SOFT ON CRIME: ANTITRUST SOFT LAW TO SOLVE CYBERSECURITY GOVERNANCE CRISES

Caroline V. Lawrence[*]

25 YALE J.L. & TECH. 219 (2023)

To combat bioterrorism and cybercrime in the 2000s, antitrust agencies stepped up where Congress failed repeatedly to pass a cybersecurity bill. Their actions were surprising both in content and method. Substantively, the policy the FTC and DOJ promoted was to encourage plausibly anticompetitive joint ventures to proceed, so long as these collaborations existed for cyber safety purposes. The administrative agencies pursued this policy not via either formal or informal rulemaking, but rather a network of non-binding guidance known as "soft law." This technique structured industry incentives such that joint ventures would continue developing cyber defense mechanisms to protect the entire country. This analysis forces questions about ongoing debates within antitrust law and theories of agency activity. The Article also muses on why decentralized regulation, typically a polarizing subject, is so universally favored for cyber governance.

[*] J.D. The author thanks Professors Alvin Klevorick, Victoria Cundiff, and Oona Hathaway of Yale Law School for inspiring and nurturing this idea over the course of several years, and especially Professor Klevorick for his extensive feedback. The author also credits the closed captioning software on Zoom, which consistently rendered "antitrust" as "Anti-Christ."

TABLE OF CONTENTS

I. INTRODUCTION

A. The Dilemma: A Clash of Incentives between Public and Private Sectors in Cybersecurity

In the very first Strategy to Secure Cyberspace report in 2003, President Bush pronounced, "[T]he cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."[1] His statement reflected a widely held sentiment that industry would naturally work out ideal security protocols, leaving the government simply to regulate and educate the private sector.[2]

Instead, experience soon proved that industry security needs differed from the needs of national cybersecurity.[3] The dilemma repeated itself: private companies would decide for themselves the level of security that was financially worthwhile to them. Because this analysis had to balance several risks and business concerns, that level was almost always lower than the government would ideally set for its own purposes.[4] Still, the government would consistently lose out to industry in engaging skilled programmers with the capacity to build sophisticated national security instruments, and so companies remained better positioned to create these tools—if only they had the incentives.[5]

Because so many critical infrastructures partake of both public *and* private actors, the security set by these companies became, de facto, the security levels for the government.[6] The

---

[1] THE WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE, at iii (Feb. 2003), https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf [https://perma.cc/Q56V-GGBJ].

[2] *See Public-Private Partnership*, INTERNET SEC. ALL., https://isalliance.org/policy-advocacy/public-private-partnership [https://perma.cc/A62H-QER8] (describing early thinking on constructing public-private partnerships).

[3] *See id.* (citing "numerous reasons why the regulatory approach to cybersecurity was ill founded," including delusions about the causes of cyberattacks and a lack of support).

[4] *See id.* (describing why private companies did not want to pay for a level of security that the government would find desirable).

[5] *See, e.g.*, Paul Roberts, *Click Here to Kill Everybody and CyberSN on Why Security Talent Walks*, SECURITY LEDGER (Sept. 10, 2018), https://securityledger.com/2018/09/podcast-episode-111-click-here-to-kill-everybody-and-cybersn-on-why-security-talent-walks [https://perma.cc/22ZP-PKLB] (describing the difficulty of retaining skilled programmers).

[6] *See* Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 233 (2013) (describing how critical infrastructure sets the pace for the government's security levels); *see also The*

internet's diversified nature effectively relegated much of the operative security decision-making to private companies,[7] which did not always have time to involve the government in the midst of a crisis. The disjointed character of the internet also meant that unilateral government action could not reliably quell problems; with a global technology, assembled and maintained globally, U.S. government action could not always reach the areas of concern.

Moreover, the traditional ways that government accessed information about the private sector did not work for cybersecurity. The intensively Washington, D.C.-driven cadre of informal working relationships and overlapping jurisdictions, to which the government was accustomed, neither provided the quality intelligence needed by the government to develop standards or practices nor provided industry leaders with the incentive to invest their own financial resources in developing these standards.[8] Similarly, the government was much keener than its industry partners on attribution-as-deterrence.[9] In this lawless new world, the government wanted to uphold diplomacy and the principles of international law by bringing cybercriminals to justice. Industry executives, on the other hand, were lukewarm on the merits of *attributing* cyberattacks, and focused instead on understanding their

---

Sedona Conference Data Privacy Primer, 19 SEDONA CONF. J. 273, § D ("Industry standards have been cited at both the state and federal levels when determining the reasonableness of an organization's data security practices and potential liability . . . . Industry standards typically provide guidance on privacy and data security best practices regarding policies, data use and retention, and information security, including encryption.").

[7] *See id.* (explaining how private companies effectively take the lead in many security decision-making instances).

[8] INTERNET SEC. ALL., *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress*, OBAMA WHITE HOUSE (2008) https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf [https://perma.cc/3L6G-QBDD] [hereinafter *Cyber Security Social Contract*] (explaining that traditional modes of information transmission in the government do not work for cybersecurity); Nelly Rosenberg, *An Uphill Battle: FTC Regulation of Data Security as an Unfair Practice*, 66 DEPAUL L. REV. 1163, 1171-72 (decrying the patchwork agency jurisdictions that characterize cybersecurity).

[9] *See, e.g.*, Elizabeth Montalbano, *Government, Private Sector Unprepared for 21st Century Cyber Warfare*, SECURITY LEDGER (Feb. 7, 2019), https://securityledger.com/2019/02/government-private-sector-unprepared-for-21st-century-cyber-warfare [https://perma.cc/K89Z-YTSG]; Sean Doherty, *Why cyber defense ultimately rests with the private sector*, FCW (Mar. 31, 2015), https://fcw.com/security/2015/03/why-cyber-defense-ultimately-rests-with-the-private-sector/207593 [https://perma.cc/F3TU-MSNY].

operations so as to shut them down and prevent them.[10] This meant that responses to a threat varied predictably, with the government searching for emails or messages that could identify the responsible actor, and industry members shunning such evidence in favor of intelligence on the attack's structure.[11]

The ranks of cyber victims in the second decade of the twenty-first century quickly swelled with prominent names within both government and industry. Stuxnet struck in 2011,[12] and Red October and Shamoon in 2012.[13] Between 2010 and 2013, the United States Chamber of Commerce,[14] Google,[15] the New York Stock Exchange and several financial service providers,[16] the White House,[17] the Alabama State Government,[18] the Probation Office for the Eastern District of Michigan,[19] important media outlets including the *New York Times* and *Wall Street Journal*,[20] Nationwide Mutual Insurance Company,[21] Facebook, Twitter, Reddit, and Microsoft[22] all fell victim to cyberattacks. Fear of cybercriminals and cyberespionage skyrocketed, and experts posited that cybercrime was "professionalizing" to increase sophistication and success of attacks.[23]

By 2013, President Obama admitted the failures of early approaches to either allow the market to arrive at an ideal solution or smother the market in regulation.[24] With Executive Order 13,636 and Decision Directive 25, Obama called for creating voluntary public-private partnerships that would collaboratively define standards and best practices for both industry and the government.[25] This order borrowed from the Cybersecurity Social Contract

---

[10] *See* Montalbano, *supra* note 9; *see also* Sasha Romanosky, *Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?*, LAWFARE (Dec. 21, 2017), https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government [https://perma.cc/AT5S-RB5Q].
[11] *See id.*
[12] *See* Teplinsky, *supra* note 6, at 270-71 (listing prominent cyber attack victims).
[13] *See id* at 248, 270.
[14] *See id* at 248.
[15] *See id.*
[16] *See id.*
[17] *See id.*
[18] *See id.*
[19] *See id.*
[20] *See id.*
[21] *See id.*
[22] *See id.* at 248-49.
[23] *See id.* at 250.
[24] *See Public-Private Partnerships*, *supra* note 2 (describing the evolution of Executive Order 13,636 and Decision Directive 25).
[25] *See id.*

presented by industry leaders and privacy advocates grouped together as the Internet Security Alliance.[26] Among the Cybersecurity Social Contract's principles was the notion that neither an entirely voluntary, laissez-faire approach nor a top-down regulatory attack would combat cybersecurity problems facing the country.[27] Instead, a collaborative model would properly incentivize industry officials, the least-cost avoiders, to enforce practices that were appropriately responsive.[28]

B. The Concept Primer: Soft Law

Already at this early stage, the elements were in place for a new style of governance to flourish: rejection of both wholesale laissez-faire and regulatory approaches in their pure academic form, trust in cybersecurity industry experts as government advisors, and a whole corpus of official speeches and guidance documents praising the value of industry-government collaboration. "Soft law" refers to a style of governance that eschews binding or enforceable rules and instead leads by example.[29] Interpretive rules, certain

---

[26] *See id.* (claiming that the orders borrowed heavily from the Cybersecurity Social Contract); *see also Cyber Security Social Contract, supra* note 8 ("Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and hence would not be comprehensive enough. A US law could put US industry at a competitive disadvantage at a time we can least afford it. Specific regulations would be too static as technology and threat vectors change. An effort for flexible regulations may be too general to have real affect [sic]. Regulations may be weaker than needed due to constant political pressure. Minimum standards can become de facto ceilings (e.g. campaign finance). It would be extremely difficult to enact legislatively wasting valuable time.").

[27] *See Cyber Security Social Contract, supra* note 8, at 36 ("Neither the laissez faire approach of the Bush Administration's National Strategy to Secure Cyber Space nor a system of federally determined mandates are likely to succeed in accomplishing our goals.").

[28] *See id.* at 5-8 (describing why the past laissez-faire model and the current regulatory model are doomed to fail, and how a properly structured voluntary model would improve outcomes).

[29] *See* Ryan Hagemann, Jennifer Huddleston Skees, & Adam Thierer, *Soft Law for Hard Problems: Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 42-46 (2018) (defining the "rough contours" of hard and soft law); Gary E. Marchant & Brad Allenby, *Soft Law: New Tools for Governing Emerging Technologies*, 73 BULL. ATOMIC SCIENTISTS 108, 108 (2017) ("All around the world, governments, industry, and the public are struggling to realize the promising benefits . . . and manage the disruptive impacts . . . of one rapidly emerging technology after another."); Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706, 712-17 (2010) (defining hard and soft law); CLYDE WAYNE CREWS, MAPPING WASHINGTON'S LAWLESSNESS: AN INVENTORY OF REGULATORY DARK MATTER 2017 EDITION 20, 49 (2017), https://cei.org/sites/default/files/Wayne%20Crews%20%20Mapping%20Washin

kinds of guidance documents, and even industry standards developed by public-private partnerships and enforced within the private sector have all been classified as soft law.[30] Soft law operates by creating new incentives that motivate companies' voluntary compliance.[31]

Soft law as a concept will receive fuller treatment in sections to come. The reader will see how it gripped policymakers' minds at the time of rising action in this narrative and, most compellingly, how it offered a route towards reliable cybersecurity policy, a goal of the government, despite a stymied Congress.

C. Playing Favorites in Antitrust: Governmental Reliance upon the Private Sector and Failure to Pass Protective Legislation

The government quickly became dependent upon the private sector to ply it with cybersecurity information. Private companies possessed superior skills and tools and lacked the overlapping agency jurisdictions that made it difficult for the federal government to progress.[32] By the late 1990s, numerous private groups were already collaborating with the government in threat detection, enforcement of better standards than a red-taped-up government could produce, security training and compliance, and more. These groups commonly operated as research consortia, a kind of joint venture (a term to be defined more fully in coming sections). Not only did they share cyber intelligence with law enforcement and help train agencies in security best practices, but many also collaborated on the substance of their research, getting greater mileage out of shared resources.

As competitor collaborations, these groups raised antitrust red flags. Nevertheless, the government had a long and storied

---

gton%27s%20Lawlessness%202017.pdf [https://perma.cc/6CT8-W6F2] (offering some examples of soft law).

[30] *See* Hagemann et al., *supra* note 29, at 44-46 (stating different types of guidance that can be understood as soft law).

[31] Agency law is clearly implicated in any discussion of soft law, but it is beyond the scope of this paper, which specifically focuses on antitrust. For a thorough treatment of administrative standards of deference in regard to soft law, *see id.*, at 112-129.

