoperability—that has made the Internet so successful.[54]

This NTIA memorandum kicked off a process that would eventually see technical management of the DNS fully transitioned to ICANN and managed privately without any U.S. government control. The formal transition used multistakeholder processes to work out details of the transition.[55]

This was an example of the "government steers and industry rows" model alluded to earlier, but in this case, it was the U.S. government prodding private industry in such a way that all future government steering would cease upon the successful transition of IANA functions to ICANN. After two years of multistakeholder meetings and negotiations involving a wide range of groups from across the globe, the IANA transition concluded on September 30, 2016, and the U.S. government's contract with ICANN expired.

The transition away from U.S. government oversight of the DNS exemplifies how soft law—and multistakeholder processes in particular—have become an important governance tool for the internet and for ICT policy making more generally. Strickling and Hill, who helped guide the IANA transition while working at the NTIA, argue that this process "was undoubtedly the largest, most complex, and most successful demonstration of the multi-stakeholder approach in history" and represented "an audacious experiment in global governance."[56]

Even critics of ICANN and the IANA transition admit that the transition process "was very transparent, and it was more open than traditional governmental and intergovernmental processes. Thus it is a good example of how multistakeholder processes can be used to discuss complex issues and arrive at widely supported conclusions."[57] The Internet Society argues that "the multi-

54. Improvement of Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826, 8832 (Feb. 20, 1998).

55. Press Release, Nat'l Telecomm. & Info. Admin., NTIA Announces Intent to Transition Key Internet Domain Name Functions (Mar. 14, 2014), https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions [https://perma.cc/YJ3M-FT4W].

56. Strickling & Hill, *supra* note 12, at 296, 297.

57. Richard Hill, *Internet Governance, Multi-stakeholder Models, and the IANA Transition: Shining Example or Dark Side?*, 1 J. CYBER POL'Y 176, 185 (2016).

stakeholder approach is widely accepted as the optimal way to make policy decisions for a globally distributed network" because "multistakeholder decision-making is accountable, sustainable and—above all—effective. The better the inputs and the more inclusive the process, the better the outputs and their implementation."[58]

Multistakeholderism is not without its critics in this or other contexts, however.[59] Some believe that the multistakeholder model is underinclusive or fails to build true democratic consensus, with some even referring to it as a "fiction, a romantic plot hoping for a happy ending."[60] Concerns about inclusion, representation, and consensus—both in terms of having all the appropriate stakeholders *and* various issues represented—have been particularly evident in global discussions about internet governance.[61] Moreover, individuals and organizations primarily focused on specific policy concerns—privacy, security, intellectual property protection, and so on—have often complained that those values are underappreciated in multistakeholder negotiations.[62]

Meanwhile, one of the great ironies of multistakeholder DNS governance is that ICANN is a private organization that has been given a monopoly over the root of the internet's naming system. ICANN's creation "represented a privatization of significant aspects of the global governance function," notes Milton Mueller, author of *Networks and States: The Global Politics of Internet Governance*.[63]

Although it is unclear how an alternative arrangement would have worked without raising serious functional challenges for global DNS management, concerns about ICANN's unique role and power remain. Under ICANN, DNS governance is likely to be less politicized than an alternative governance regime under the ITU, but that does not mean ICANN's decisions steer clear of all politicized international disputes. The United States and other nations advise ICANN through its Governmental Advisory Committee. For context, this Committee held up the assignment of the *.amazon* top-level domain to the American e-commerce company (rather than the geographic region of the Amazon basin) for several years. The governments of the United States and other nations advise ICANN through its Governmental Advisory Committee, which, for example, held up the assignment of the *.amazon* top-level domain to the American e-commerce

58. *Internet Governance—Why the Multistakeholder Approach Works*, INTERNET SOC'Y, (Apr. 26, 2016), https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works [https://perma.cc/7M7L-FPRK].

59. *See* Hill, *supra* note 57.

60. Jeanette Hofmann, *Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice*, 1 J. CYBER POL'Y, 29, 44 (2016).

61. *See* John B. Morris, *Injecting the Public Interest into Internet Standards*, *in* OPENING STANDARDS: THE GLOBAL POLITICS OF INTEROPERABILITY 3, 3–12 (Laura DeNardis ed., 2011).

62. *See* Hofmann, *supra* note 60, at 42.

63. MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 61 (Ernest J. Wilson III ed., 2010).

company (rather than the geographic region of the Amazon basin) for several years.[64]

Nonetheless, soft law, and multistakeholderism in particular, has worked surprisingly well for coordination issues concerning technical domain names. The very fact that such a global, fast-growing "network of networks" remains so open, interoperable, and reliable is a genuine achievement. Jonathan Zittrain of Harvard Law School has observed that the principle of mutual aid is often at work when technical internet governance matters are being addressed.[65] "Historically, the Internet domain has seen infrastructural advances not through carefully planned interventions forged self-consciously at any given moment among stakeholders participating in a worldwide summit, but rather through an open architecture that allows ideas to be floated for general adoption," Zittrain argues.[66] This mutual aid principle has been at work since the internet's earliest days, and this principle came to infuse a variety of other governance processes and arrangements.

V. CASE STUDY: CONTENT MODERATION AND CHILD SAFETY

Content oversight is one of the oldest rationales for ICT governance. Even before the rise of the internet and digital platforms, soft law played a role in governing speech and content over older networks, oftentimes in an effort to protect children from content that some deemed objectionable. However, the use of soft law in this context was controversial, and that remains true today.

Since its inception as the Federal Radio Commission in 1927, the FCC has possessed broad "public interest" powers to police broadcast radio and television programming for obscene, indecent, or even profane content. Fines and license revocation are possible. This is obviously a hard law approach to content oversight and regulation. In practice, however, strict enforcement of those policies was rare. An obvious tension existed between such content controls and the First Amendment of the U.S. Constitution. Court battles often ensued whenever the agency sought to enforce its content regulations. As time passed and judicial scrutiny of content regulation grew more intense, courts gradually curtailed the FCC's enforcement powers.

For better or worse, the agency adapted to these enforcement limitations by tapping various soft law governance techniques, although they were not called that at the time. The FCC's preferred soft law approach was a combination of industry consultations, guidance documents, licensing transfer conditions, and "agency threats."

---

64. *See* Joi Ito, *It's OK That Amazon Will (Likely) Get the .amazon Domain*, WIRED (May 25, 2019), https://www.wired.com/story/its-ok-that-amazon-will-likely-get-amazon-domain [https://perma.cc/PQL7-YZP5].

65. Jonathan Zittrain, *A Mutual Aid Treaty for the Internet* 1, 5 (Brookings Inst., Future of the Const. Series No. 8, 2011), https://www.brookings.edu/wp-content/uploads/2016/06/0127_internet_treaty_zittrain.pdf [https://perma.cc/NE4M-6WLG].

66. *Id.* at 10.

The agency's use of letters of inquiry (LOIs)—letters sent to broadcast license holders inquiring about programming decisions—became an effective way to avoid First Amendment concerns and potential objections by the courts. These LOIs contained the implicit threat of license revocation should broadcasters not answer questions (or alter programming) to the FCC's satisfaction. This tactic was used so much that industry insiders came to refer to it as "regulation by raised eyebrow."[67] One scholar defined it as using "regulatory threats that cajole industry members into slight modifications" of their programming content.[68] These letters were "often sufficient to bring licensees' behaviors into compliance with FCC policies," another scholar concluded.[69] This was the case even though license revocation was extremely rare; the mere threat was often an effective way for the FCC to influence content decisions because license revocation constituted the equivalent of a regulatory death penalty for broadcasters.

In addition to LOIs, FCC commissioners would also engage in jawboning or "agency threats"[70] in speeches and other public statements, including talks at major events and industry conventions.[71] This jawboning strategy would sometimes also be used by members of Congress during congressional hearings on content-related matters. While the FCC's use of jawboning and agency threats in this context declined somewhat in recent years—mostly due to losses in major First Amendment cases—the agency has also used its authority to review license transfers (primarily in the context of merger and acquisition reviews) to extract various concessions from companies seeking the agency's blessing.[72]

The FCC also used guidance documents to explain its content enforcement policies, although sometimes it did not provide much useful clarification about what was and was not considered indecent content.[73] Language and behavior ruled indecent in one context was often found not to be indecent in another.[74]

---

67. THOMAS STREETER, SELLING THE AIR: A CRITIQUE OF THE POLICY OF COMMERCIAL BROADCASTING IN THE UNITED STATES 189 (1996).

68. *Id.*

69. PAUL SIEGEL, COMMUNICATION LAW IN AMERICA 404 (3d ed. 2011).

70. Jerry Brito, "*Agency Threats" and the Rule of Law: An Offer You Can't Refuse*, 37 HARV. J.L. & PUB. POL'Y 553 (2014).

71. KIMBERLY A. ZARKIN & MICHAEL J. ZARKIN, THE FEDERAL COMMUNICATIONS COMMISSION: FRONT LINES IN THE CULTURE AND REGULATION WARS 146 (2006) ("These 'suggestions' have often come in the form of speeches made by commissioners at the National Associations of Broadcasters annual convention.").