[32] *See* Doherty, *supra* note 9 (describing overlapping authority and red tape in the federal agencies); *see also* Chuck Brooks, *Public Private Partnerships And The Cybersecurity Challenge Of Protecting Critical Infrastructure*, FORBES (May 6, 2019), https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/?sh=64007df65a57 [https://perma.cc/6HQH-ZP9Y] (emphasizing need for private co-governance of critical infrastructure).

history of carving out special antitrust treatments specifically for competitor collaborations whose projects served the national interest, and it had no intention of stopping now. Its guiding principle, the avoidance of overdeterrence, had perhaps best been articulated by the Court in *United States. v. United States Gypsum Co.*:

> The imposition of criminal liability …for engaging in such conduct *which only after the fact is determined to violate the statute because of anticompetitive effects*…holds out the distinct possibility of overdeterrence; *salutary and procompetitive conduct lying close to the borderline of impermissible conduct might be shunned by businessmen* who chose to be excessively cautious in the face of uncertainty regarding possible exposure to criminal punishment for *even a good-faith error of judgment* (emphasis added).

438 U.S. 422, 441 (1978). The government knew that, because it lacked effective deterrence and information-gathering tools of its own, "excessive[] cautious[ness]" on the part of its cybersecurity partners could lead to digital disaster.[33] As such, it paved a path in antitrust to improve clarity of standards and to encourage cybersecurity industry members to continue working with each other and with the government. Early steps included business review letters and legislation protecting joint ventures in the areas of concern. As data breaches intensified, though, calls mounted for major cybersecurity information-sharing legislation.[34]

Congressional efforts flailed; in two years, over fifty bills were introduced and rejected.[35] The very reason for these bills' introduction was also what made them so hard to pass. Each bill focused on the sharing of information between the public and private sector, acknowledging the by now widely-held notion that

---

[33] *See* Sanford Kadish, *Some Observations On the Use of Criminal Sanctions in Enforcing Economic Regulations*, 30 U. CHI. L. REV. 423, 441-442 (1963) ("Even where there is no immediate choice, the effect could sometimes be to influence persons to arrange their affairs to reduce to a minimum the possibilities of accidental violation; in short, to exercise extraordinary care. Further, the persistent use of such laws by legislatures and their strong support by persons charged with their enforcement makes it dogmatic to insist they cannot deter in these ways.").

[34] *See, e.g.*, Kathleen B. Rice, Mary Bono & Robert J. Ehrich, *Congress Must Pass Cyber Legislation Before Next Attack*, LAW360 (Oct. 31, 2014), https://www.law360.com/articles/590230/congress-must-pass-cyber-legislation-before-next-attack [https://perma.cc/GC6G-J67K].

[35] *See* Brian B. Kelly, *Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U.L. REV. 1663, 1687 (Oct. 2012) (describing the enormous number of rejected bills during this phase).

government could not succeed in cybersecurity without the help of industry. Though all of Congress agreed that cooperation would be critical to the eventual bill's success, the goal of cooperation itself also exposed the government to noisy scrutiny from civil liberties watchdogs, who accused the bills of creating loopholes for the NSA to spy on American citizens.[36]

This Article argues that the DOJ and FTC rose to the occasion at this time and filled the gap left by Congress's failed efforts via "soft law" in the form of a Joint Policy Statement that, while not enforceable or binding, gave joint ventures the go-ahead on information sharing. Section II discusses how "soft law"[37] may have proven an ideal method for governing, at least in the interim, a rapidly evolving entity that the government was ideologically and practically committed not to ensnare under regulations or legislation. Moreover, antitrust guidance provided an appealing backdoor route away from the outcries of watchful privacy activists.

Sections III and IV present case studies of two cybersecurity private-public partnerships operating during the early 2010s, when the main events of this Article took place. The groups were chosen to represent two of the models that these partnerships may use. Though they differ in membership and scope, both groups discussed served as clearinghouses for industry leaders to share information with each other and with the government. The groups also facilitated industry leaders in aiding the government in enforcement, improvement of standards, and other cybersecurity best practices. These Sections discuss how the partnerships not only provided the government with cybersecurity intelligence but also aided in its regulatory tasks.

Section V describes how research consortia or joint ventures tend to share information, both during the time of this narrative and in the past, and how the government has implicitly promoted these practices. We overview the difficulties associated with defining a joint venture and determining which antitrust tests apply, especially before interventions like the 2000 Joint Guidelines on Competitor Collaboration, and how they potentially created a threat of overdeterrence as articulated in *Gypsum*. We also analyze how the government solved this problem for competitor collaborations

---

[36] *See* Mike Masnick, *Forget SOPA, You Should Be Worried About This Cybersecurity Bill*, TECHDIRT (Apr. 22, 2012), https://www.techdirt.com/articles/20120402/04425118325/forget-sopa-you-should-be-worried-about-this-cybersecurity-bill.shtml [https://perma.cc/FFF8-W7XU].

[37] *See, e.g.*, Shaffer & Pollack, *supra* note 29; *see also infra* Section II.

whose projects it favored, such as the semiconductor industry or the Toyota/GM collaboration, by selectively underenforcing antitrust laws or treating collaborative efforts as joint ventures rather than mergers.

Sections VI-IX chronicle the government's evolving promotions of cybersecurity information-sharing joint ventures. Through a variety of traditional legislative methods such as the National Cooperative Research Act and "soft law" mechanisms such as policy statements and business review letters, the government encouraged joint ventures in certain areas to share information freely, so long as these joint ventures did not directly pertain to pricing or other bases of per se violations. These Sections prove two points. First, they provide evidence that promoting information sharing in innovation sectors was a governmental priority. Second, they suggest that the agencies were helping to fill a gap for Congress as it struggled to pass an information-sharing law. The 2014 Joint Policy Statement on Cybersecurity is entirely redundant and self-consciously so, given the document's extensive quoting of its predecessors. Because it seems unlikely that the FTC and DOJ would spontaneously collaborate on a joint statement—a rare occurrence—that merely rehashed their previous guidance, this supports the conclusion that the agencies were doing what they could to aid Congress in its repeated salvos toward a cybersecurity information-sharing law.

Section X considers the conflicts associated with passing the Cybersecurity Information Sharing Act of 2015 and the failure of other information-sharing laws in the early 2010s, just before the 2014 joint guidance was issued. The long march toward a cybersecurity law suggests that, despite early commitments not to clog the security space with mandates, the government keenly felt a need for further standard-setting and struggled to meet this need via the legislative process. This created a gap that the 2014 Joint Guidelines ultimately filled.

Finally, Section XI considers the implications of such a narrative for antitrust, cybersecurity, and governance in general. We comment on the difficulty of passing legislation, particularly when it affects areas highly salient to the public, such as digital privacy. We speculate that, in line with what other commentators have observed, "soft law" may capture the bulk of future technology governance. We then reflect on what this means for joint-venture jurisprudence and antitrust law's own conceptions of the per se rule and rule of reason.

II. DOJ, FTC, AND SOFT LAW

Legal scholars have increasingly drawn attention to "soft law," as opposed to traditional legislation and regulatory guidance, and its ascendancy in areas of science and technology.[38] Whereas "hard law" describes all standardized government procedures and outcomes, including both formal and informal administrative rulemaking,[39] "soft law" covers, in the words of Professors Marchant and Allenby, "a variety of nonbinding norms and techniques," including "instruments or arrangements that create substantive expectations that are not directly enforceable."[40] Interpretive rules, certain kinds of guidance documents, and even industry standards developed by public-private partnerships and enforced within the private sector have all been classified as soft law.[41] The engines of soft law are "soft criteria," such as guidance documents, speeches at official events, multistakeholder processes, agency threats and inquiries, and other activities that give rise to "norms and techniques;" these criteria do not formally enforce soft law but rather promote it.[42] Though sometimes criticized as toothless, soft law operates by creating new incentives that motivate companies' voluntary compliance.[43] Many agencies, especially those, like the FDA, that regularly interact with emerging technologies, have been noted for releasing large volumes of soft law in the past ten years.[44]

Legal scholars posit that soft law is becoming a default mode of regulating innovation sectors for a few reasons. First, hard law commonly loses the arms race to regulate emerging technologies, which have evolved even further by the time the law catches up to them.[45] Second, in part because of this, tech juggernauts flee to more permissive jurisdictions in what is known as "innovation arbitrage," and the United States loses out on economic benefits.[46] Moreover,

---

[38] *See* Hagemann et al., *supra* note 29; Marchant & Allenby, *supra* note 29; Shaffer & Pollack, *supra* note 29; Crews, *supra* note 29.
[39] *See* Hagemann et al., *supra* note 29, at 42-43 (outlining hard and soft law).
[40] Marchant and Allenby, *supra* note 29, at 112.
[41] *See* Hagemann et al., *supra* note. 29, at 44-46 (stating different types of guidance that can be understood as soft law).
[42] *Id.* at 44 (describing how soft law changes behavior).
[43] *Id.* at 112-129.
[44] *Id.* at 47-48 (describing the FDA's heavy use of soft law).
[45] *See id.* at 68 ("Formulating such laws or agencies would be challenging and time-consuming. But more problematic is that such efforts would run up against the reality of the pacing problem – they would likely be outdated before they are even finalized.").
[46] *See id.* at 71-74 (describing the process of innovation arbitrage). Of course, the fact that hard law takes a long time to catch up to emerging tech has both positive and negative effects on those in the industry.

emerging technologies straddle wide and unexpected areas of law, and soft law enables all sectors involved to be meaningfully involved in regulation.[47] Antitrust may not deal directly with the technologies themselves, but it is almost always heavily implicated in the creation and distribution of innovations and is therefore an efficient area from within which to prevent certain harms. Indeed, the FTC has been observed to engage in quite a bit of soft law-making of its own, including in the area of cybersecurity,[48] and has increasingly used the mantle of the Federal Trade Commission Act §45(a) to prosecute companies for data security violations as "unfair or deceptive acts."[49]

The concept of soft law fits well within the story of cybersecurity and innovation regulation that will unfold in the following sections: industry standards and nonbinding policy statements as the main policy vehicle, a focus on incentives and voluntary compliance, and a preoccupation with clarity of standards as a way to reduce overdeterrence. Indeed, soft law filled gaps in this area and seemed to have done the work of regulation that Congress was unable to do. Nevertheless, the fully functioning soft-law mechanisms did not satisfy the desire for a massive cybersecurity law, which culminated in the Cybersecurity Information Sharing Act (CISA) of 2015, a year after the DOJ/FTC Joint Policy Statement on Competitor Collaboration. This suggests that soft law, while useful and maybe even more functional than some other interventions, may often be temporary, and in any event does not supplant the need or desire for traditional forms of governance.[50] We return to this theme in the conclusion.

---

[47] *See id.* at 68 (referring to the problem of agency overlap and how soft law solves this problem).

[48] *See id.* at 48-49 ("The FTC's partnership with the Better Business Bureau's National Advertising Division, for example, aims to use more self-regulatory mechanisms as an alternative to more heavy-handed approaches."); *see also* FTC, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Jan. 2015) [https://perma.cc/35CL-PFKA].

[49] *See* 15 U.S.C. §§ 45(a), 53(b); FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (bringing a case against a company for unfair or deceptive data security practices that violated what the company advertised); *In re* LabMD Inc., 2015 FTC LEXIS 272 (2016) (exemplifying another case against a company for unfair practices and deceptive advertising of its data security protocols); *see also* Amanda R. Moncada, Comment: *When a Data Breach Comes A-Knockin', the FTC Comes A-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches*, 64 DEPAUL L. REV. 911, 921-24.

[50] *But see* Hagemann et al., *supra* note 29, at 46 ("In modern times, however, soft law systems have become more formalized and more prevalent across federal agencies, often pursued as the first—and sometimes only—option.").

III. CASE STUDY: INFORMATION SHARING AND ANALYSIS CENTERS

In 1998, President Clinton signed Presidential Decision Directive 63, encouraging entities in critical infrastructure sectors to share cyber risk information among themselves and with the federal government.[51] Soon, twenty-five different sectors each had their own Information Sharing and Analysis Center (ISAC), which still operate today.[52] Commonly structured as nonprofit entities, ISACS serve as trusted providers of information. They set cybersecurity threat levels for their industries,[53] maintain 24/7 response systems,[54] and broker the exchange of technical information on cyber threats.[55] Not only do these ISACs facilitate information among all of their members, but they alert the government, too.[56] In many instances, they can respond more rapidly to cyberthreats than the government.[57]

The flowchart of information-sharing within each ISAC varies. For the purposes of this paper, the Health ISAC (H-ISAC) will furnish an example, as it began operating early during the second decade of the twenty-first century, when the action central to the paper took place. The group was founded in 2010 to facilitate cybersecurity information sharing and data security practices among hospitals, medical providers, medical device manufacturers, and other members of the health care sector.[58]

---

[51] *See About ISACs*, NATIONAL COUNCIL OF ISACS, https://www.nationalisacs.org/about-isacs [https://perma.cc/H8FJ-49BL] (chronicling the history of ISACs).

[52] Sectors with ISACS currently operating in 2021 include chemistry, automotive, aviation, telecommunications, small broadband providers, downstream natural gas, elections infrastructure, electricity, emergency management and response, financial services, health care, information technology, maritime, media and entertainment, national defense, oil and natural gas, real estate, research and education, retail and hospitality, public transportation, water, space, and federal-state-local branches of government. *See id.*

[53] *See id.*

[54] *See id.*

[55] *See id.*

[56] *See Home*, NATIONAL COUNCIL OF ISACS, https://www.nationalisacs.org [https://perma.cc/H42E-4D4S] (stating that the National Council of ISACs is "designed to maximize information flow across the private sector critical infrastructures and with government"); *see also Frequently Asked Questions*, HEALTH ISAC, https://h-isac.org/h-isac-faq/ [https://perma.cc/6MW3-7T76] (stating that "on occasion, whenever a sector wide threat is apparent, de-identified cybersecurity threat and vulnerability information is shared with appropriate intelligence agencies for mitigation and incident response purposes").

[57] *See id.* (stating that "many ISACs have a track record of responding to and sharing actionable and relevant information more quickly than government partners").

[58] *See Frequently Asked Questions*, *supra* note 56.

H-ISAC vets its members, which may be providers, insurers, public health departments, medical device manufacturers, pharmaceutical companies, and more. All members must pay a fee to join, with higher fees granting greater access to H-ISAC's offerings. H-ISAC then investigates the applicant for compliance with various laws and regulations, such as HIPAA.[59]

Once accepted, members can access security programs and trainings designed to detect and mitigate threats. One of H-ISAC's main projects is "sharing timely, actionable and relevant information [among members] including intelligence on threats, incidents and vulnerabilities that can include data."[60] The central organization hosts a portal into which members can upload any indicators of compromise, as well as insight into the tactics of cyberthreats.[61] H-ISAC then alerts its members of this crowdsourced intelligence so that they can secure their systems.[62] Numerous working groups, with names ranging from Supply Chain to Policy and Governance to Third Party Risk, permit members to collaborate.[63] H-ISAC also trains members on data security best practices. For instance, it encourages all members to adopt and train their employees on the Traffic Light Protocol, a uniform system developed by H-ISAC for denoting the sensitivity of various communications. This is meant to help prevent data from falling into the wrong hands.[64] H-ISAC also publishes data security best practices for various nonmember organizations in the health sector, so as to help members avoid being compromised via an unwise partnership.[65] Members can also access shared services at a discount to help streamline their security practices, such as an identity verification program or a third-party risk management program.[66]

H-ISAC collaborates with the government in a variety of ways. Government agencies, including global law enforcement entities, number among H-ISAC members. Hence, they benefit from alerts when others upload a threat, make use of the uniform Traffic

---

[59] *See id.*
[60] *Id.*
[61] *See id.*
[62] *See id.*
[63] *See I-ISAC Committees & Working Groups*, HEALTH ISAC, https://h-isac.org/committees-working-groups [https://perma.cc/XFF9-XDZA].
[64] *See Traffic Light Protocol*, HEALTH ISAC, https://h-isac.org/h-isac-tlp-definition [https://perma.cc/9WAK-A937].
[65] *See Medical Device Manufacturing Security*, HEALTH ISAC, https://h-isac.org/mdm-security [https://perma.cc/WQ9G-5JCA].
[66] *See Shared Services*, HEALTH ISAC, https://h-isac.org/shared-services/#ThreatIntel [https://perma.cc/E5W9-7FGD].

Light Protocol as a common ground for coordinating within the government and with private partners, and access the trainings and shared services.[67] When certain sector-wide threats arise, H-ISAC shares de-identified information with intelligence officials to craft a response.[68]

H-ISAC, in line with the other ISACs, engineers incentives to promote a safer culture of cybersecurity for both members and nonmembers. For instance, if most of the sector's companies are H-ISAC members and comply with the Traffic Light Protocol, they will expect their partners to do the same, even if they are not members, to avoid undermining the entire sector's safety. Similarly, organizations that do not want the formality or expense that comes with membership may still be swayed by the loss of business that will accompany a negative security rating from H-ISAC, so they alter their practices to match. The Traffic Light Protocol also promotes safer security practices within a vast government bureaucracy, which may otherwise be compromised by a single weak link. H-ISAC thus benefits the government by providing intelligence on current threats and evidence for enforcement against cyberattacks. Perhaps more to the point, however, it tremendously relieves the government of standard development, enforcement, and compliance duties.

IV. CASE STUDY: INTERNATIONAL GENE SYNTHESIS CONSORTIUM AND COLLABORATION WITH THE FBI

While attending a 2009 conference hosted by the FBI, five independent DNA synthesis companies realized that protocols for cybersecurity and request tracking within their field were inadequate, and that they, not the government, had the knowledge to formulate a better system.[69] Together, they jointly adopted a screening protocol for requests for biological materials and mechanisms for tracking these requests, and they dubbed themselves the International Gene Synthesis Consortium (IGSC).[70] The IGSC quickly amassed an 80% worldwide membership rate

[67] *See Traffic Light Protocol*, *supra* note 64.
[68] *See Frequently Asked Questions*, *supra* note 56.
[69] *See* James Diggans and Emily LeProust, *Next Steps for Access to Safe, Secure DNA Access*, 7 FRONTIERS IN BIOENGINEERING AND BIOTECHNOLOGY 1, 1 (2019) (describing the birth of IGSC); Comments of Damon Terril to IGSC, pp. 3-4, 2010, Philadelphia, PA, https://genesynthesisconsortium.org/wp-content/uploads/IGSC-Presentation-at-PCSBI-9_14_10.pdf [https://perma.cc/CA8G-ZCXP] (mentioning that the IGSC was the brainchild of genetics companies gathered at an FBI conference).
[70] Comments of Damon Terril to IGSC, *supra* note 69.

among manufacturers of synthetic DNA, and its membership continues to grow internationally.[71]

IGSC members collaborate amongst themselves and with the FBI to ensure genetic material does not fall into the wrong hands—and that bad actors do not exploit loopholes in cybersecurity practices to obtain these materials.[72] Under the IGSC Harmonized Screening Protocol, all participating companies investigate a customer who has placed an order, the gene they have requested, and whether the desired sequence is appropriate for this customer.[73] First, the company screens potential clients against the Office of Foreign Asset Control's Specially Designated Nationals List, the Department of State's Debarred List, the Bureau of Industry and Security's Denied Persons, Entity, and Unverified lists, the HADDEX exports and sanctions lists, and any other list required by relevant national regulations.[74]

Next, the company screens the gene order, as well as its full amino acid sequence, against a Regulated Pathogen Database maintained internally by the IGSC.[75] It includes data for all organisms on a number of national lists of regulated pathogens, including the Select Agent list and the Australia Group list. The company also screens the requests against internationally coordinated sequence reference databanks. The Harmonized Screening Protocol's requirements are both stricter and more up-to-date than those of the United States Select Agents and Toxins or

---

[71] *See id.*; *see also International Gene Synthesis Consortium Updates Screening Protocols for Synthetic DNA Products and Services*, CISION NEWSWIRE (Jan. 3, 2018), https://www.prnewswire.com/news-releases/international-gene-synthesis-consortium-updates-screening-protocols-for-synthetic-dna-products-and-services-300576867.html?tc=eml_cleartime [https://perma.cc/JS7Q-X2KD].

[72] *See* International Gene Synthesis Consortium, *Harmonized Screening Protocol*, GENE SYNTHESIS CONSORTIUM 1, 1 (Nov. 19, 2017), https://genesynthesisconsortium.org/wp-content/uploads/IGSCHarmonizedProtocol11-21-17.pdf [https://perma.cc/YQV4-CNM3] (offering a preamble to the protocol).

[73] *See id.* at 1-2 (stating customer review mechanisms).

[74] *See id.* at 2 ("Potential customers are screened against OFAC's SDN List, the Department of State's Debarred List, and BIS's Denied Persons, Entity, and Unverified lists, or the HADDEX list, and/or any other list required by applicable national regulations.").

[75] *See id.* at 3 ("IGSC members collaborate to: 7.1. Update annually the IGSC Regulated Pathogen Database to include all gene sequences identified as potentially hazardous by authoritative groups such as the CDC, the Australia Group, and the U.S. and European governments. 7.2. Ensure that we use the best and most effective algorithms to screen gene sequences against the Regulated Pathogen Database.").

Commerce Control lists.[76] In 2017, the IGSC added a rule against producing sequences involving variola virus DNA in response to non-binding World Health Organization recommendations, which had not yet been adopted by the Centers for Disease Control.[77]

If the request runs afoul of one of these lists, IGSC members will grant the request only if the customer is a verified government lab, university, non-profit, or industry researcher engaging in legitimate work.[78] The IGSC grants requests only to end users, so they are certain that their customers will not provide their materials to others downstream.[79] Despite these safeguards, the IGSC exercises caution and denies riskier requests even to reliable users, as in the case of an academic research team that requested and was denied the building blocks of a disease resembling smallpox.[80]

---

[76] *See id.* ("IGSC members screen the complete DNA sequence of every synthetic gene order against the DNA sequences in a common Regulated Pathogen Database (RPD), and against all entries found in one or more of the internationally coordinated sequence reference databanks (i.e., NCBI/GenBank, EBI/EMBL, or DDBJ). The IGSC has assembled and curated the RPD to include data from all organisms on the Select Agent list, the Australia Group List, and other national lists of regulated pathogens. This database is shared and deployed amongst IGSC members where members frequently supplement their biosecurity systems with additional sequence data. As a baseline, IGSC companies screen against all pathogen and toxin genes as specified in the US Select Agents and Toxins List, the US Commerce Control List, and the EU list of dual-use items.").

[77] *See id.* ("IGSC members will not synthesize gene sequences unique to and derived from Variola virus DNA."); *see id.* at 4 (showing this policy as a non-binding recommendation of the WHO).

[78] *See id.* at 2 ("Although the U.S. Select Agent Regulations and the European Commission regulations do not restrict access to all Select Agent genes, IGSC members supply genes from regulated pathogens only to researchers in bona fide government laboratories, universities, non-profit research institutions, or industrial laboratories demonstrably engaged in legitimate research. Customers ordering Select Agent or Australia Group DNA fragments must provide a written description of the intended use of the synthetic product; we verify independently a) the identity of the potential customer and purchasing organization, and b) that the described use is consistent with the activities of the purchasing organization.").

[79] *See id.* ("In general, IGSC members only sell DNA or fragments of regulated pathogens to bone fide end-users. We do not sell or ship such material to distributers or other resellers, unless those companies identify the end-user receiving the products and demonstrate their compliance with every requirement otherwise applicable to that end user.").

[80] *See* Nell Greenfield Boyce, *As Made-To-Order DNA Gets Cheaper, Keeping It Out Of The Wrong Hands Gets Harder,* NPR, (Sept. 24, 2019), https://npr.org/sections/health-shots/2019/09/24/762834987/as-made-to-order-dna-gets-cheaper-keeping-it-out-of-the-wrong-hands-gets-harder [https://perma.cc/LD2U-68U3] (recounting the case of the denied request based on an interview with IGSC members).

Regardless of the outcome, the IGSC records every screening and delivery and retains that record for a minimum of eight years.[81] Thus, when screening a potential customer, companies can check the database to see if the requesting party has been making similar requests of other companies and the outcome of these requests. This helps to prevent "venue shopping" among various companies.[82] In certain events, the IGSC makes use of its "established relationships with local and national law enforcement and intelligence authorities"[83] and shares customer information with the FBI to mitigate potential threats.[84] Companies within the IGSC periodically engage in red-teaming, a practice lifted from cybersecurity, where somebody knowledgeable is charged to try hacking into a system to see how secure it is.[85] Thus, they regularly ensure the integrity of their database.