72. Brent Skorup & Christopher Koopman, *The FCC's Transaction Reviews and First Amendment Risks*, 39 HARV. J.L. & PUB. POL'Y 675, 677 (2016) ("Increasingly, the FCC extracts nominally voluntary concessions from firms—including programming decisions, hiring practices, and 'net neutrality' compliance—via coercive conditions to transaction approvals. In many cases, the FCC is legally barred from enforcing or unwilling to enforce these policies through the normal regulatory process."); Bryan N. Tramont, *Too Much Power, Too Little Restraint: How the FCC Expands Its Reach Through Unenforceable and Unwieldy 'Voluntary' Agreements*, 53 FED. COMM. L.J. 49 (2000).

73. *See* Industry Guidance on the Commission's Case Law Interpreting 18 U.S.C. 1464 and Enforcement Policies Regarding Broadcast Indecency, Policy Statement, 16 F.C.C.R. 7999, ¶ 1, 23 Comm. Reg. (P & F) 857 (2001).

74. Adam Thierer, *Why Regulate Broadcasting: Toward a Consistent First Amendment Standard for the Information Age*, 15 COMMLAW CONSPECTUS 431 (2007).

The use of guidance documents for these purposes has declined in recent years, however.

Nonetheless, the FCC and other agencies that oversee ICT activity, such as the Federal Trade Commission (FTC), still tap some of these same strategies today when taking advantage of modern social media platforms to communicate their concerns or questions to private parties in an attempt to alter their behavior. For example, FCC and FTC officials often use blog postings and social media messages to explain new agency decisions. Both agencies and individual commissioners increasingly also use Twitter to expound upon their policy objectives. In the process, they often lean on industry and others to change their behavior in various ways.

In 2011, the U.S. Government Accountability Office began identifying how "federal agencies have been adapting commercially provided social media technologies to support their missions," including Facebook, Twitter, and YouTube.[75] It also stated: "These include reposting information available on official agency Web sites, posting information not otherwise available on agency Web sites, soliciting comments from the public, responding to comments on posted content, and providing links to non-government sites."[76]

The use of social media by agencies and agency officials has only expanded since then. What makes this notable is that the postings agencies make on social media are essentially the least formal of the various types of informal guidance techniques that agencies use. The effect of such social media–enabled soft law approaches remains unclear, but it seems likely to grow. Some analysts fear that social media guidance could become a form of "stealth regulation" that avoids the accountability and transparency requirements associated with the Administrative Procedure Act and other formal rulemaking procedures.[77] Nonetheless, these practices represent a major new frontier in soft law policy making.

Soft law has also played an important governance role for movies, video games, and social media platforms. In these cases, industry self-regulation became the dominant soft law governance approach after various others schemes failed. For motion pictures, the familiar rating system of the Motion Picture Association of America (MPAA) is a self-regulatory content-labeling scheme that has been enforced by the movie industry and theater operators since 1968. MPAA ratings have expanded over time and are also accompanied by additional content descriptors explaining what viewers can expect to see in the movie.

The MPAA system replaced a very strict industry-enforced censorship regime known as the Hays Code, which tightly limited creative choices by

---

75. U.S. GOV'T ACCOUNTABILITY OFF., HIGHLIGHTS OF GAO-11-605: FEDERAL AGENCIES NEED POLICIES AND PROCEDURES FOR MANAGING AND PROTECTING INFORMATION THEY ACCESS AND DISSEMINATE 1 (June 2011), https://www.gao.gov/assets/330/320251.pdf [https://perma.cc/4KQP-Y2GW].

76. *Id.*

77. James Broughel, *The Hidden Dangers of Government Tweets—and Not Just Trump's*, FISCAL TIMES (Mar. 23, 2017), https://www.thefiscaltimes.com/Columns/2017/03/23/Hidden-Dangers-Government-Tweets-and-Not-Just-Trump-s [https://perma.cc/F7AB-69NW].

filmmakers to ensure content was "wholesome" and "moral."[78] While not formal regulation, the Hays Code was a highly restrictive effort meant to appease politicians and other critics of motion picture content, which included municipal censorship boards. The MPAA developed its rating system to allow more artistic freedom, but also more content transparency and choice for movie producers and the public. In essence, a restrictive form of self-regulatory soft law (a self-censorship code of conduct) was replaced by a more flexible form of soft law (content classification ratings plus voluntary labels and educational efforts).

Video game content labeling is another area where soft law has played an important role and, in some ways, followed in the footsteps of the movie industry. Almost as soon as video games began capturing the public's attention, parental concerns grew in response to gaming content that many deemed excessively violent for children.[79] Eventually, lawmakers began responding to these concerns with hearings and then legislative proposals aimed at limiting children's access to violently themed games.[80]

Video game developers and others concerned about free speech issues began working together to devise self-regulatory solutions to respond to pressure from federal and state lawmakers, who were pitching a variety of more formal restrictions on youth access to video games. The result was the 1994 formation of the Entertainment Software Rating Board (ESRB), a self-regulatory rating and labeling body for video game content. The ESRB content rating system was even more robust than the MPAA scheme for movies, with many additional content descriptors for game content.[81]

Importantly, enforcement of the ESRB rating system was facilitated by the willingness of leading video game console makers like Sony, Microsoft, and Nintendo. Those companies agreed to embed within their systems' metadata screening capabilities that let parents easily block games rated inappropriate for children under a certain age by the ESRB.[82] The ESRB also enforces self-regulatory advertising code of conduct and various privacy certification "seals" which are intended to demonstrate that participating companies adhere to certain best practices for web and mobile privacy.[83] Today, the ESRB soft law ratings scheme is the primary governance mechanism in this arena, especially after

78. Bob Mondello, *Remembering Hollywood's Hays Code, 40 Years On*, NPR (Aug. 8, 2008), https://www.npr.org/templates/story/story.php?storyId=93301189 [https://perma.cc/6JBK-A5W7].

79. Adam Thierer, *Confessions of a 'Vidiot': 50 Years of Video Games & Moral Panics*, BRIDGE (July 17, 2019), https://www.mercatus.org/bridge/commentary/confessions-vidiot [https://perma.cc/2SLH-65WG].

80. Tiffany Hsu, *When Mortal Kombat Came Under Congressional Scrutiny*, N.Y. TIMES (Mar. 8, 2018), https://www.nytimes.com/2018/03/08/business/video-games-violence.html [https://perma.cc/HJ7G-ST96].

81. Charlie Hall, *A Brief History of the ESRB Rating System*, POLYGON (Mar. 3, 2018, 12:00 PM), https://www.polygon.com/2018/3/3/17068788/esrb-ratings-changes-history-loot-boxes [https://perma.cc/KC5E-NMGK].

82. *Id.*

83. *Program Services*, ESRB.org, https://www.esrb.org/privacy/program-services/ [https://web.archive.org/web/20200228121247/https://www.esrb.org/privacy/program-services/].

state-based efforts aimed at regulating access to video games eventually lost in court battles that went all the way to the Supreme Court.[84]

While the effectiveness of MPAA and ESRB voluntary classification and rating schemes is still debated, those systems continue to evolve to cover a growing universe of movie and video game content. At least in terms of longevity, visibility, and adaptability, they have been relatively effective soft law governance schemes. The same is not true of internet content rating schemes that were developed partially in response to growing calls for online content regulation, primarily to limit underage access to adult materials.

In the mid-1990s, various online child protection laws were proposed or implemented, both in the United States and abroad. In the United States, Congress initially sought to bring the internet under the regulatory regime of the broadcast era through the Child Online Protection Act (COPA), which was later ruled to be unconstitutional. But this and other regulatory efforts led providers of major global information technology (Microsoft, AOL, British Telecom) and other parties to form the Internet Content Rating Association (ICRA) in 1999.[85]

ICRA did not rate internet websites or the content itself, but instead left it to the content providers to do so voluntarily, using the ICRA content classification system. These voluntarily imposed ICRA labels (affixed to web sites in the form of metadata tags) were then supposed to be screenable by web browsers according to user specifications.[86] ICRA also made a free internet filter available to the public that let users block content according to their desired specifications. At the same time, the World Wide Web Consortium was helping develop the Platform for Internet Content Selection (PICS), another metadata labeling and screening system. Launched in 1995, PICS attempted to make it easier for users to filter objectionable online content using various third-party rating services.[87]

ICRA and PICS floundered from the beginning due to the daunting complexity of the task at hand. While MPAA and ESRB voluntary content ratings proved fairly successful, the ICRA and PICS labeling schemes never gained traction and were eventually abandoned altogether. One reason for this failure relates to the scope of covered material. ICRA and PICS had the impossible task of getting voluntary ratings and screenable metadata tags associated with all internet pages globally. Few sites were willing or able to self-label their constantly

84. Adam Thierer, *Thoughts on SCOTUS Video Games Decision in Brown v. EMA*, TECH. LIBERATION FRONT (June 27, 2011), https://techliberation.com/2011/06/27/thoughts-on-scotus-video-games-decision-in-brown-v-ema [https://perma.cc/35BF-2SEF].

85. *Internet Content Rating Association Formed to Provide Global System for Protecting Children and Free Speech on the Internet*, MICROSOFT (May 12, 1999), https://news.microsoft.com/1999/05/12/internet-content-rating-association-formed-to-provide-global-system-for-protecting-children-and-free-speech-on-the-internet [https://perma.cc/V472-9BNP].

86. *About ICRA*, ICANN.ORG, https://www.icann.org/en/system/files/files/about-icra-05jan07-en.pdf [https://perma.cc/X73P-8SE3].