The IGSC makes government collaboration a cornerstone of its Harmonized Screening Protocol. It helps the FBI to develop pilot programs in related fields and assists the governments where it operates in improving their oversight, as well as promoting international coordination.[86] It incorporates forward-thinking enforcement into new areas, such as by advocating for all grant applications to include a safety and cybersecurity section and for young scientists to be taught early about security awareness.[87] The IGSC also makes enforcement much easier for the government. First, the government simply does not have the expertise or flexibility to develop standards of the same quality as IGSC, which partially instigated its formation in the first place. Second, by preventing harms through this extensive screening process and advising the government on policy, the IGSC reduces the amount of work involved in government enforcement. It also collects information to expedite government action when threats do arise.

V. HOW PRIVATE RESEARCH CONSORTIA SHARE INFORMATION (AND HOW ANTITRUST POLICY FAVORS THEM)

---

[81] *See Harmonized Screening Protocol*, *supra* note 72, at 2.
[82] *See* Diggans & LeProust, *supra* note 69, at 4.
[83] *See Harmonized Screening Protocol*, *supra* note 72, at 2.
[84] *See* Comments of Damon Terrill, *supra* note 69, at 3-4 (describing IGSC collaborations with the FBI).
[85] *See* Diggans & LeProust, *supra* note 69, at 2 (recounting IGSC's red-teaming procedures).
[86] *See* Comments of Damon Terrill, *supra* note 69, at 3-4 ("The IGSC member companies have worked closely with federal law enforcement, most especially with the Federal Bureau of Investigation as it developed its Pilot Program for reporting by gene synthesis companies of problematic orders.").
[87] *See* Diggans & LeProust, *supra* note 69, at 6 (promoting these as novel preventative measures for cybersecurity).

H-ISAC and IGSC are just two examples of the many public-private partnerships whereby industry members collaborate amongst themselves, both for security and for research and development (R&D), and share information with the government as well as with each other. These arrangements commonly take the form of research consortia, a form of joint venture.

Research consortia have procompetitive benefits and efficiencies. For instance, they can reduce the search costs in acquiring know-how or factual knowledge, pool intellectual property and skilled professionals, and reduce costs associated with production and pass those savings onto consumers. However, collaboration among competitors smacks of antitrust violations. For one, it runs the risk that the competitors will become too cozy and start to share more than just information pertaining to research or cybersecurity. As David Clanton, former FTC commissioner and academic, has put it, "Cooperative endeavors among competitors pose a dilemma for antitrust analysis because they offer the prospect of simultaneously enhancing and restricting interbrand competition."[88] The fear of antitrust suits has, at times, evidently been enough to dissuade some companies from engaging in research consortia.[89]

In antitrust, many research consortia are best understood as a type of joint venture. Loosely, a joint venture can be defined for antitrust purposes as temporary and partial integration of independent entities, or in the words of some commentators, an "ad hoc partnership."[90] Professor Joseph Brodley has defined joint ventures as those collaborations where a) an enterprise is jointly controlled by parent entities, which are not under related control, b) the enterprise exists as a business entity separate from either of these

---

[88] David A. Clanton, *Horizontal Agreements, the Rule of Reason, and the General Motors-Toyota Joint Venture*, 30 WAYNE L. REV. 1239, 1240 (1984).

[89] *See* Evan Wolff, David Laing, Elizabeth Blumenfeld, & Kate M. Growley, *Industry Collaborations on Cybersecurity*, 29 CRIM. JUST. 31, 32 (2014) (reporting how many companies found that "The line between lawful information-sharing among competitors and an 'agreement in restraint of trade' that violates the Sherman Act can at times be difficult to discern."); *see also* Business Review Request Letter of Barbara Greenspan, Associate General Counsel of EPRI, to Joel Klein, Assistant Attorney General 4 (2000), https://www.justice.gov/sites/default/files/atr/legacy/2014/01/08/302319.pdf [https://perma.cc/4DFQ-5TYP] (explaining how participants in a previous program had been wary of sharing information until the DOJ explicitly cleared the practice for similar programs).

[90] *See* N. LATTIN, R. JENNINGS & R. BUXBAUM, CORPORATIONS: CASES AND MATERIALS 35 (4th ed. 1968) (citing Christopher O.B. Wright, *The National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures*, 1 HIGH TECH L.J. 122, 145 (1986)).

parents, c) each parent substantially contributes to the enterprise, and d) the enterprise creates new capabilities that neither of the parents themselves had.[91] Joint ventures need not always result in a new marketing entity; some create new standards and a collaborative protocol for internal policing of the industry.[92] Currently, the National Cooperative Research and Production Act statutorily defines a joint venture for its own purposes, including particular activities the entity may undertake.[93]

Especially before the advent of this statutory definition, however, ambiguity surrounded joint ventures in antitrust. Many different types of collaborations could be called joint ventures. Indeed, one scholar observed that the heterogeneity of joint ventures precluded the adoption of any single set of rules.[94] Nor was there a natural occasion for courts to clarify the category of joint ventures; in antitrust litigation, an entity's status as a joint venture mattered less than the competitive effects of its actions. Therefore, because the proper way to analyze joint ventures was generally not the main issue, the Court had not had occasion to articulate a standard definition.

Because of the legal ambiguity, joint ventures had long faced uncertainty about whether courts would evaluate them under the per se rule or rule of reason. As multiple scholars have noted, the Court has applied both of the main antitrust analyses under §1 of the Sherman Act, the rule of reason and per se rule,[95] to joint ventures, even in cases where the facts were arguably similar.[96] In *Broadcast Music, Inc. v. Columbia Broadcasting System, Inc.*, Broadcast Music functioned as a joint venture among artists[97] and served as an intermediary in negotiations with individual users, offering a

---

[91] *See* Joseph F. Brodley, *Joint Ventures and Antitrust Policy*, 95 HARV. L. REV. 1521 (1982).
[92] *See* Clanton, *supra* note 88, at 1240.
[93] *See* 15 U.S.C. § 4301(6) (defining a joint R&D venture). In general, because this paper will be discussing history, this act will be referred to in its 1984 version, as the National Cooperative Research Act, rather than its amended name of the National Cooperative Research and Development Act of 1993. Deviations from this will be noted.
[94] *See* Clanton, *supra* note 88, at 1265.
[95] We will define both of these at greater length in Section VI.
[96] *See id.* at 1243-44 (classifying the present cases as joint ventures and describing the discrepancy in the Supreme Court's treatment of the cases); *see also* Thomas A. Piraino, Jr., *Beyond Per Se, Rule of Reason or Merger Analysis: A New Antitrust Standard for Joint Ventures*, 76 MINN. L. REV. 1, 17, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=3438&context=mlr [https://perma.cc/26PW-MYXW] (outlining the inconsistency of the cases).
[97] This was broadly defined to include composers, writers, and publishers. *See* 441 U.S. 1, 15 (1978).

blanket license to BMI's accumulated works. This resulted in a "fixed price" because it was simply easier to offer the same terms and conditions each time than for the artists to negotiate individually for each song. The Court applied the rule of reason, finding that cooperation to license copyrighted music was critical to the market's function, as it was "impracticab[le to] negotiat[e] individual licenses for each composition."[98] It found that, while a price had literally been agreed upon by multiple artists, because these artists' collaboration allowed them to meaningfully participate in a market that was otherwise stacked against them, this could not be price-fixing of the anticompetitive sort that antitrust guarded against.[99]

Four years later, in *Arizona v. Maricopa County Medical Society,* the Court seemingly deviated from this ruling by applying the per se rule, not the rule of reason, to the actions of the Maricopa Foundation for Medical Care. The Maricopa Foundation functioned as a joint venture among doctors and served as their intermediary in dealings with insurance carriers, setting maximum fee schedules. The doctors argued that this was akin to BMI's blanket licenses and not a true instance of price-fixing.[100] The Court rejected the Maricopa doctors' attempts to align the actions of their joint venture with those of Broadcast Music, calling the cases "fundamentally different;"[101] the Maricopa Foundation for Medical Care produced no competitive offering and merely allowed the doctors to sell their services at higher rates, whereas the collaboration in BMI did produce a new competitive offering by making the licensing process feasible for artists.[102] Hence, the venture's actions were not necessary to the market in the way BMI's had been. Though these decisions may have intuitively appealed to many, scholars have pointed out that, conjunctively, they demonstrate a lack of clear precedent for evaluating joint ventures.[103] Although the question of

---

[98] 441 U.S. 1, 15 (1978).
[99] 441 U.S. 1, 9, 20 (1978).
[100] *See* 457 U.S. 332, 339-43 (1982).
[101] *Id.* at 356.
[102] *See id.* (explaining why the cases are "fundamentally different").
[103] *See, e.g.,* Clanton, *supra* note 88, at 1244 ("Read together, *Broadcast Music* and *Maricopa* leave unsettled the question of what kind of factual showing is necessary to trigger the rule of reason."); Piraino, *supra* note 96, at 16-17 ("In several subsequent cases, however, the Court confused the implications of its holding in Broadcast Music by continuing to apply a standard of summary illegality to various restrictions incidental to competitors' cooperative arrangements. In *Arizona v. Maricopa County Medical Society*, for example, the Court applied the per se rule when a physicians' organization established maximum fees that its members could charge under an insurance plan . . . . The Court concluded that even when potential efficiencies are involved, 'the anticompetitive potential inherent in all price-fixing agreements justifies their

whether an action was necessary to the business seemed to predict which rule would be applied, it proved difficult to distill from these cases what facts would need to be proven to show cooperation was a necessary practice. Indeed, lower courts struggled to apply the rulings.[104]

Even had it been clear whether joint ventures merited the per se rule or rule of reason, haziness surrounded *what*, exactly, constituted a joint venture, as opposed to a merger. This mattered because structural market merger review under §7 of the Clayton Act and the Horizontal Merger Guidelines deviates from both of the tests of §1 of the Sherman Act.[105] Modern merger review imposes a stepwise inquiry wherein the agency defines the relevant product and geographic markets and then assesses each party's share of those markets, the present market concentration and resultant increase in market concentration should the merger complete, the resultant risk of anticompetitive harms in light of any entry or efficiency considerations, and whether one of the firms would fail if not for the merger.[106] Especially in previous decades, if a merger would produce a firm that would control an "undue percentage share"—the threshold for which, at points in history, could be quite low—of a market, and so would result in a significant increase in the concentration of that market, then the merger would be "so inherently likely to lessen competition substantially that [the merger] must be enjoined" absent clear evidence that it would not produce these harmful effects.[107] Especially during the 1960s, the Supreme Court and lower courts sometimes reviewed joint ventures under §7 of the Clayton Act using a structural market approach, in addition to assessment under §1 of the Sherman Act using the per se rule or rule of reason.[108] As Professor Thomas A. Piraino, Jr. has

---

facial invalidation.' Consideration of efficiencies, however, is precisely what the Court had appeared to mandate in Broadcast Music.").

[104] *See* Clanton, *supra* note 88, at 1246-49 (describing how lower courts struggled in evaluating the rule in the wake of these holdings).

[105] *See id. at* 1258 (describing the lack of clarity on distinguishing mergers and joint ventures). *See also* Paraino, *supra* note 96, at 22 (arguing that the current approach leaves joint ventures unsettled as to whether they will be treated as mergers).

[106] *See* DEP'T OF JUST. & FED. TRADE COMM'N, *Horizontal Merger Guidelines* (1992, revised 1997), available at https://www.usdoj.gov/atr/public/guidelines/hmg.html [https://perma.cc/CN3M-M4RU].

[107] *See generally* United States v. Philadelphia National Bank, 374 U.S. 321 (1963) (describing a style of merger review that has since given way.) The percentage share found to be impermissibly high was around 30%.

[108] *See* United States v. Penn-Olin Co., 378 U.S. 158 (1964) (applying the structural market analysis reminiscent of merger analysis to a joint venture); *see also* Piraino, *supra* note 96, at 12-14 (discussing the case).

observed, merger analysis was unpredictable and expensive for the parties to litigation, and so may have dissuaded companies from embarking upon joint ventures for fear of being subjected to this rule.[109]

The difference between mergers and joint ventures was eventually elucidated in a 2000 Joint Policy Statement of the FTC and DOJ. Mergers "completely end competition between the merging parties in the relevant market(s)"[110] and are meant to be permanent.[111] Joint ventures, on the other hand, are often temporary, and participants continue to compete or at least retain the possibility of competing.[112] Hence, joint ventures should be evaluated under the rule of reason and not be subject to merger inquiry. The FTC and DOJ have since articulated that they treat competitor collaborations as horizontal mergers, triggering application of merger analysis, only when a) the participants are competitors in the relevant market, b) the collaboration involves an integration of economic activity that creates efficiencies in the relevant market, c) the integration of economic activity obliterates competition among the collaborators in that relevant market, and d) the collaboration does not have some provision whereby it will terminate within a specific and sufficiently limited time.[113] The 2000 Joint Guidelines thus pacified fears about whether joint ventures needed to worry about being treated as mergers. For years, however, joint ventures had lacked this assurance.

Even before definitions were forthcoming, one thing was clear: the United States government needs its joint R&D ventures, and it has long shown a willingness to pave the way for joint ventures where the enterprise serves some interest of the government, such as promoting international competitiveness in technology or the sciences, so long as it is not blatantly sharing pricing information or carving up the market. One example comes from the semiconductor industry, which, for decades, and especially through the 1970s, operated an informal joint venture to develop and bring semiconductors to market. As extensively chronicled by Professor Richard Levin, the major semiconductor companies held

---

[109] *See* Piraino, *supra* note 96, at 15. This is, of course, not untrue of the rule of reason.

[110] U.S. FED. TRADE COMM'N & U.S. DEP'T OF JUST., *Antitrust Guidelines for Collaborations Among Competitors* 5 (2000) [hereinafter *2000 Joint Guidelines*].

[111] *See id.*

[112] *See id.*

[113] *See id.* at 5 (announcing these factors).

symposia for each other to share know-how[114] and cross-licensed their patents extensively.[115] (Levin wrote that, when one firm dared to accuse another of infringement, "the accused firm usually respond[ed] by proclaiming its innocence and sending the accuser 'a pound or two' of possibly germane patents which it believe[d] the accuser to be infringing."[116]) This structure made sense in light of their market structure, which was too dynamic for any one firm to control. Semiconductors involved a plethora of parts, and each innovation launched a technology race from which only a few firms emerged into the new product market. Because dozens of these product markets appeared at any point in time, with each firm dividing its efforts, no single firm seemed likely to succeed in more than a few.[117] Many of these innovations were not patentable because they were either subject matter ineligible or highly inconvenient, given rampant cross-infringement (meaning it was not possible to seek a patent without infringing on some untold number of other patents) and industry-wide aversion to the legal process.[118] Moreover, in such a new area, progress came spasmodically and did not always track scientific theory, making continued success unreliable even for the most prominent companies.[119] Entry costs were also low, and key personnel moved companies frequently.[120] Early transistors were expensive to produce and required finicky procedures, from whose know-how all could benefit.[121] Moreover, the innovation was coveted by the US government, particularly the military, and Levin describes how the government created a favorable environment for the nascent semiconductor industry via public procurement of semiconductors and support for research and production.[122]

The government also created favorable conditions through its antitrust policy—specifically, by the failure to pursue strict antitrust outcomes against the companies involved. At a time when the antitrust acceptability of joint research ventures would have been even more in question than today, the government may not have acted decisively to produce certainty for research joint ventures, but

---

[114] *See* Richard Levin, *The Semiconductor Industry*, in GOVERNMENT AND TECHNICAL PROGRESS: A CROSS-INDUSTRY ANALYSIS 77 (Richard Nelson, ed.) (1982) (relating the open sharing of know-how among participating companies).
[115] *See id.* at 81.
[116] *Id.* (citing von Hippel, 1982).
[117] *See id.* at 31 (explaining the peculiar market characteristics of the semiconductor industry).
[118] *See id.* at 36-37.
[119] *See id.* at 41.
[120] *See id.* at 28-29, 78.
[121] *See id.* at 42.
[122] *See id.* at 57-58.

it did allow the ventures to flourish without intervening. In 1949, the Department of Justice filed an antitrust suit against Western Electric and its parent company, AT&T, not for its semiconductor patent pool, but for dividing the broadcasting market.[123] The upshot of seven years of litigation was a settlement making all AT&T patents royalty-free and preventing AT&T from entering any market other than common carrier communications, except to provide services to the government.[124] Levin points out that this did little other than formalize AT&T's corporate policy; it was already freely sharing its semiconductor patents with its collaborator/competitors, and for years it had not attempted to penetrate the consumer semiconductor market, preferring to contract with the government.[125] From this, Levin concluded that the threat of antitrust held different power, at different times, for the companies involved. AT&T took mincing steps during the years of its antitrust litigation, whereas other firms in the semiconductor industry were not restrained in this fashion.[126] Nevertheless, its behaviors were not truly constrained, as the settlement it reached was highly permissive.[127] In contrast, Bell, another semiconductor company which was not under government scrutiny during the time of AT&T's settlement, cross-licensed with abandon and hosted symposia where it shared "everything [it] knew" with competitors.[128] This was based in part on the fact that an attempt to hoard semiconductor licenses to itself would invite lawsuits from other competitors, and in part on a realization that the technology was too large for one firm alone to meaningfully

[123] *See id.* at 75.
[124] *See id.*
[125] *See id.* at 75-76 ("Interestingly, the consent decree did little other than ratify what was already the corporate policy and practice of AT&T").
[126] *See id.* at 76 ("The naive inference to be drawn from this recitation of facts is that antitrust policy had no effect on AT&T's behavior, and hence no impact on the structural and technological evolution of the semiconductor industry. But the issue requires a more subtle treatment. Clearly, in the years following the invention of the transistor and prior to the consent decree, AT&T operated under severe constraint. Any attempt to dominate the youthful semiconductor industry would have surely jeopardized its antitrust case. Nevertheless, it is at least arguable that Bell would have behaved no differently even in the absence of antitrust prosecution.").
[127] *See id.* at 75 ("Interestingly, the consent decree did little other than ratify what was already the corporate policy and practice of AT&T.").
[128] *Id.* ("According to [a] Bell executive, 'There was nothing new about licensing our patents to anyone who wanted them. But it was a departure to tell our licensees everything we knew' (attributed to Jack Morton, cited in Tilton, 1971)."). *See also id.* ("In addition to licensing its patents liberally, Bell held a series of landmark symposia on semiconductor technology at which it conveyed substantial information and know-how to its licensees . . . . This policy . . . further supports the view that antitrust policy was not decisive in [Bell's] decision to spread transistor technology.").

develop.[129] To firms in Bell's position, Levin reasoned, antitrust may not have made much of a difference in strategy, though the consent decree on AT&T may have made it easier for Bell to rise in the industry.[130] Either way, at a time when the research behavior's legality would have been in doubt, antitrust created a space for the semiconductor industry to continue collaborating, so long as its violations were not blatant. It is impossible to overlook the government's (and military's) eagerness for semiconductor technology as a motivating factor.

Similarly, scholars writing in 1984, who were contemporaries of the proposed twelve-year joint venture between Toyota and General Motors to build and sell a new small car, chastened the FTC for allowing its desire for the economic fuel of this collaboration to motivate a "significant departure from [its approach in] other joint venture cases."[131] This case took place before the 2000 Joint Guidelines articulating standards for when to evaluate a joint venture as a merger, and at least some scholars had expected it would be handled as a merger.[132] Instead, the Federal Trade Commission blessed the agreement as a joint venture, so long as its parent companies agreed to a consent order limiting the venture's output and the exchange of competitively sensitive price and marketing data.[133] In its statement, the FTC rendered an analysis that heavily weighted efficiencies. First, the FTC noted the procompetitive benefits, which included increased total output of small cars available to the United States, a car that would be cheaper for GM to produce than other options, and an opportunity for GM to learn about Japanese manufacturing and management.[134] Anticompetitive harms were dismissed as being "of low probability or small magnitude when balanced against the procompetitive benefits of the joint venture."[135] The FTC concluded the market was diversified enough that there was no great risk after the joint venture ended that parties would continue the exchange of sensitive pricing data, tacit or express collusion, and ongoing collaborations.[136] The FTC further wrote that the venture should not be considered a merger because "the areas of continued competition between the

[129] *See id.* at 77 ("the transistor was probably just too big and too important to be effectively exploited within one organization").
[130] *See id.* at 75-79.
[131] Clanton, *supra* note 88, at 1263. *See also* Piraino, *supra* note 96, at 10 (commenting on the Toyota-GM joint venture).
[132] *See id.* at 1257-61.
[133] *See id.* at 1257 (relating the events).
[134] Statement of Federal Trade Commission at 3, 6 (citing Clanton, *supra* note 88, at 1258).
[135] *Id.* at 6.
[136] *Id*. (describing the FTC's analysis of the joint venture).

companies will dwarf the limited area of cooperation."[137] Thus, "traditional concentration analysis, whether expressed through Herfindahl's or other measures, will be of limited value."[138] Professor and prior FTC commissioner David Clanton, writing just a year after the FTC gave this blessing, argued that the FTC's analysis of this matter more closely resembled a rule of reason inquiry under §1 of the Sherman Act than it did a Clayton Act §7 merger analysis, which had seemed to be the rule at least for joint ventures that had not demonstrated necessity of the act—and a very forgiving one at that. [139] Clanton also accused the FTC of treating cost savings and efficiencies as dispositive rather than weighing them alongside other factors, observing, "Even if a venture with another Japanese partner might be more efficient than GM going it alone, the fact that Toyota is the least costly partner appears dispositive to the commission and its staff."[140] Nowhere did the FTC claim this arrangement was necessary or essential. Clanton later remarked on his surprise, given the FTC's typical reluctance to accept efficiencies as a defense to horizontal mergers, that the FTC accepted efficiencies defenses so readily, especially managerial efficiencies, which are frowned upon in the Horizontal Merger Guidelines (newly articulated at the time) as hard to quantify.[141] The fact that contemporaries were surprised by the FTC's choice to treat this as a joint venture, not a merger, points to the confusion at the time over how each kind of business arrangement would be treated. The doctrine-lite departure from horizontal merger precedent also points to motivated reasoning on the part of the FTC, which, at the same time, was wary of losing innovation competitions to Japan, Germany, or France, whose antitrust laws were less strict.[142] Once again, the GM-Toyota venture exemplifies ways in which the antitrust agencies have always permitted a wider berth to

[137] *Id.* at 3.
[138] *Id.*
[139] *See id.* at 1257-61 (critiquing the FTC's reasoning and decision).
[140] *Id.* at 1261.
[141] *See id.* at 1262 ("Typically, antitrust commentators and authorities have expressed reservations about the feasibility of accepting an efficiencies defense to horizontal mergers; more specifically, they have expressed strong reservations about the practicability of a managerial efficiency defense.").
[142] *See* Christopher O.B. Wright, *The National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures*, 1 HIGH TECH L.J. 122, 139 (1986) ("In considering antitrust exemptions for cooperative research ventures, some members of Congress seemed particularly concerned American antitrust laws were much stricter than those of our competitors. 'Our major trading partners—Japan, Germany, and France, for example—have all sanctioned collaborative efforts on development,' noted Congressman Henry Hyde (R.-Ill.)."). As described in note 93, I will refer to it by its pre-amendment name throughout this section as it is a history.

collaborative efforts that advance the country in science and technology, so long as their antitrust violations are not overt.

The following sections describe how various branches of the government have enacted this antitrust preference for beneficial R&D programs by carving out safety zones in legislation and regulation.

VI. THE NATIONAL COOPERATIVE RESEARCH ACT OF 1984

The National Cooperative Research Act (NCRA) of 1984 exemplifies the government's granting leeway to research joint ventures insofar as they further the government's goals. By 1984, the United States feared the loss of innovation battles to other countries with more permissive antitrust laws.[143] Congress rallied to pass a law clarifying to research joint ventures that they could proceed with innovation without fear of antitrust consequences. Indeed, the bill passed with strong bipartisan support for the bill.[144]

The National Cooperative Research Act of 1984 (later amended as the National Cooperative Research and Production Act of 1993)[145] softened a number of antitrust provisions for certain kinds of joint ventures that engaged in R&D favored by the U.S. government. First, the NCRA of 1984 defined a group of research efforts that would receive special treatment in antitrust—specifically, research projects in the areas of scientific or technological innovation, which were desirable to the government. Especially because the NCRA was codified well before the 2000 Joint Guidelines on competitor collaborations, defining joint ventures for the purpose of this statute created much-needed clarity.[146] The statute's definition included

---

[143] *See id.*

[144] *See id.* at 143-44 (describing the bill's bipartisan support and the successful compromise-brokering in its passage).