87. *PICS Frequently Asked Questions (FAQ)*, W3C (Jan. 2, 2003), https://www.w3.org/2000/03/PICS-FAQ [https://perma.cc/B4DT-S8AN].

changing web pages.[88] There were also definitional challenges that made classification difficult. By contrast, MPAA and ESRB had far more focused missions. Those organizations only sought to rate "professional" movies and video games, respectively, which constituted a far smaller universe of content relative to all internet websites and content.

Moreover, once MPAA and ESRB rated content, they only needed buy-in from major movie and game distributors to make sure their respective rating systems were enforced. Theaters and game console makers went along with the plans, and the rating schemes became widely used and recognized. The same was not true for ICRA or PICS. Operating at the scale of the global internet and asking countless website managers to voluntarily self-label so much content proved an impossible task.

Internet content management has grown more sophisticated since the demise of ICRA and PICS, but challenges have multiplied. Major digital platforms like Google, Facebook, and Twitter have developed robust content management policies and tools that help the public avoid too easily stumbling upon pornographic sites or images. This was accomplished using automated algorithmic screening systems backed up by human review. However, pornography was not the only type of potentially objectionable content online providers confronted. Today's debates over "content moderation at scale" involve various types of hate speech, communications from extremist groups, trolling, cyberstalking, and even so-called fake news.[89]

Semantic debates about what each of these terms means has created new challenges for ICT governance efforts.[90] Moreover, the "volume problem"—that is, the ever-increasing volume of information available online—has become more acute. Mike Masnick of *TechDirt* has noted that roughly 6,000 videos are uploaded every minute to Google-owned YouTube alone, which equals about 8.6 million videos per day, and approximately 250 million new videos in a month. Masnick observes that even if Google is 99.99 percent "accurate" in screening out objectionable content, it would still mean roughly 26,000 "mistakes" each month. And that is assuming a level of accuracy that is impossible to achieve in practice.[91]

---

88. Phil Archer, ICRAfail: A Lesson for the Future 9 (Nov. 26, 2009) (unpublished manuscript), ("The problem with a safety system that has a label at one end and a filter at the other is that unlabeled sites can only be treated as a single group, i.e. you either block them all or allow them all. Since the number of labelled sites was very small, blocking all unlabeled sites would effectively shut off most of the Web.").

89. James Grimmelmann, *The Platform Is the Message*, 2 GEO. L. TECH. REV. 217 (2018), https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Grimmelmann-pp-217-33.pdf [https://perma.cc/67BD-6CND].

90. Kirsten Grind & John D. McKinnon, *Facebook, Twitter Turn to Right-Leaning Groups to Help Referee Political Speech*, WALL ST. J. (Jan. 8, 2019, 12:10 PM), https://www.wsj.com/articles/facebook-twitter-solicit-outside-groups-often-on-the-right-to-referee-political-speech-11546966779 [https://perma.cc/D5DM-99PS].

91. Mike Masnick, *Google CEO Admits That It's Impossible to Moderate YouTube Perfectly; CNBC Blasts Him*, TECHDIRT (June 20, 2019, 2:12 PM), https://www.techdirt.com/articles/201906

The combination of technical and legal challenges led many experts to recommend greater reliance on educational efforts and user-empowerment solutions. Over the past two decades, governments and private organizations formed several blue-ribbon task forces to study new governance approaches that might help address online safety and content management concerns. Between 2000 and 2009 alone, five major task forces or blue-ribbon commissions were formed to study online safety issues and consider what should be done to address them.[92] Generally speaking, these were multistakeholder efforts involving a diverse set of experts from academia and think tanks, corporations and professional trade associations, advocacy organizations, and various government agencies. There was consensus in their final recommendations, which included a variety of online safety best practices, educational approaches, and technological empowerment solutions. Again, these represent soft law efforts because governments often blessed these groups and efforts but then left it to them to establish best practices for online content management.

In summary, for content management in ICT sectors, there has been an unmistakable trend away from hard law and toward various types of soft law solutions. At least in the United States, this trend is likely to continue. It remains to be seen how the more decentralized soft law approaches favored by the United States adjust to the more restrictive speech and content controls sometimes enacted by global governments. This is a particularly difficult challenge for large, U.S.-based multinational companies confronted with conflicting speech values and content management policies in the other countries in which they provide service.[93]

VI. CASE STUDY: DIGITAL PRIVACY

While content-related issues have been a long-standing focus of ICT governance, privacy and data protection represent more recent concerns. There were, however, some important hard law enactments focused on privacy issues over the past fifty years. Congress passed targeted privacy or data protection laws such as the Fair Credit Reporting Act of 1970,[94] the Cable Communications Policy Act of 1984,[95] the Video Privacy Protection Act of 1998,[96] the Health

18/17362542426/google-ceo-admits-that-impossible-to-moderate-youtube-perfectly-cnbc-blasts-him.shtml [https://perma.cc/9UBL-YVLY].

92. Adam Thierer, *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, PROGRESS ON POINT (Progress & Freedom Found., Wash., D.C.), July 2009, at 1.

93. Cara Curtis, *Facebook's Global Content Moderation Fails to Account for Regional Sensibilities*, TNW (Feb. 26, 2019), https://thenextweb.com/socialmedia/2019/02/26/facebooks-global-content-moderation-fails-to-account-for-regional-sensibilities [https://perma.cc/G8MY-UGET.

94. 15 U.S.C. §§ 1681–1681(u).

95. 47 U.S.C. § 551.

96. 18 U.S.C. § 2710.

Insurance Portability and Accountability Act (HIPAA) of 1996,[97] and the Children's Online Privacy Protection Act (COPPA) of 1998.[98] But the United States never implemented an overarching national privacy law as other countries did.

As online activity expanded in the late 1990s, interest in digital privacy issues increased alongside it. Because the United States lacks a lead privacy regulator or national data protection agency, it fell to the FTC to monitor online privacy concerns at the federal level, while states engaged in selective privacy enforcement activities. The NTIA also played an important role in guiding federal privacy policy, especially during the Obama administration. The FTC and NTIA's activities are reviewed in turn.

The FTC's broad authority to police "unfair and deceptive practices" under section 5 of the Federal Trade Commission Act gave the agency leeway to address privacy and data security matters as the digital economy grew.[99] The agency used its consumer protection authority to pursue hundreds of privacy- and data security-related cases over the past two decades, including enforcement actions against large tech companies like Google, Facebook, Twitter, Microsoft, and many others.[100] The FTC's body of consent decrees has grown so extensively that some legal scholars refer to it as "the new common law of privacy."[101] Consent decrees are settlements that regulatory agencies broker with private actors and which impose penalties on those actors for violating rules enforced by the agency.

What the FTC created through these consent decrees is akin to a new *soft law* of privacy that reinforces a set of practices the agency has recommended over time.[102] The FTC used these enforcement actions both "to hold those companies accountable for the promises they make"[103] to the public, and also to

97. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

98. 15 U.S.C. § 6501.

99. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273 (2011) ("[T]he Federal Trade Commission has actively used its broad authority under section 5 of the FTC Act, which prohibits 'unfair or deceptive practices,' to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.").

100. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2018, at 3 (2018) https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [https://perma.cc/EF6M-W7P5].

101. *See e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583 (2014).

102. Geoffrey Manne, *Congressional Testimony on Legislative Reform Proposals for the FTC*, TRUTH ON MARKET (May 26, 2016), https://truthonthemarket.com/2016/05/26/congressional-testimony-on-legislative-reform-proposals-for-the-ftc/ [https://perma.cc/65B4-JWG7]; Jennifer Huddleston, *Unprecedented: The Issue of Agency Action by Consent Order on Innovation*, MEDIUM: PLAIN TEXT (Sept. 22, 2017), https://readplaintext.com/unprecedented-the-issue-of-agency-action-by-consent-order-on-innovation-b23ab7b09f42 [https://perma.cc/4PZ9-9DKQ].

103. Fed. Trade Comm'n, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, Comment to the National Telecommunications and Information Administration, Docket No. 180821780–8780–01, at 20 (Nov. 9, 2018), https://www.ftc.gov/system/files/docum

recommend to others a set of broad-based best practices for handling data going forward. Those consent-decree enforcement efforts went hand in hand with the agency's increased reliance on other soft law efforts to fill some of the gaps left by the absence of an overarching legislative framework for privacy.

The FTC's privacy-related efforts expanded significantly during the Obama administration. In early 2012, it released a report entitled, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*.[104] The White House referred to it as their "Privacy Blueprint."[105] While calling for Congress to enact a formal "Consumer Privacy Bill of Rights," the document also advocated "a multistakeholder process to produce enforceable codes of conduct that implement the Consumer Privacy Bill of Rights."

Congress failed to act on the administration's call for comprehensive privacy legislation, which meant the multistakeholder approach took on greater significance over time. In its Privacy Blueprint, the administration made it clear that it wanted several privacy-related values respected. Those values included individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[106] These principles were built on Fair Information Practice Principles (FIPPs) that infused earlier hard law privacy efforts, both within the United States and abroad.[107] Privacy by design was the touchstone of these efforts and came to infuse soft law activity at both the FTC and NTIA.

At this point, the NTIA's role expanded considerably. Shortly after the Obama administration released its Privacy Blueprint, the NTIA hosted the first in a series of multistakeholder discussions in July 2012. The NTIA's initial privacy multistakeholder process focused on mobile app transparency and encouraged stakeholders to "engage in an open, transparent, consensus-driven process to develop a code of conduct,"[108] which they finalized in July of 2013.[109]

A few years later, NTIA tapped this model again, this time for drone privacy. Following a February 2015 presidential memorandum issued by President

---

ents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf [https://perma.cc/G7XX-S92G].

104. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/ZA63-K9FE].

105. *Privacy Multistakeholder Process: Mobile Application Transparency*, NAT'L TELECOM. & INFO. ADMIN. (Nov. 12, 2013), https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency [https://perma.cc/JJL3-Y9T5].

106. WHITE HOUSE, *supra* note 104, at 10.

107. *Fair Information Practice Principles*, IAPP, https://iapp.org/resources/article/fair-information-practices [https://perma.cc/QZ3Z-HMBQ].

108. *First Privacy Multistakeholder Meeting: July 12, 2012*, NAT'L TELECOM. & INFO. ADMIN. (June 15, 2012), https://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012 [https://perma.cc/V58E-7WCG].

109. NAT'L TELECOM. & INFO. ADMIN., SHORT FORM NOTICE CODE OF CONDUCT TO PROMOTE TRANSPARENCY IN MOBILE APP PRACTICES (July 25, 2013), https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf [https://perma.cc/9P6H-WPNJ].

Obama on unmanned aircraft systems (UAS), [110] the NTIA was tasked with forming a multistakeholder process to address "the privacy, civil rights, and civil liberties concerns these systems may raise." The NTIA hosted numerous stakeholder meetings "and a diverse group of stakeholders came to consensus on a best practices document."[111] The final report contained five voluntary best practices to "focus on data collected via a UAS, which includes both commercial and non-commercial UAS."[112]

These multistakeholder efforts served as examples of the "government steers, industry rows" approach alluded to earlier. In each case, a common set of best practices infused the soft law efforts used by the FTC, NTIA, and other government agencies when addressing privacy-related matters. Yet, it fell to industry (primarily major trade associations), civil society, and various other groups to work out the details of how these principles would be established and enforced. In each instance, these multistakeholder efforts yielded multiple events or workshops, ongoing consultations between affected parties and regulatory officials, and a consensus document containing best practices for the matter at hand.

But not all of these multistakeholder efforts have borne fruit. A multistakeholder proceeding intended to address the privacy issues surrounding commercial facial recognition technologies[113] led to heated negotiations and a collective walkout by privacy advocacy organizations that wanted private companies to agree to comprehensive restraints on the use of such technologies.[114]

Still, there were other important privacy-related soft law developments over the past two decades. The use of workshops, workshop reports, and other special reports to advance privacy and data security goals was a particularly notable development. For example, the FTC estimates that, since 1996, it "has hosted more than 70 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security."[115] Beginning in 2016, the agency also initiated an annual PrivacyCon event "to bring together a diverse group of stakeholders, including white-hat researchers, aca-

110. Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, 80 Fed. Reg. 9,355 (Feb. 20, 2015).

111. *Multistakeholder Process: Unmanned Aircraft System*, NAT'L TELECOM. & INFO. ADMIN. (June 21, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems [https://perma.cc/ANA8-46UF].

112. NAT'L TELECOM. & INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY 5–6 (2016).

113. NAT'L TELECOM. & INFO. ADMIN., PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL FACIAL RECOGNITION USE (2016) (encouraging transparency, developing good data management practices, allowing people to control the sharing of their data, using security safeguards, ensuring data quality, and allowing problem resolution and redress), https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf [https://perma.cc/V489-W9DZ].

114. Elizabeth Weise, *Privacy Groups Leave Over Dispute on Facial Recognition Software*, USA TODAY (June 16, 2015, 12:48 AM), https://www.usatoday.com/story/tech/2015/06/16/facial-recognition-software-google-facebook-moments-ntia/28793157 [https://perma.cc/Z4AJ-DQMR].

115. FED. TRADE COMM'N, *supra* note 100, at 12.

demics, industry representatives, consumer advocates, and government regulators, to discuss the latest research and trends related to consumer privacy and data security."[116]

Although not always billed as formal multistakeholder proceedings, these workshops played a similar role by bringing diverse parties together to identify privacy threats and potential remedies to them (usually in the form of voluntary best practices). Several important privacy-related reports have accompanied these FTC proceedings, including a major 2012 report on *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*.[117] The agency followed up with reports focused on the specific privacy concerns surrounding technologies such as big data,[118] IoT,[119] facial recognition,[120] and cross-device tracking capabilities.[121] Each report reinforced a common set of privacy best practices the agency hoped private developers would follow.

The FTC has simultaneously expanded use of its website and social media accounts to provide additional guidance on these matters.[122] Through blog posts, YouTube videos, and Twitter postings, the agency has reinforced best practices it has repeatedly itemized in its workshops, reports, and consent decrees. The agency also uses education and awareness-building efforts to advance privacy and data security objectives through OnGuardOnline, a website that offers privacy and security advice to individuals and businesses.[123] Once again, the FTC used these educational mechanisms to encourage privacy by design.

---

116. *PrivacyCon*, FED. TRADE COMM'N (Jan. 14, 2016, 9:00 AM), https://www.ftc.gov/news-events/events-calendar/privacycon [https://perma.cc/93DH-4CDQ].

117. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at i (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/9NNZ-LK9L].

118. FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, at i (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/H7MJ-VACQ].

119. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, at i (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/AZE8-EWDX].

120. FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, at ii (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/H3SU-G5FS].

121. FED. TRADE COMM'N, CROSS-DEVICE TRACKING: A FEDERAL TRADE COMMISSION STAFF REPORT, at ii (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [https://perma.cc/ND3X-FKFD].

122. *See Blog Posts Tagged with Privacy and Security*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/blogs/terms/245 [https://perma.cc/G36U-WBHC]; *Federal Trade Commission*, FACEBOOK, https://www.facebook.com/federaltradecommission [https://perma.cc/3WAF-BTPZ].

123. *OnGuardOnline*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/features/feature-0038-onguardonline [https://perma.cc/LWY2-DA69].

The agency, however, never makes it clear whether any of the advice found in its workshop reports, its website, or its social media accounts constitutes binding rulemaking. Most agency followers assume that such activity is *not* formally binding. Nonetheless, using these tools, the agency has repeatedly stressed the importance of privacy and data security best practices that it clearly expects digital innovators to follow. The open question is whether that activity and advice forms baseline expectations in the minds of the affected parties that come to influence corporate decisions about privacy and data practices.

It is impossible to know how much influence these FTC soft law efforts have had on private actors, but it seems they are having some effect. In a 2011 law review article, Kenneth A. Bamberger and Deirdre K. Mulligan explored the distinction between what they referred to as "Privacy on the Books and on the Ground."[124] They identified how privacy best practices were emerging in a decentralized fashion thanks to the activities of corporate privacy officers and privacy associations who helped formulate best practices in data collection and handling.[125]

These efforts have been greatly facilitated by professional bodies and nonprofit organizations such as the International Association of Privacy Professionals (IAPP), the Future of Privacy Forum, and the Council of Better Business Bureaus, among others. "The individuals managing corporate privacy have an applicant pool of trained professionals to draw from," Bamberger and Mulligan noted. Furthermore, they stated: "There is ongoing training, certification, and networking. A community of corporate privacy managers has emerged. Ready evidence suggests that substantial effort is made to manage privacy."[126]

These efforts have expanded considerably since Bamberger and Mulligan wrote their article in 2011. For example, IAPP membership jumped from 20,000 members in 2015 to 50,000 in 2019.[127] Because IAPP certifies privacy professionals, this serves as a rough proxy for the growth of "on the ground" corporate compliance efforts.

One reason corporate legal counsels and privacy managers may be expanding privacy actions and certification efforts is to respond to the FTC's (and NTIA's) expanding soft law efforts. Presumably, those private actors also hope to avoid onerous regulatory interventions or consent decrees if they fail to make such efforts. They are also responding to hard law enactments happening internationally. It remains difficult to determine how much influence these forms of FTC soft law have on private behavior relative to other state actions. This issue deserves greater study.

Other questions remain ripe for further exploration. As it pertains to agency-recommended privacy and data security best practices, where is the line between agency *advice* and agency *threats*? Similarly, when considering what

124. Bamberger & Mulligan, *supra* note 99.

125. *Id.* at 255–56.

126. *Id.* at 260.