[145] Because I am commenting on this bill from a historical perspective, I will mostly refer to it as the NCRA, not the NCRPA. The only real change of the 1993 amendment was to include production joint ventures, which simply expanded the number of joint ventures that stood to benefit from this law. *See* Charles D. Weller, *A "New" Rule of Reason from Justice Brandeis' "Concentric Circles" and Other Changes in Law*, 44 ANTITRUST BULL. 881, 893 (1999) ("The 1984 Act provided three types of antitrust relief to research and development joint ventures. The NCRPA extended the 1984 protections to many 'production' joint ventures.").

[146] *See* John A. Maher and Nancy Lamont, *National Cooperative Research Act of 1984: Cartelism for High Tech?*, 7 DICKINSON J. INT'L LAW 1, 7-13 (1988) (describing at length the definition of joint venture in the statute).

> any group of activities . . . by two or more persons for the purpose of . . . a) theoretical analysis, experimentation, or systemic study of phenomena or observable facts, b) the development or testing of basic engineering techniques, c) the extension of investigative findings or theory of a scientific or technical nature into practical application for experimental and demonstration purposes . . . , d) the production of a product . . . , e) the testing in connection with the production of a product…, [or] f) the collection, exchange, and analysis of research or production information . . . .

15 U.S.C. § 4301(a)(6)(a-f) (1984). A subsequent 1993 amendment folded into this definition joint ventures "engaged in production."[147] Scientific research groups that qualified under the NCRA's definition were still barred from "exchanging information among competitors relating to [production . . . if such information is not] reasonably required to carry out the purpose of such venture, entering into any agreement . . . restricting [the] marketing . . . of any product,"[148] or "any other conduct" that might tend towards anticompetitive behavior.[149]

The NCRA then specified the treatment these joint R&D ventures, as well as standards development organizations, should expect in antitrust. First, it instructed courts to use the more flexible rule of reason, rather than the stricter per se rule, in judging "any action under the antitrust laws, or under any State law similar to the antitrust laws,"[150] against qualifying joint R&D ventures.

A pause is warranted here to explain the two main analyses in antitrust for §1 of the Sherman Act, the per se rule and rule of reason.[151] The per se rule is reserved for agreements or activities in restraint of trade that are "so likely to harm competition and to have no significant procompetitive benefit that they do not warrant the time and expense required for particularized inquiry into their

---

[147] *See id.*
[148] 15 U.S.C. § 4301(a)(6), (b) (1984).
[149] *See* 15 U.S.C. § 4301(b)(1-8).
[150] *See* 15 U.S.C. § 4302.
[151] *See generally* Herbert Hovenkamp, *The Rule of Reason*, 70 FLA. L. REV. 81, 122-24 (2018). In developing this body of doctrine, the Supreme Court has articulated new intermediate tests like the quick look and sliding scale, and has debated whether these analyses differ in kind or in degree. *See, e.g.*, California Dental Ass'n v. FTC, 526 U.S. 756, 780 (1999) (endorsing the sliding scale model).

effects."[152] Especially before the 1970s, the Supreme Court was quick to strike horizontal restraints among competitors as per se illegal, regardless of any pro-competitive efficiencies.[153]

The rule of reason is a more flexible and often defendant-friendly inquiry,[154] its motivation having been classically articulated by Justice Brandeis in *Chicago Board of Trade v. United States:* to decipher

> whether the restraint imposed is such as merely regulates, and perhaps thereby promotes competition, or whether it is such as may suppress or even destroy competition. To determine this question, the court must ordinarily consider the facts peculiar to the business…not because a good intention will save an otherwise objectionable regulation, or

---

[152] *2000 Joint Guidelines*, *supra* note 110, at 3. *See, e.g.*, FTC v. Superior Court Trial Lawyers Ass'n, 493 U.S. 411, 432-36 (1990) (finding that a group boycott with the intent to force a price change is a per se violation of §1 of the Sherman Act); United States v. Topco Assocs., Inc., 405 U.S. 596, 609 n.10 (1972) (finding that an agreement to divide a market into exclusive territories per se violates §1 of the Sherman Act); United States v. Socony-Vacuum Oil Co., 310 U.S. 150 (1940) (finding that horizontal price-fixing agreements per se violate §1 of the Sherman Act).

[153] *See* Piraino, *supra* note 96, at 15 (noting the court's rampant use of the per se rule in prior to the late 1970s).

[154] Courts, in applying the rule of reason, have established a framework for shifting the burden of proof at trial. As observed by Hovenkamp, *supra* note 151, at 102, ("Assignment of the burden is frequently dispositive of the outcome [in antitrust]. Indeed, very likely the principal reason that plaintiffs go to such lengths to bring their case within the boundaries of the per se rule or the so-called 'quick look' is that they cannot carry an evidentiary burden requiring them to demonstrate power and anticompetitive effects."). Under the rule of reason, the plaintiff must allege and prove that the defendants possess the requisite market power to create anticompetitive harms and that they have, in fact, imposed the harms. If the plaintiff states this prima facie case, the burden switches to the defendant to provide procompetitive justifications. If the defendant then meets this burden, the burden returns to the plaintiff to show that these procompetitive benefits could have been achieved through less restrictive ends. *See, e.g.*, California Dental v. FTC, 526 U.S. 756 (1999). Especially at the summary judgment stage, the court may employ a sliding scale and require more evidence for a less plausible claim. *See* Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986). As a result, plaintiffs (commonly the government, at least at the start of proceedings) favor the per se rule, and defendants (commonly private actors) typically favor the rule of reason. This paper would not be complete without at least acknowledging this central feature of the rule of reason. Nevertheless, many companies in this sector are savvy repeat players with good counsel. At issue for them is not so much *why* they would prefer to be reviewed under the rule of reason, but how certain they can be ahead of time that their actions, if they do offend antitrust laws, will be reviewed under this test. As such, I will not dwell further on burden shifting.

> the reverse, but because knowledge of intent may help the court to interpret facts and to predict consequences.

246 U.S. 231, 238-39 (1918). Brandeis then lists the elements that the court ought to consider, such as the business's condition before and after the restraint, the restraint's nature, and its effects, both actual and probable.[155] Contemporary rule-of-reason analyses tend to probe into the character of the agreement, including the business purpose and whether any anticompetitive harm has already resulted; a detailed market analysis, including market shares, concentration, and the incentives of all participants to compete; other market circumstances, such as entry or incentives, that may prevent or precipitate harms; any procompetitive benefits or efficiencies; and the availability of less restrictive substitutes.[156] When applying the rule of reason to cases of information sharing among competitors, the Court has emphasized two factors in particular: the structure of the market—such as the competitive status of the parties, the fungibility of the products, or the market concentration—and the attributes of the information shared—such as the competitive sensitivity of the information, the effect of these exchanges, or their availability to the public or to other government agencies.[157] The Court has also tended towards the rule of reason when the parents of a joint venture kept their brands separate and continued to compete.[158]

---

[155] *See* Chicago Board of Trade, 246 U.S. at 238-39 (listing these as factors to consider when applying the rule of reason). *See also* Michael A. Carrier, *The Rule of Reason: An Empirical Update for the 21st Century*, 16 GEO. MASON L. REV. 827, 828 (2009) ("Courts dispose of 97% of [rule of reason] cases at the first stage, on the grounds that there is no anticompetitive effect. They balance in only 2% of cases.").

[156] *See 2000 Joint Guidelines*, *supra* note 110, at 4, 10-25; *2014 Joint Policy Statement* at 5. *See, e.g.*, FTC v. Indiana Fed'n of Dentists, 476 U.S. 447, 459-61 (1986) (applying the rule of reason); National Collegiate Athletic Ass'n v. Board of Regents of the Univ. of Okla., 468 U.S. 85, 104-13 (1984) (applying the rule of reason).

[157] *See* LEXISNEXIS, *§8: Information Gathering and Reporting*, in THE LAW OF ASSOCIATIONS 1-3 (1975) [hereinafter THE LAW OF ASSOCIATIONS] (listing these factors as critical in rule of reason cases for information sharing among competitors). *See also* United States v. United States Gypsum Co., 438 U.S. 422, n.16 (stating that the two "most prominent" factors in the rule of reason analysis of a data exchange are "the structure of the industry involved and the nature of the information exchanged").

[158] *See* Texaco v. Dagher, 547 U.S. 1, 3 (2006) (permitting a joint venture between two gas stations evaluated under the rule of reason because the competitors retained their separate brands and continued to compete). *See also* THE LAW OF ASSOCIATIONS, *supra* note 157, at 10 for a discussion of ancillary effects in joint venture analysis.

Thus, in telling joint R&D ventures to expect a rule of reason analysis, the NCRA accomplished two things. First, it created certainty for joint ventures where none had previously existed. Second, it promised joint ventures that they could rely upon the more easygoing rule of reason being used. The NCRA even went so far as to direct courts that, as part of the market-analysis step of the rule of reason, "worldwide capacity shall be considered to the extent that it may be appropriate in the circumstances."[159] Defining the relevant market as larger, in many cases, would decrease the market concentration measure and, therefore, the likelihood that joint R&D ventures would be found in violation of antitrust laws. Thus, the direction to consider worldwide capacity where appropriate would likely lead to more permissive treatment in antitrust of joint R&D ventures embraced under the NCRA.

Even more benefits accrued to the joint R&D ventures that chose to register with the Federal Trade Commission. To qualify, a joint venture would identify its parties, nature, and objectives, to be published in the Federal Register.[160] Registration was purely voluntary and, of course, imposed some risk-benefit analysis upon the companies in deciding whether and to what extent to reveal the nature of their work. Those who registered, however, were protected from paying treble damages if they were found, even with the more generous rule of reason, to have violated antitrust law.[161]

Thus, the NCRA, later amended as the NCRPA, established a pattern of gentler antitrust treatment of businesses that the government favors, particularly in science and innovation sectors. Implicit in its language is the notion that, if a company is engaged in business that serves the government's interests, the courts ought to consider this favorably – not just by applying the less strict judicial analysis, not just as a procompetitive benefit, but even in the seemingly empirical area of market definitions.

VII. 2000 GUIDELINES FOR COLLABORATION AMONG COMPETITORS

In 2000, the DOJ and FTC created even more certainty for science-based collaborations that were sharing information with each other and, critically, the government. They did so in a joint policy statement – a prime example of soft law and a rare collaboration between these agencies, which underscored its

[159] 15 U.S.C. § 4302.
[160] *See* 15 U.S.C. § 4305 (a).
[161] *See* 15 U.S.C. § 4303(a)(1).

importance.[162] The 2000 Joint Guidelines on Collaboration Among Competitors set favorable new policies for collaborating entities, especially in areas of innovation, and studded the document with plentiful examples and hypotheticals to improve confidence in proceeding as advised.