127. *IAPP Hits 50,000 Members Marking Milestone for Organization and Growth of Privacy Profession*, INT'L ASS'N PRIV. PROS. (May 2, 2019), https://iapp.org/about/iapp-hits-50000-members-marking-milestone-for-organization-and-growth-of-privacy-profession [https://perma.cc/Y7BC-HNT7].

might trigger enforcement activities and consent decrees, is it fair to hold companies to best practices that were never promulgated through APA procedures? These questions are beyond the scope of this paper, but the agency obviously hopes that its soft law activities are having *some* influence on corporate behavior. It remains to be seen whether agency officials can hold private actors to standards that are unpromulgated and ever changing, and whether courts will grant agencies broad deference to enforce soft law more generally.[128]

Other government agencies besides the FTC and NTIA are tapping soft law mechanisms to address privacy concerns. Meanwhile, the Trump administration employed multistakeholder approaches and soft law mechanisms to address privacy, in some cases continuing efforts initiated by the Obama administration.[129]

In September 2019, the National Institute of Standards and Technology (NIST), which is part of the Department of Commerce, released preliminary voluntary privacy guidelines "to help organizations manage privacy risks" by encouraging privacy-by-design efforts.[130] As with other soft law guidance documents, NIST's *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* is even "versioned" like software, with its preliminary draft being labeled "Version 1.0."[131] Other soft law efforts have also been versioned as if they were computer software (Version 1.0, 1.1, etc.), reflecting the way government agencies increasingly view soft law as an iterative and adaptive process rather than a fixed endpoint.[132] The NIST document, which was developed "in collaboration with private and public stakeholders,"[133] stresses the need for a "risk-based approach"[134] to dealing with privacy concerns. This effort builds on the NIST's Cybersecurity Framework, which will be discussed in the following section.

---

128. Jennifer Huddleston, *Disrupting Deference for Disruptive Technology*, (Ctr. for the Study of the Admin. State Working Paper No. 19-35, 2019), https://administrativestate.gmu.edu/wp-content/uploads/sites/29/2019/11/Huddleston-Disruptive-Deference-for-Disruptive-Technology.pdf [https://perma.cc/R8DB-ERC8] (presented Nov. 25, 2019 at the conference on Technology, Innovation, and Regulation).

129. *See Request for Comments on Developing the Administration's Approach to Consumer Privacy*, NAT'L TELECOM. & INFO. ADMIN. (Sept. 25, 2018), https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy [https://perma.cc/X4A2-3CYQ].

130. NAT'L. INST. OF STANDARDS & TECH., PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT 4 (Sept. 6, 2019), https://www.nist.gov/system/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf [https://perma.cc/R52G-978D].

131. *Id.* at 1.

132. Jennifer Huddleston et al., *Mitigating Privacy Risks While Enabling Emerging Technologies*, MERCATUS CTR. (Oct. 24, 2019), https://www.mercatus.org/publications/regulation/mitigating-privacy-risks-while-enabling-emerging-technologies [https://perma.cc/2TKW-UHHG] ("When faced with the rapid changes associated with technological advancement, the use of soft law can facilitate a governance approach that is able to evolve with and enable innovation better than traditional policy tools.").

133. NAT'L. INST. OF STANDARDS & TECH., *supra* note 130, at 1.

134. *Id.* at 10.

Privacy-related hard law enactments may yet prevail and render moot many of these soft law efforts. Over the past decade, privacy advocates have expressed dissatisfaction with the state of soft law governance and continued their push for more aggressive hard law efforts, including a comprehensive "baseline" federal privacy law.[135] After repeated failures to enact such a measure, legislative efforts shifted to the state level, where California has led the way with a major new law that became effective in 2020.[136] State-based privacy laws might raise constitutional issues on Commerce Clause grounds, however, and could face court challenges or federal preemption.[137] If they are struck down, soft law might, once again, need to fill the gaps.

It is worth noting that some technical industry-led self-regulatory efforts to address privacy and data protection have not achieved much success, although soft law experiments of this type continue. The Platform for Privacy Preferences (P3P) is a good example. Like ICRA before it, P3P began in the early 2000s and was intended to serve as a website screening tool, except in this case for privacy purposes. P3P let content providers voluntarily add machine-readable metadata to their website, which could then be automatically screened by web browsers.[138] The system was supposed to signal to users the sort of user information the site collected and then allow them to configure their web browsers to determine how much of their data could be seen or collected.

The World Wide Web Consortium, which oversaw the effort, abandoned P3P after it failed to gain traction. As with ICRA, the challenge of labeling such a massive and ever-expanding universe of sites and content was likely its undoing. As P3P began fading out of consciousness in the late 2000s, the W3C turned its attention to the formulation of a Do Not Track (DNT) system, which is a web browser standard that allows users to disable tracking by websites and ad services. Despite support from many privacy advocates as well as the FTC,[139] the effort ultimately went down as another failed experiment due to the inability of

---

135. *See e.g.*, Stacey Gray, *Long Overdue: Comprehensive Federal Privacy Law*, FUTURE PRIV. F. (Nov. 15, 2018), https://fpf.org/2018/11/15/fpf-comments-on-a-national-baseline-consumer-privacy-law [https://perma.cc/M6LE-87WR].

136. *See* Jeff John Roberts, *Here Comes America's First Privacy Law: What the CCPA Means for Business and Consumers*, FORTUNE, (Sept. 13, 2019, 3:30 AM), https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law [https://perma.cc/B4LF-KJKN].

137. JENNIFER HUDDLESTON & IAN ADAMS, POTENTIAL CONSTITUTIONAL CONFLICTS IN STATE AND LOCAL DATA PRIVACY REGULATIONS 10–12 (Dec. 2, 2019), https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf [https://perma.cc/L68M-TLAM] (released by the Regulatory Transparency Project of the Federalist Society); Jeff Kosseff, *Ten Reasons Why California's New Data Protection Law Is Unworkable, Burdensome, and Possibly Unconstitutional*, TECH. & MKTG. L. BLOG, (Jul. 9, 2018), https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm [https://perma.cc/A7LJ-89RU].

138. *Platform for Privacy Preferences (P3P) Project*, W3C, https://www.w3.org/P3P [https://perma.cc/8KPS-GLN4].

139. Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers [https://perma.cc/LT7Z-Q98F].

industry and privacy advocates to reach consensus about the nature and scope of the DNT standard during ongoing multistakeholder discussions.[140]

In the absence of a more comprehensive effort, the Digital Advertising Alliance (DAA), a consortium of the leading national advertising and marketing trade groups, continues to operate a fully self-regulatory program called YourAdChoices, which allows users to tailor interest-based advertising preferences.[141] But this system only applies to DAA member companies and does not incorporate the comprehensive type of blocking that the Do Not Track standard would allow. Meanwhile, private ad-blocking technologies and other privacy-enhancing tools continue to be developed by others. The consultancy eMarketer estimates that "one in four US internet users have installed some type of ad blocking software on at least one of their devices."[142]

In summary, a wide range of soft law mechanisms continues to play a role in privacy governance in the United States. After many fits and starts, however, hard law efforts appear closer to gaining traction. The history of soft law in this particular context remains in flux.

VII. CASE STUDY: CYBERSECURITY

While the quality, security, and reliability of interconnected communications systems has long been a focus of ICT policy,[143] these concerns have expanded considerably with the growth of the internet and global digital networks. Spam, malware, viruses, data breaches, and critical system intrusions are among today's leading network security concerns. Soft law efforts have played a role in addressing these matters for many years.

It is worth noting that the internet's progenitor, Advanced Research Projects Agency Network (ARPANET), was developed by the Defense Advanced Research Projects Agency at the U.S. Department of Defense (DOD) and grew out of a Cold War–era fear that traditional communications networks might fail during an enemy attack.[144] In 1964, Paul Baran, working at RAND for the U.S. Air Force, published *On Distributed Communications*, which critiqued existing

140. Kashmir Hill, '*Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, GIZMODO (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324 [https://perma.cc/AD45-JDKP]

141. *YourAdChoices Gives You Control*, YOURADCHOICES, https://youradchoices.com/control [https://perma.cc/JUE5-GFDF].

142. Nicole Perrin, *Consumer Attitudes on Marketing 2019: Privacy Concerns Mount, and Ad Blocking Isn't Going Away*, EMARKETER (Aug. 29, 2019), https://www.emarketer.com/content/consumer-attitudes-on-marketing-2019 [https://perma.cc/7YQN-U7NV].

143. *See* Henry A. Malec, *Communications Reliability: A Historical Perspective*, 47 IEEE TRANSACTIONS ON RELIABILITY 333, 333–45 (1998).

144. Zoë Jackson, *Communications Revolution: ARPANET and the Development of the Internet, 50 Years Later*, PERSPS. ON HIST. (May 14, 2019), https://www.historians.org/publications-and-directories/perspectives-on-history/may-2019/communication-revolution-arpanet-and-the-development-of-the-internet-50-years-later [https://perma.cc/2CU9-NL25].

military communications network design as centralized and vulnerable.[145] Baran envisioned a new network that was "designed for data transmission and for survivability at the outset."[146]

He advocated that the DOD consider reworking their entire communications system, moving to a decentralized, all-digital, packet-switched design. In this network, diagramed in his paper as a mesh network, there was no central point of control, and redundant links served each node in the network. In other words, secure and reliable communications were the touchstone of this proposed new system, which would eventually influence the creation of ARPANET and then, many years later, grow to become the internet.

While the internet has indeed proven to be the sort of robust, resilient, and all-digital "network of networks" that Baran hoped for, other security vulnerabilities developed over time. Spam, or unsolicited email, quickly became an annoyance on the commercialized internet. Hard law efforts such as the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003, which aimed to curtail the flow of unsolicited email across digital systems, were largely ineffective at stemming the tide.[147] Additionally, cybersecurity-oriented legislative proposals have stalled due to the lawmaking roadblocks identified earlier. As a result, these problems have been addressed with various soft law efforts.

Companies, trade associations, university centers, and various private organizations have spontaneously developed what Eli Dourado labels "Internet Security without Law."[148] More specifically, internet security is currently being pursued largely without hard law. Soft law methods, however, have been central to cybersecurity protection for many years.

Dourado documented how "informal institutions carry out the functions of a formal legal system—they establish and enforce rules for the prevention, punishment, and redress of cybersecurity-related harms."[149] Network security norms and solutions have been cobbled together not through central design or regulatory edicts, but through decentralized efforts of many organizations working collaboratively. These players include internet service providers (ISPs), domain name registrars, hosting companies, digital activist organizations, and assorted university-based computer science and engineering programs. These individuals and entities work with computer security incident response teams (CSIRTs), which are embedded within organizations, to address security vulnerabilities by sharing information and research about network vulnerabilities

145. Memorandum from Paul Baran On Distributed Communications to the United States Air Force Project Rand (Aug. 1964), https://www.rand.org/pubs/research_memoranda/RM3420.html (follow hyperlink to download ebook).

146. *Id.* at 34.

147. 15 U.S.C. § 7701(b).

148. *See* Eli Dourado, *Internet Security Without Law: How Security Providers Create Online Order* 1, 3 (Mercatus Ctr. at George Mason Univ. Working Paper, No. 12-19, 2012), https://www.mercatus.org/system/files/ISP_Dourado_WP1219.pdf [https://perma.cc/CJG3-EY99].

149. *Id.* at 1.

and online security attacks.[150] Many online cybersecurity discussion forums and security blogs also exist, where experts and layman discuss security issues.

Led by private developers, voluntary security groups like The Cavalry help build awareness about digital security threats and then devise solutions to address them.[151] Likewise, the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) was formed in 2004 as "a technology-neutral, non-political working body" to "work against botnets, malware, spam, viruses, DoS attacks and other online exploitation."[152] With over 200 members, it is the largest global industry association of its kind. M3AAWG develops best practices and education material and assists governments in developing policies for these issues.

The Internet Society's Online Trust Alliance also "identifies and promotes security and privacy best practices that build consumer confidence in the Internet," often by forming or facilitating multistakeholder initiatives.[153] Likewise, the National Cyber Security Alliance promotes internet safety and security efforts among a variety of companies and coordinates Data Privacy Day (held annually on January 28)[154] and National Cyber Security Awareness Month (every October),[155] which are collaborative efforts between government and industry that raise nationwide cybersecurity awareness. The Department of Homeland Security hosts a website promoting National Cyber Security Awareness Month, which offers a constantly updated toolkit of best practices.[156]

More recently, in early 2019, the Electronic Frontier Foundation (a digital rights organization), created the Threat Lab, which has been described as a "small, nonprofit cybersecurity consulting firm" and "a kind of security crisis hotline" for the general public.[157] In September 2019, the Council to Secure the

---

150. Robin Ruefle, *Defining Computer Security Incident Response Teams*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Jan. 24, 2007), https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams [https://perma.cc/5A6F-V63P] ("A CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility of providing part of the incident management capability for a particular organization. When a CSIRT exists in an organization, it is generally the focal point for coordinating and supporting incident response.").

151. *Safer. Sooner. Together.*, I AM CAVALRY, https://www.iamthecavalry.org [https://perma.cc/4USM-B4CX].

152. *Why M3AAWG?*, MESSAGING MALWARE & MOBILE ANTI-ABUSE WORKING GRP., https://www.m3aawg.org/about-m3aawg [https://perma.cc/V2BB-DVUX].

153. *Online Trust Alliance (OTA)*, INTERNET SOC'Y, https://www.internetsociety.org/ota [https://perma.cc/V8M3-H9E3].

154. *About Data Privacy Day*, NAT'L CYBER SEC. ALL., https://staysafeonline.org/data-privacy-day/about-dpd/http://www.staysafeonline.org/data-privacy-day [https://perma.cc/DUR8-MTMM].

155. *Cybersecurity Awareness Month*, NAT'L CYBER SEC. ALL., https://staysafeonline.org/cybersecurity-awareness-month/ [https://perma.cc/VYF9-VA3K].

156. NAT'L INITIATIVE FOR CYBERSECURITY CAREERS & STUD., NATIONAL CYBERSECURITY AWARENESS MONTH: 2019 TOOLKIT (2019), https://niccs.us-cert.gov/sites/default/files/documents/pdf/dhs_ncsam2019_toolkit_508c.pdf?trackDocs=dhs_ncsam2019_toolkit_508c.pdf [https://perma.cc/GS2J-PWJH].

157. Andy Greenberg, *Stories of People Who Are Racing to Save Us*, WIRED: WIRED25 (Oct. 15, 2019, 6:00 AM), https://www.wired.com/story/wired25-stories-people-racing-to-save-us/ [https://perma.cc/LXG7-Q7FH].

Digital Economy—a partnership of 20 major technology trade associations—released two major cybersecurity reports outlining solutions to major cyber threats facing consumers, businesses and governments.[158] One report outlined "the foundations for multi-stakeholder coordination during cybersecurity crises" and included a wide variety of best practices to achieve better security.[159]

These security-focused individuals and organizations interact and coordinate with other experts across the globe, which means they are able to quickly address concerns that territorial hard law regulations and liability regimes could not reach as effectively, if at all. Taken together, these efforts exemplify Zittrain's notion of mutual aid at work.[160] Mutual aid has been an essential part of cybersecurity and online content management efforts since the turn of the century. "The critical lesson is that multi-stakeholder cooperation can take many forms, and the Internet can be mediated minute-to-minute through technology and praxis as much as through formal hierarchy," he observes.[161] We should expect the trend to continue with various players "working together in highly provisional, spontaneous, and self-organized ways" to create more robust and resilient networks and systems.[162]

Although most of these developments have occurred outside traditional hard law processes, soft law in the cybersecurity arena has been influenced by government actors, and occasionally, even the threat of regulatory intervention. For the most part, government actors have played more of a coordinator and educator role on this front.

For example, in 2011, the FCC created the Communications Security, Reliability, and Interoperability Council (CSRIC), a federal advisory committee established pursuant to the Federal Advisory Committee Act to advise the agency on various network security matters.[163] CSRIC convened 11 different working groups made up of stakeholders from industry, academia, nonprofits, and other groups. These working groups issued reports on network security and

158. COUNCIL TO SECURE THE DIGIT. ECON., THE C2 CONSENSUS ON IOT DEVICE SECURITY BASELINE CAPABILITIES (2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf [https://perma.cc/9GG4-D3VD]; COUNCIL TO SECURE THE DIGIT. ECON., CYBER CRISIS: FOUNDATIONS OF MULTI-STAKEHOLDER COORDINATION (2019) [hereinafter CSDE, CYBER CRISIS], https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf [https://perma.cc/7CVZ-8SVQ].

159. CSDE, CYBER CRISIS, *supra* note 158, at 2.

160. Zittrain, *supra* note 65, at 10.

161. *Id.*

162. Anne Hobson, *The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem* (Ctr. for Growth & Opportunity at Utah State Univ., Pol'y Paper No. 2019.004, 2019), https://www.thecgo.org/wp-content/uploads/2020/07/The-Resilience-Approach-to-Cybersecurity-Policy-in-the-Internet-of-Things-Ecosystem.pdf [https://perma.cc/3VDE-NW9U].

163. *Charter of the FCC'S Communications Security, Reliability, and Interoperability Council*, FED. Commc'ns COMM'N (Mar. 18, 2011), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC%20Charter%20Renewal%202011%20FINAL.pdf [https://perma.cc/QB5T-XQBC].

outage best practices, botnet remediation efforts, consensus cybersecurity controls, and more.[164] Many of the security groups mentioned earlier, including M3AAWG and the Online Trust Alliance, were part of these collaborative multistakeholder efforts.

More recently, the FCC has attempted to address the problem of robocalls (unwanted automated phone calls) by encouraging communications and technology companies to work together on a technical solution. This resulted in the development of a new standard called SHAKEN/STIR, which are acronyms for Signature-Based Handling of Asserted information using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR) standards.[165] The North American Numbering Council (another federal advisory committee) helped develop the standard,[166] which was then supported by the FCC through formal regulatory action encouraging its adoption by voice service providers.[167]

These are two examples of soft law models that mix agency encouragement and direction with hard work by third parties to develop best practices or technical solutions to vexing security issues. These FCC efforts might be thought of as additional examples of the "government steers and industry rows" model of soft law in action. The extent of agency steering versus private sector rowing varies in almost every case, however. For older agencies with extensive regulatory authority, there tends to be a lot more steering and a greater expectation that private actors will fall in line with "voluntary" guidance (almost as if it represents formal regulation).

For example, the FDA is another agency that, like the FCC, enjoys a long history and extensive regulatory authority (including generous leeway from Congress to regulate "in the public interest"). Despite broad regulatory authority, the FDA is advancing cybersecurity goals for advanced medical devices mostly through guidance documents.[168] As with many other FDA guidances, the agency's 2016 "Postmarket Management of Cybersecurity in Medical Devices" guidance document has the phrase "Contains Nonbinding Recommendations" stamped prominently at the top of each page. In practice, however, the recommendations found in "nonbinding" guidances or codes of conduct tend to be

164. *See generally Communications Security, Reliability, and Interoperability Council III*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability [https://perma.cc/MZH8-PHVF].

165. *Combating Spoofed Robocalls with Caller ID Authentication*, FED. COMMC'NS COMM'N, https://www.fcc.gov/call-authentication [https://perma.cc/HE8J-NPTN].