In the Guidelines, the agencies set out "safety zones" for certain collaborative arrangements among competitors.[163] These were meant "to provide participants in a competitor collaboration with a degree of certainty in those situations in which anticompetitive effects are so unlikely that the Agencies presume the arrangements to be lawful without inquiring into particular circumstances."[164] The general market safety zone provided that the agencies would not challenge a collaborative effort where the combined market shares of the collaboration and its participants accounted for no more than 20 percent of each relevant market.[165] The safety zones for "innovation markets," those markets "consist[ing] of the research and development directed to particular new or improved goods or processes and the close substitutes for that research and development,"[166] were even more freewheeling than those for general markets. For innovation markets, the agencies did not impose a market share requirement, but rather promised not to challenge a collaboration where at least three competitors not in the collaboration *could* enter into R&D that was "a close substitute" for the collaboration's activity.[167] A "close substitute" could be determined by, "among other things, the nature, scope, and magnitude of the R&D efforts; their access to financial support; their access to intellectual property, skilled personnel, or other specialized assets; their timing; and their ability, either acting alone or through others, to successfully commercialize innovations."[168] This list created a wide berth to consider potential entrants capable of producing close substitutes. The Guidelines further clarified that these safety zones extended to a wide range of collective efforts, so long as they did not behave as a merger or run afoul of other antitrust

---

[162] *See* Wolff et al., *supra* note 89, at 33 (2014) (referring to the practice of issuing joint statements, albeit in response to the 2014 joint statement, as "rare"). The DOJ and FTC had also recently collaborated on joint statements for the areas of intellectual property (1995) and health care (1996). Their analyses are similar to the 2000 statement and so will not be treated in depth, but their existence further underscores how keen the government was to promote cross-licensing and other collaborations in science and technology.
[163] *See 2000 Joint Guidelines*, *supra* note 110, at 25-27.
[164] *Id.* at 29.
[165] *See id.* at 26.
[166] *Id.* at 17.
[167] *Id.* at 27.
[168] *Id*.

laws.[169] Throughout, they relied upon case studies and examples to elaborate upon the rule and make it clear to readers, including an entire appendix of hypothetical cases and analyses.[170]

This guidance proceeded by first defining for readers the analyses used in antitrust, the per se rule and rule of reason, in language indicating the per se rule was rarely used. It characterized the per se rule as reserved for "certain types of agreements [that] are so likely to harm competition and to have no significant procompetitive benefit that they do not warrant the time and expense required for particularized inquiry into their effects."[171] The rule of reason, meanwhile, applied to "all other agreements."[172] The Guidelines explained that the DOJ and FTC default to the rule of reason even for agreements that might be considered per se illegal when those agreements are reasonably related to an efficiency-enhancing integration of economic activity and reasonably necessary to achieve procompetitive benefits.[173] This is because such agreements "benefit, or potentially benefit, consumers by expanding output, reducing price, or enhancing quality, service, or innovation."[174] One test upon which would-be collaborators could rely is "whether practical, significantly less restrictive means were reasonably available when the agreement was entered into,"[175] and the agencies assuaged readers that they would not search for an alternative that would not have been feasible.[176] This guidance

[169] *See id.* at 27 ("The antitrust safety zone does not apply to agreements that are per se illegal, or that would be challenged without a detailed market analysis, or to competitor collaborations to which a merger analysis is applied.").
[170] *See id.* at 28-35 (providing an appendix of examples).
[171] *Id.* at 3. The 2000 Joint Guidelines cited as exemplary of the per se rule the case FTC v. Superior Court Trial Lawyers Ass'n, 493 U.S. 411, 432-36 (1990).
[172] *Id.* at 3. The Guidelines here cited California Dental Ass'n v. FTC, 526 U.S. 756, 780 (1999); FTC v. Indiana Fed'n of Dentists, 476 U.S. 447, 459-61 (1986); National Collegiate Athletic Ass'n v. Board of Regents of the Univ. of Okla., 468 U.S. 85, 104-13 (1984).
[173] *See id.* at 8; *see also id.* at 30 (providing Example 4, a hypothetical involving two companies agreeing on prices for their software, a seeming per se violation. The example provides that "the agreement to jointly set price may be challenged as per se illegal, unless it is reasonably related to, and reasonably necessary to achieve procompetitive benefits from, an efficiency-enhancing integration of economic activity").
[174] *Id.* at 8.
[175] *Id.* at 9.
[176] *See id.* At 9. The Joint Guidelines cited to the by-now-infamous duo of *Maricopa County Medical Society* and *Broadcast Music* to illustrate the necessity rule. *See* Arizona v. Maricopa County Medical Soc'y, 457 U.S. 332, 339 n.7, 356-57 (1982) (finding no integration), 352-53 (observing that even if a maximum fee schedule for physicians' services were desirable, it was not necessary that the schedule be established by physicians rather than by insurers); Broadcast Music, 441 U.S. at 20-21 (setting of the price "necessary" for the blanket license).

combined to make the application of the rule of reason seem much more likely to a potential joint venture.

The 2000 Joint Guidelines next explained how competitor collaborations could avoid the heightened scrutiny of the Horizontal Merger Guidelines by avoiding agreements that permanently ended competition among the parties.[177] They articulated a four-part test to assess whether a collaboration was a horizontal merger: whether the participants were competitors in the relevant market, whether the collaboration involved an efficiency-enhancing integration of activity in that market, whether the integration eliminated all competition, and whether the collaboration is meant to terminate by itself within a limited period.[178]

To illustrate, the statement offered an example of two oil companies that agreed to integrate all of their refining and refined product marketing operations, but maintained separate crude oil operations. Their integration of operations was set to expire after twelve years or could be terminated by either party on six months' notice.[179] The sample analysis noted that the collaboration involved an efficiency-enhancing integration of operations in the refined and refining product markets, and that it eliminated competition between the participants in those markets.[180] Though the agreement limited itself to twelve years, this would likely not be found a "sufficiently limited period,"[181] and the provision allowing either party to terminate at any time is not a termination "by the collaboration's own specific and express terms."[182] Hence, the guidelines concluded that this agreement would be reviewed under the Horizontal Merger Guidelines.[183] The agencies warned that they would still evaluate the substance of agreements over their form: "In any case, labeling an arrangement a 'joint venture' will not protect what is merely a device to raise price or restrict output; the nature of the conduct, not its designation, is determinative."[184] By providing clear definitions and examples, the Policy Statement helped inform would-be collaborators of how to avoid running afoul of the Horizontal Merger Guidelines and to preserve their favorable treatment.

---

[177] *See id.* at 5.
[178] *Id.*
[179] *See id*. at 28 (presenting and analyzing Example 1).
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id* at 9; *see also* Timken Roller Bearing Co. v. United States, 341 U.S. 593, 598 (1951) (stating that a per se violation does not merit rule of reason analysis simply because the group called itself a joint venture).

The 2000 Policy Statement opened up the safety zones and guidance even to collaborations that did not formally call themselves joint ventures. In a sample analysis of procompetitive benefits under the rule of reason, the Agencies noted that "a variety of contractual arrangements including joint ventures, trade or professional associations, licensing arrangements, or strategic alliances"[185] may achieve procompetitive benefits cognizable by the rule of reason. The statement went on to list examples, such as production collaborations, marketing collaborations, buying collaborations, or research and development collaborations.[186] By this overt statement, the Guidelines acknowledged the definitional confusion surrounding joint ventures and expressed a willingness for all beneficial collaborations to proceed as though they would receive the favorable treatment accorded a joint venture. The Guidelines then noted that R&D collaborations might best be evaluated by the Intellectual Property Guidelines, which had been released in 1995.[187] These provided a "safety zone" for IP licensing restraints that were not "facially anticompetitive" and involved no more than twenty percent of each relevant market "significantly affected" by the restraint.[188] This represented a standard that was both more reliable and more lenient.

Altogether, the 2000 Guidelines serve as a prime example of soft law. While not strictly enforceable, the document creates clarity and induces reliance for industry readers, which in turn would promote their voluntarily engagement in collaborative practices that these policies were designed to favor.[189]

VIII. 2000 BUSINESS REVIEW LETTER TO ELECTRIC POWER RESEARCH INSTITUTE

2000 saw yet another influential bit of antitrust soft-law guidance on competitor collaboration, this one specifically in the realm of cybersecurity. The Department of Justice's Antitrust Division offers a review service for businesses to propose actions for review before committing to any potential antitrust liability. One such review, granted to the Electric Power Research Institute (EPRI)

---

[185] *Id* at 6.
[186] *See id.* at 13-14.
[187] *See id.* at 17.
[188] *See* DEP'T OF JUST. & FED. TRADE COMM'N, *1995 Antitrust Guidelines for the Licensing Of Intellectual Property*, section 4.3 (describing the safety zones). Because the analyses in this and the 2000 Joint Guidelines are so similar, but the Joint Guidelines are more influential, these guidelines were not discussed at length.
[189] *See* Hagemann et al., *supra* note 29, at 106 (discussing how soft law promotes clarity).

in 2000, is often cited and has formed the basis for much guidance in cybersecurity.

EPRI is a nonprofit organization promoting technology- and evidence-based solutions to problems within the energy industry. It publishes the results of its research and makes them available on a non-discriminatory basis, and membership in EPRI is open and voluntary.[190] At the time, EPRI had just concluded a program it called the "Year 2000 Embedded Systems Program," which facilitated the exchange of technical information about cybersecurity problems in embedded systems like electricity, oil, and natural gas.[191] EPRI noticed that participation in the Year 2000 program increased, meaning that members actually exchanged more information, after the DOJ issued favorable business review letters to similar programs in different fields.[192] In crafting a similar new program, the Enterprise Infrastructure Security (EIS) program, it therefore sought specific approval from the DOJ.[193]

In EPRI's request for sanction of its EIS program, it noted that Presidential Decision Directive 63 of 1998 had called for information sharing between companies and the government to promote the critical infrastructure necessary for cyber defense.[194] The EIS program, it explained, was open to all companies involved in the energy sector. It would provide a forum for collaboration on technical cybersecurity issues that arose by way of operating equipment, electronic information systems, or communications systems.[195] The information exchanged would be technical or related to security management, and would be related either to experience or principle.[196] The program would set explicit limits on sharing information about prices, services, or any other facet of competition.[197] Indeed, EPRI argued the EIS program would be pro-competitive, permitting the sector to address its risks efficiently.[198]

---

[190] *See* Business Review Request Letter of Barbara Greenspan, Associate General Counsel of EPRI, to Joel Klein, Assistant Attorney General 2 (2000), https://www.justice.gov/sites/default/files/atr/legacy/2014/01/08/302319.pdf [https://perma.cc/EA3M-9GKF] (describing the nature and activities of EPRI).
[191] *See id.* at 1.
[192] *See id.* at 1-2.
[193] *See id.* at 4 (describing the EIS), 7-8.
[194] *See id.* at 3 (gesturing to current events that made such programs important).
[195] *See id.* at 4.
[196] *See id*.
[197] *See id.* at 6.
[198] *See id.* at 7.

In a letter dated October 2000, the DOJ agreed with EPRI that its EIS program would not pose harm to competition.[199] It reiterated that the EIS program would not disadvantage any segment of the energy sector and that participation would be open and voluntary.[200] It premised its assessment upon EPRI's assurance that the only information exchanged would be technical: either cybersecurity "best practices" or vulnerabilities that members identified within their own systems.[201] The DOJ also described the measures EPRI had adopted to lessen the risk of anticompetitive harm, such as explicitly proscribing the sharing of price information or future market plans.[202]

The DOJ concluded that, on the basis of EPRI's description of the EIS program, "it does not appear that the proposed information exchange will restrict competition in any of the…markets in which the participants do business,"[203] so long as they continued limiting the information exchanged to technical cybersecurity issue.[204] The DOJ agreed that EIS could even be pro-competitive, if it resulted in "more efficient means of reducing cyber-security costs, and such savings redound to the benefit of consumers."[205]

The EPRI business review letters overtly acknowledge that sharing of cybersecurity information between private entities and the government was explicitly sanctioned and acknowledged by the DOJ as critical to the government's own efforts. As a result, it is no surprise that the EPRI letters form the basis of much guidance for R&D joint ventures.

IX. THE REDUNDANCY OF THE 2014 JOINT POLICY STATEMENT ON CYBERSECURITY INFORMATION-SHARING

As we have seen, as early as 1950 with the semiconductor industry and up through 2000 with the EPRI Business Review Letter and the Joint Guidelines, antitrust agencies carved out special treatment for research collaborative efforts and joint ventures in numerous ways, providing certainty through special inducements,

---

[199] *See* Business Review Letter of Joel Klein, Assistant Attorney General, to Barbara Greenspan, Associate General Counsel of EPRI 3-4 (2000), https://www.justice.gov/atr/response-electric-power-research-institute-incs-request-business-review-letter [https://perma.cc/8L2S-H3EP].
[200] *See id.* at 1-2.
[201] *See id.* at 2.
[202] *Id.* at 3.
[203] *Id.*
[204] *Id.*
[205] *Id.* at 4.

clear definitions and examples, the possibility of business review judgments, and safety zones. Nevertheless, in 2014, the DOJ and FTC again released joint guidance.[206] This was a rarity, as noted by commentators: "That the DOJ and FTC made the effort to reaffirm in a joint statement—a relatively rare event in federal antitrust enforcement—this long-standing policy is one more example of how the federal government is…encouraging greater cybersecurity in the private sector."[207] The 2014 joint statement merely rearticulated extant policy, the cybersecurity angle changing no part of the analysis.