166. *Id*.

167. Press Release, Fed. Commc'ns Comm'n, FCC Affirms Robocall Blocking Default to Help Protect Consumers (June 6, 2019), https://docs.fcc.gov/public/attachments/DOC-357852A1.pdf [https://perma.cc/82JX-46FS].

168. *E.g.*, U.S. FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (Dec. 28, 2016), https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf [https://perma.cc/GDU2-3EZ4].

followed because affected parties hope to avoid unwanted regulatory attention and aggressive agency action.[169]

Cybersecurity for connected cars is also a governance concern, and soft law approaches have been used in this context as well. In October 2016, the National Highway Traffic Safety Administration (NHTSA) released "nonbinding guidance to the automotive industry for improving motor vehicle cybersecurity," which included various best practices for the sector.[170] In mid-2017, the FTC and NHTSA hosted a joint workshop on privacy and cybersecurity for connected vehicles.[171] The FTC has also provided ongoing reports, websites, and videos offering cybersecurity advice to small business operators.[172]

Still other security-oriented soft law governance efforts are underway. In 2017, NIST hosted a public workshop on "Enhancing Resilience of the Internet and Communications Ecosystem."[173] This followed NIST's development of a "Framework for Improving Critical Infrastructure Cybersecurity," which consists of standards, guidelines, and best practices to manage cybersecurity-related risk.[174] The first iteration of that Framework was issued in early 2014, and then a revised version was released in April 2018. This reflects an effort to adapt guidance documents and best practices at a more rapid pace, in line with technological developments. The NIST Cybersecurity Framework and cyber insurance have a symbiotic relationship. Insurers play a role in enforcing best practices through requirements in the cyber insurance underwriting process, while encouraging adoption of the NIST Cybersecurity Framework through lower premiums.[175]

Various presidential executive orders were also issued by the Obama and Trump administrations that include soft law elements or procedures. In 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastruc-

---

169. Johnson, *supra* note 7, at 512 ("Though voluntary codes of conduct lack the traditional force of law, private entities generally seek to comply with adopted codes because noncompliance may compel those entities to publicly explain their departure from the code.").

170. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., DOT HS 812 333, CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES 5 (Oct. 2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf [https://perma.cc/4KU4-JWRZ].

171. *See generally Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, FED. TRADE COMM'N (June 28, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected [https://perma.cc/NBB4-6WC5].

172. *See generally Cybersecurity Basics*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics [https://perma.cc/N92Q-JMFN].

173. *See generally Enhancing Resilience of the Internet and Communications Ecosystem*, NAT'L. INST. STANDARDS & TECH, https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem [https://perma.cc/25VQ-3YUD] (describing July 11–12, 2017 public workshop).

174. NAT'L. INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, at v (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/6RYC-9CPY].

175. Anne Hobson, *Aligning Cybersecurity Incentives in an Interconnected World*, R ST. POL'Y STUDY (R St., Washington, D.C.), Feb. 2017, at 1, 3, https://www.rstreet.org/wp-content/uploads/2018/04/86-1.pdf. [https://perma.cc/DA68-C2EB].

ture Cybersecurity," which created a consultative process encouraging interaction and information sharing among public and private actors.[176] It required sector-specific agencies to "develop implementation guidance or supplemental materials to address sector-specific risks."[177] This was followed in 2015 by Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing."[178] It encouraged the development of Information Sharing and Analysis Organizations to facilitate cybersecurity information sharing and collaboration between the private sector and government agencies.[179] On May 11, 2017, President Trump issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[180] It required federal agencies to work collaboratively to create "an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks."[181]

Finally, since mid-2018, the NTIA has been running a Software Component Transparency multistakeholder working group that explores, "how manufacturers and vendors can communicate useful and actionable information about the third-party software components that comprise modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices."[182] This working group built on an earlier NTIA policy effort on cybersecurity vulnerability disclosure, which resulted in multistakeholder efforts and reports.[183]

These efforts reflect the continuing reliance upon soft law and multistakeholder process as essential governance strategies for network security in different ICT contexts. Barring catastrophic security incidents that prompt rapid legislative or sweeping regulatory responses, it seems likely that the use of these soft law tools and procedures will become predominant in coming years.

176. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

177. *Id.* at 11742.

178. Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 13, 2015).

179. *Id.*

180. Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017).

181. *Id.* at 22394.

182. *NTIA Software Component Transparency*, NAT'L TELECOMM. & INFO. ADMIN. (July 7, 2020), https://www.ntia.doc.gov/SoftwareTransparency [https://perma.cc/L428-JR5Y].

183. Press Release, Nat'l Telecomm. & Info. Admin., Internet Policy Task Force Seeks Comment on Multistakeholder Process Addressing Key Cybersecurity Issues (Mar. 13, 2015), https://www.ntia.doc.gov/press-release/2015/iptf-seeks-comment-key-cybersecurity-issues [https://perma.cc/CKE3-K92N]; *Multistakeholder Process: Cybersecurity Vulnerabilities*, NAT'L TELECOMM. & INFO. ADMIN. (Dec. 15, 2016), https://www.ntia.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities [https://perma.cc/85QB-XFRJ].

VIII. GENERAL LESSONS FROM ICT SOFT LAW CASE STUDIES

Drawing upon the case studies presented here—as well as the author's personal experience as a participant in multistakeholder processes and other soft law efforts—Part VIII offers some general thoughts about the use of soft law within ICT sectors, and what lessons it might hold for its use in other contexts.

- ***The informality of soft law is both its primary strength and greatest weakness***. The soft law governance approaches used in the ICT arena have been remarkably varied. Critics tend to be frustrated by how soft law mechanisms are inherently informal and open-ended, while defenders stress their flexibility and adaptability. That tension will persist. With soft law, there is no Goldilocks formula for getting things *just right*. Nor does soft law offer any silver-bullet solutions.[184] Much the same is true of hard law, of course, but soft law requires an even greater willingness to settle for what will feel like a second-best outcome to many. Participants in soft law processes need to temper their expectations and define reasonable metrics of success. It is better to view soft law as an iterative, ongoing *process* and not a definitive *endpoint*.

- ***Getting solutions to scale is challenging***. ***Large private institutions may sometimes be needed to help administer soft law standards and coordinate governance regimes***. Soft law efforts can face serious challenges when the scale of the problem being addressed is at the level of the entire global internet, or when definitional disputes make coordinated governance difficult. This was one of the likely reasons that the ICRA content-labeling system failed while the ESRB rating system succeeded. The ESRB system worked not only because it needed to address a limited universe of content, but also because some of the largest players in the industry (specifically console makers like Sony, Microsoft, and Nintendo) agreed to enforce the voluntary ratings scheme (and the machine-readable metadata triggers that made it work for consumers).

  Recall how ICANN became the favored solution for domain name management even though it would have enormous power over the internet's root. While that degree of concentrated power continues to raise concerns, it is possible that it is the only way to operate a global, interconnected, and reliable DNS system. The uncomfortable reality in both these examples is that it took a certain amount of private market power among industry leaders, or private organizations, to coordinate multistakeholder-negotiated standards and voluntary governance schemes. The greater irony is that, although soft law and multistakeholder processes are more decentralized than traditional hard law schemes, a certain degree of centralization may still be needed to make those systems work effectively.

184. Gary Marchant, *Conclusion: Emerging Governance for Emerging Technologies*, *in* INNOVATIVE GOVERNANCE MODELS FOR EMERGING TECHNOLOGIES 256 (Gary E. Marchant et al. eds., 2014). (Noting that with regard to new soft law mechanisms more generally, "there is no single approach, process or institution that will work for all technologies. There is no magic bullet.").

- ***Soft law is more likely to achieve concrete, lasting results for technical matters than for amorphous social problems.*** Technical governance objectives, such as domain name management or specific cybersecurity standards, can be complicated and controversial. It is fair to say, however, that such technical matters are probably more easily addressed using soft law mechanisms compared to amorphous social values such as online safety and privacy. The very terms *safety* and *privacy* can lead to endless and quite contentious philosophical debates about how to define and protect them, as well as how to address potential conflicts with other important values (especially freedom of speech). It does not mean soft law will be completely ineffective in these contexts, but rather that expectations will again need to be tempered when amorphous, value-laden matters are being deliberated. Achieving consensus and workable solutions will be far more challenging. If stakeholders can tighten the focus of the inquiry, it will improve the chances for more concrete and workable solutions. Once again, this is all just as true for hard law.

- ***A tradeoff may sometimes exist between the number of stakeholders involved in multistakeholder processes and the quality of negotiations, or the potential for positive outcomes***. To ensure that soft law governance efforts (especially multistakeholder processes) are democratic, diverse, and representative, it is optimal to involve as many stakeholders as possible. Defining who the right stakeholders are can be complicated,[185] and some limits may be required to achieve both workability and the potential for meaningful consensus. As with traditional legislative and regulatory processes, not everyone will get a proverbial seat at the table. Nonetheless, organizers of soft law efforts can use other mechanisms to ensure as many voices are heard as possible. At a minimum, open public comments and ongoing public input are essential. Stakeholders invited to the table need to have some "skin in the game" and be willing to work toward consensus and avoid trying to "win" through maximalist demands in one direction or another.

- ***Potential tension exists between transparency and quality of outcomes in some soft law negotiations***. On one hand, transparency is optimal in multistakeholder initiatives and other soft law efforts to ensure trust and legitimacy. On the other hand, frank conversation and high-quality negotiations may require a certain amount of privacy among stakeholders to hammer out workable solutions. This represents an inherent tension in all soft law systems. Striking the balance may require a limited space for private negotiating while ensuring that most proceedings and major decisions are made in an open and transparent fashion.

- ***Soft law and hard law can be compliments, but hard law can sometimes crowd out soft law, either by intention or accident.*** As noted, soft law represents a continuum of governance mechanisms that vary in terms of how much government action is involved. Government officials will often

185. MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 265 (2010) ("One of the chief problems with multistakeholderism is the plasticity and imprecision inherent in the concept of a *stakeholder*.").

tap soft law mechanisms while simultaneously pursuing hard law enactments. This has been the case on the privacy front for many years. But if those officials are preoccupied with the hard law initiatives, the soft law tools might become neglected or crowded out. For example, the Broadband Internet Technical Advisory Group (BITAG) is a multistakeholder organization that defines best practices for broadband network management and provide technical guidance to industry and to the public on those issues. The group, which was created in 2010, includes computer scientists and other technologists from universities, corporations, or other expert organizations.[186] In essence, BITAG was intended to be a technological ombudsman that could sort through potentially contentious network management issues and serve as "a neutral, expert technical forum and promote a greater consensus around technical practices within the Internet community."[187]

BITAG has issued many important reports over the past decade to further those objectives, but the group's work always felt secondary to the FCC's push for a formal net neutrality regulatory regime. A protracted multiyear fight over net neutrality rules continues today, while BITAG's soft law efforts are largely unknown to the public. This does not mean BITAG has been a failure, but it does raise the question of whether the group might have been more visible and effective had the sort of all-or-nothing political wrangling over formal net neutrality rules not overshadowed its efforts.

- ***Education and awareness-building efforts will likely become an increasingly important part of the soft law governance toolkit.*** This paper identified several leading soft law methods used repeatedly for ICT sectors, including multistakeholder arrangements, best practice formulation, agency workshops and reports, experimental sandboxes, and more. These approaches have speed and flexibility advantages over hard law. But the pacing problem can challenge soft law approaches, and could force policymakers and affected parties to seek out other flexible governance options. When all else fails, education and awareness-building approaches offer some of the very softest of soft law options. For some regulatory agencies, such as the FTC and FDA, risk education and communication are already part of their missions, but are often secondary to their enforcement efforts.[188] As other governance mechanisms—hard or soft—are formulated, education and risk communication efforts offer government officials a backup plan to help inform citizens about risks associated with new technological capabilities. Public education and risk communication are particularly well suited for fast-moving, hard-to-classify technologies such as IoT and artificial intelligence. Accordingly, we should expect them to become a bigger part of the soft law toolkit. Critics will likely

186. Broadband Internet Tech. Advisory Grp., *Initial Plans for Broadband Internet Technical Advisory Group Announced*, PRNEWSWIRE (June 9, 2010, 9:01 AM), https://www.prnewswire.com/news-releases/initial-plans-for-broadband-internet-technical-advisory-group-announced-95950709.html [https://perma.cc/JF9G-U2QE].

187. *Id.*

188. Adam Thierer, The Right to Try and the Future of the FDA in the Age of Personalized Medicine 15–18 (July 2016), https://www.mercatus.org/system/files/Thierer-Right-to-Try-FDA-v1.pdf [https://perma.cc/Q5T6-64SM] (unnumbered working paper).

> protest that education and risk communication efforts are largely toothless because they lack any enforcement element. But these strategies may, in certain instances, be the only options governments can tap to continue to have input in the way risky technologies are developed or used.

IX. SOFT LAW AS ONGOING CONVERSATION

The case studies discussed in this Article dealt mostly with ICT as defined traditionally. However, as noted from the outset, we live in an age of rapid convergence in which the same decentralizing technologies and disruptive forces that drove the rise of the internet and the digital economy are now spreading to every other sector of the economy. Software and digital technology really are "eating the world," as venture capitalist Marc Andreessen says.[189]

As this occurs, the same soft law tools and approaches used for traditional ICT sectors are spreading throughout many other sectors. Over the past decade, soft law and multistakeholder processes have been used for technologies as diverse as big data, machine learning, and artificial intelligence;[190] IoT (i.e., internet-enabled devices and applications);[191] policy concerning autonomous vehicles (i.e., driverless cars);[192] health and medical smartphone applications;[193]

189. Marc Andreessen, *Why Software Is Eating the World*, WALL ST. J. (Aug. 20, 2011), https://www.wsj.com/articles/SB10001424053111903480904576512250915629460 [https://perma.cc/E3UL-ZT27].

190. FED. TRADE COMM'N, *supra* note 118; NAT'L SCI. & TECH. COUNCIL COMM. ON TECH., EXEC. OFF. OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE (Oct. 2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf [https://perma.cc/47K7-EMWK]; EXEC. OFF. OF THE PRESIDENT, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf [https://perma.cc/V7RZ-ZKG2].

191. FED. TRADE COMM'N, *supra* note 119; FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (Jan. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf [https://perma.cc/7K2P-U4Z7]; Adam Thierer et al., *The Internet of Things and Consumer Product Hazards*, MERCATUS CTR. (June 14, 2018), https://www.mercatus.org/publications/technology-and-innovation/internet-things-and-consumer-product-hazards [https://perma.cc/H3CY-PSAA].

192. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T TRANSP., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY (Sept. 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf [https://perma.cc/2XYU-EUY7]; Jennifer Huddleston, Adam Thierer, & Ryan Hagemann, *'Soft Law' Is Eating the World: Driverless Car Edition*, MERCATUS CTR.: BRIDGE (Oct. 11, 2018), https://www.mercatus.org/bridge/commentary/soft-law-eating-world-driverless-car [https://perma.cc/6PY8-RREU].

193. U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS (Sept. 2019), https://www.fda.gov/media/80958/download [https://perma.cc/BLD6-9NMV].

medical advertising on social media platforms;[194] mobile applications for children;[195] 3D-printed medical devices;[196] and drones.[197]

Meanwhile, "soft law mechanisms are also used as a tool for technology policy at the state and local level," notes Jennifer Huddleston.[198] Many states have used various soft law approaches to address policy concerns surrounding autonomous vehicles.[199] Others have tapped regulatory sandboxes to address fintech governance.[200]

Each of these and the many other soft law processes discussed throughout this Article played out a bit differently. Soft law is inherently informal and ever changing. As a governance philosophy, soft law might best be thought of as an ongoing conversation instead of the definitive final word on anything.

That is why, in the end, soft law governance requires a commitment to continuous deliberation, consensus building, and pragmatic outcomes. Good-faith negotiation is essential to achieve workable results. Parties have to be willing to take small steps and achieve "wins" where they can get them, even if they may not feel like major victories at the time. None of this will likely feel satisfying to participants in these processes. Nevertheless, it may be the best that can be hoped for as hard law mechanisms become less effective in emerging technology contexts and soft law comes to fill the resulting governance gaps.

---

194. U.S. FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY: INTERNET/SOCIAL MEDIA PLATFORMS WITH CHARACTER SPACE LIMITATIONS—PRESENTING RISK AND BENEFIT INFORMATION FOR PRESCRIPTION DRUGS AND MEDICAL DEVICES (June 2014), https://www.fda.gov/media/88551/download [https://perma.cc/G5MW-4CZG].

195. FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (Dec. 2012), https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf [https://perma.cc/2QTN-MK5R].

196. U.S. FOOD & DRUG ADMIN., TECHNICAL CONSIDERATIONS FOR ADDITIVE MANUFACTURED MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Dec. 5, 2017), https://www.fda.gov/media/97633/download [https://perma.cc/WD6G-6GTE].

197. FED. AVIATION ADMIN., U.S. DEP'T OF TRANSP., AC No. 107-2, SMALL UNMANNED AIRCRAFT SYSTEMS (June 21, 2016), https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf [https://perma.cc/7X85-55M7]; *UAS Integration Pilot Program*, FED. AVIATION ADMIN., https://www.faa.gov/uas/programs_partnerships/integration_pilot_program [https://perma.cc/AZ9U-R9FD].

198. Jennifer Huddleston, *Soft Law and Emerging Technology in the States*, J. JAMES MADISON INST., Fall 2019, at 19, 20, https://www.jamesmadison.org/wp-content/uploads/2019/09/Journal_Fall2019_Content_v06_web.pdf [https://perma.cc/E973-KCZ2].

199. Jennifer Huddleston & Adam Thierer, *Pennsylvania's Innovative Approach to Regulating Innovation: Autonomous Vehicles Policy Offers a Case Study in Soft Law*, MERCATUS CTR.: BRIDGE (Sept. 5, 2018), https://www.mercatus.org/bridge/commentary/pennsylvanias-innovative-approach-regulating-innovation [https://perma.cc/LMP2-WLAP].

200. Brian Knight, *How to Build a Good Regulatory Sandbox: Four Principles to Help Policymakers Get It Right*, MERCATUS CTR.: BRIDGE (Apr. 17, 2019), https://www.mercatus.org/bridge/commentary/how-build-good-regulatory-sandbox [https://perma.cc/S9NZ-4WWK].