The statement began with a preamble describing the importance of sharing cybersecurity information among private groups and the government as a prevention measure.[208] It acknowledged that this behavior was already occurring, but worried that fear of antitrust consequences could dissuade some groups from this helpful behavior (a statement for which it provided no evidence). Thus, its intent was to reduce uncertainty for would-be cybersecurity collaborators wary of antitrust concerns.[209]

The 2014 statement then articulated a rule of reason analysis for the sharing of cybersecurity information.[210] (The words "per se" do not appear anywhere in the document.) In so doing, though, it depended on previous guidance rather than sharing new content. It quoted entire paragraphs out of the 2000 Joint Guidelines when explaining the rule of reason.[211] When it provided a sample rule of reason analysis for the sharing of cybersecurity information, it lifted paragraphs directly from the 2000 EPRI business review letter.[212] What sample analysis it did provide was vague. Its predecessors had provided plentiful examples of fact-based analysis: the 2000 Guidelines created pages of case studies to provide clarity, and the EPRI letter responded to a real set of facts on cybersecurity information sharing. In contrast, the 2014 statement did not create any hypotheticals, despite observing in one place that "the nature of

---

[206] *See* Wolff et al., *supra* note 89, at 33 (2014) (describing the Joint Policy Statement at length).
[207] *Id.* at 34.
[208] *See* DEP'T OF JUST. & FED. TRADE COMM'N, *Antitrust Policy Statement on Sharing of Cybersecurity Information* 1, 1-4 (2014) [hereinafter 2014 Joint Policy Statement] (describing how ISACs and other exchanges share cybersecurity information with the government and reiterating this process's vitality to cyberdefense).
[209] *See id.* at 4.
[210] *See id.* at 5-8.
[211] *See id.* at 5, 6 (depositing long block quotes from the *2000 Joint Guidelines* into the text).
[212] *See id.* at 8-9 (using the EPRI review process as an example and quoting from the DOJ's response letter).

the information being shared is very important to the analysis"[213] and in another that "this type of analysis is intensely fact-driven."[214] Perhaps even more surprisingly, it began the sample analysis with the efficiencies and procompetitive benefits of cybersecurity information sharing, exhibiting the same hunger for financial benefits as the FTC did in its Toyota/GM review. One wonders whether the joint statement here subjects itself to the same criticism that Clanton leveled against the FTC while evaluating the GM/Toyota joint venture: that it treats efficiencies as "dispositive."[215] This lends support to the idea that, despite doctrine, the agencies believed that collaborations helping the government should be treated preferentially in antitrust. Due to their vagueness and failure to articulate new content, the 2014 guidelines are actually less specific and less informative than those upon which they sought to expand.

The 2014 guidelines implicitly admit their own redundancy in their heavy reliance upon earlier documents and failure to add anything novel of substance to the guidance. Nor was this policy statement's redundancy lost on the legal community at the time. In a *Law360* article entitled "Antitrust Guidance Reaffirms Old Approach," two lawyers observed that the substance of the statement was "not new."[216] Another article stated flatly, "The Cybersecurity Antitrust Statement affirms enforcement policies regarding information-sharing that the two federal antitrust agencies have articulated numerous times."[217]

At first, it seems perplexing that the two agencies would "ma[k]e the effort to reaffirm in a joint statement[,] a relatively rare event in federal antitrust enforcement,"[218] a corpus of policies that already fully covered the collaborations in question. However, the legislative context at the time may help to explain the joint statement. As the next section explores, Congress was badly stifled in its eagerness to pass major cybersecurity information-sharing legislation, repeatedly stymied by privacy advocates. The legal community seems to have been at least somewhat aware of this context; two attorneys in *Law360* wrote that though [the 2014 Policy Statement] is "consistent with prior DOJ guidance," it "is

---

[213] *Id.* at 7.
[214] *Id.* at 8.
[215] *See* Clanton, *supra* note 88, at 1265.
[216] Jamillia Padua Ferris & Paul M. Tiao, *Antitrust Guidance Reaffirms Old Approach,* LAW360 (Apr. 16, 2014, 3:11 PM), https://www.law360.com/articles/528873/antitrust-guidance-on-cybersecurity-reaffirms-old-approach [https://perma.cc/9XYX-HF3V].
[217] Wolff et al., *supra* note 89, at 33.
[218] *Id*. at 34.

significant," as "it does not appear likely that cybersecurity legislation will become law any time soon."[219] The FTC was also making strides elsewhere to pursue cybersecurity through antitrust, suing two major companies in federal court for inadequate data security practices that amounted to unfair trade practices in violation of 15 USC §45(a), substantially harming consumers.[220] Outside the strictures of formal legislation, the FTC and DOJ were using antitrust soft law to gap-fill for Congress.

Moreover, debates on the House and Senate floor centered around privacy, a major sticking point, as well as the correct alignment of incentives and enforcement mechanisms in the bills. It was largely agreed that "carrots," or voluntary incentives, would produce better results than "sticks," but architects of the bills disagreed on how to craft this framework. In such a setting, antitrust guidance might have seemed like a perfect solution: it would be watched less keenly by privacy and civil liberties activists than major bills and would not need to cut through the congressional gridlock. Furthermore, "soft law" guidance, such as Joint Policy Statements, would be well-positioned to create systems of voluntary compliance.[221]

X. FAILED ATTEMPTS AT INFORMATION-SHARING LEGISLATION

Beginning in 2011, a torrent of cybersecurity-oriented information-sharing bills materialized in Congress, were voted down, and then resurrected with some minor amendments, only to again be spurned. Though the desire for cybersecurity legislation was not necessarily shared by all,[222] Congress continued to propose bills that ultimately failed. This cycle continued until 2015, when the Cybersecurity Information Sharing Act of 2015 (CISA) finally passed.

The following paragraphs display the precise policies that sparked so much disagreement, but more importantly for this argument, they convey the strife that accompanied the stillbirth of each of these bills. Congress's repeated failure to pass any

[219] Padua Ferris & Tiao, *supra* note 216.
[220] *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re* LabMD Inc., 2015 FTC LEXIS 272 (2015). *See also supra* note 49.
[221] *See* Hagemann et al., *supra* note 29, at 85-91 (reaffirming the centrality of voluntary compliance in soft law methods).
[222] *See* Masnick, *supra* note 36 ("Even if we accept the mantra that new cybersecurity laws are needed (despite a near total lack of evidence to support this – and, no, fearmongering about planes falling from the sky doesn't count), this bill has serious problems.").

cybersecurity laws set the stage for antitrust to fill the gap via soft law.

The first major cybersecurity information-sharing bill was the PRECISE Act of 2011. This bill proposed to create a new semi-private group called the National Information Sharing Organization (NISO), which would be monitored by a board comprised of both public and private officials from government agencies and cyber-related companies.[223] The NISO would collect certain types of de-identified "cyber data," including "cyber threat information" or anything "necessary to identify or describe" the threat, and would distribute this information to its members. The federal government and private entities would be empowered to use this information for security purposes or to investigate or prosecute a cybercriminal.[224] It induced private entities to share their information with the NISO by protecting them against certain civil or criminal actions in both federal and state courts, so long as they shared the information with NISO.[225] This bill represented one of the first efforts at a cybersecurity information-sharing law, but it received no floor time and was not revived in subsequent congressional sessions.[226]

The next bill, the Cyber Intelligence Sharing and Protection Act of 2011 (later 2013), was even more embattled. CISPA created provisions for cybersecurity providers to share information "directly pertaining to" cyber threats with any private or governmental entity as long as the entity receiving the cybersecurity protection gave consent for this information to be shared.[227] Supporters of CISPA called it an "information-sharing bill"[228] and touted its alignment of

---

[223] *See* AM. C.L. UNION, *Comparison of Cybersecurity Information Sharing Legislation* (Mar. 2012), https://www.aclu.org/files/assets/aclu_cs_info_sharing_leg_chart_march_2012__final.pdf [https://perma.cc/4DWT-NYS5] (describing the cybersecurity bills introduced between 2011 and 2012); Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011, H.R. 3674, 112th Cong., § 243(b) (2011).

[224] *See* AM. C.L. UNION,, *supra* note 223; H.R. 3674 § 248(a)(2)-(3), (b)(3)-(4), (f)(2).

[225] *See* AM. C.L. UNION,, *supra* note 223; H.R. 3674 § 248(b)(6).

[226] ERIC FISCHER, CONG. RSCH. SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 8 (2014) https://fas.org/sgp/crs/natsec/R42114.pdf [https://perma.cc/VF9S-HTWU].

[227] *See* AM. C.L. UNION, *supra* note 223; Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong., § 2 (2011) [hereinafter CONGRESSIONAL RESEARCH SERVICE].

[228] *See* Teplinsky, *supra* note 6, at 286; Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475, 1494 (describing CISPA along with other information-sharing bills).

incentives to promote voluntary sharing between the private sector and government.[229] Tech commentators quickly denounced CISPA, decrying its "broad definitions, very few limits on who can get the data, almost no limitations on how the government can use the data (i.e. they can use it to monitor, not just for cybersecurity reasons) and (of course) no real oversight at all for how the data is (ab)used."[230] Critics accused the government of trying to incentivize companies to send private communications data to the NSA and foster its "spy[ing] on people."[231] CISPA passed in the House in 2012, but the Obama administration objected to its "overly broad liability protections for private-sector entities and insufficient protections for individual privacy, confidentiality, and civil liberties,"[232] and it did not pass the Senate. The same bill was reintroduced in 2013 and met the same fate.[233]

The SECURE IT Act of 2012, another revival of a previous Senate bill, met with no more success, although its sponsors attempted to learn from the mistakes of their forebears by providing that any customer or client would have "reasonable opportunity" to object to their cybersecurity provider sharing their data.[234] Also branding itself as an "information-sharing" bill,[235] it provided that the nine types of cyber data it statutorily defined could be shared with existing cybersecurity centers within the federal government or "any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security."[236] The SECURE IT Act did not give the government any new regulatory powers, instead relying upon a market-based, voluntary approach.[237] Nevertheless, the SECURE IT Act was, as with the others, wildly unpopular. Civil liberties activists called the bill a "back-door wiretap"[238] enabling the NSA to snoop on private citizens, claiming

---

[229] *See id.*
[230] Masnick, *supra* note 36.
[231] *Id.*
[232] CONGRESSIONAL RESEARCH SERVICE, *supra* note 227, at 7 n.24.
[233] *See id.* at 8 (describing failure of CISPA).
[234] *See* AM. C.L. UNION, *supra* note 223; Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, S. 2151, 112th Cong., § 102(a)(3) (2012) (original) and S. 3342, 112th Cong. §102(a)(3) (2012) (revised). *See also* CONGRESSIONAL RESEARCH SERVICE *supra* note 227, at 9.
[235] *See* CONGRESSIONAL RESEARCH SERVICE *supra* note 227, at 15.
[236] S. 2151 § 102(a)(2); *see also* AM. C.L. UNION, *supra* note 223.
[237] *See id.*
[238] Greg Nojeim & Jon Miller, *SECURE IT: Building a Better Back-Door Wiretap*, CTR. FOR DEMOCRACY & TECH. (Jul. 30, 2012), https://cdt.org/insights/secure-it-building-a-better-back-door-wiretap [https://perma.cc/KQ4R-5GC4] (describing fears over SECURE-IT).

it permitted far too much information to flow to multiple channels of the government.[239]

Neither did the Cybersecurity Act of 2012 (CSA) escape public scrutiny. In line with the previous proposals, the CSA of 2012 delineated eight types of cyber data that may be "indicative of" a threat, and eliminated liability for private entities that monitor their own information systems for such cyber data and alert other private entities, Department of Homeland Security (DHS)-approved private exchanges, and government exchanges.[240] The original CSA allowed DHS to establish a mandatory baseline for performance requirements on cybersecurity measures in critical infrastructures, a shift to a regulatory or mandatory framework rather than the voluntary incentives-based model that was favored by experts.[241] After the 2012 bill failed, the 2013 amended version returned to a voluntary model for compliance with DHS-established standards.[242] It also altered the information-sharing provisions by proposing a new federal cybersecurity information exchange that would be led by a civilian agency, with substantial limits to how much private-sector information other federal agencies could access.[243] Critics objected to CSA less on grounds of civil liberties atrocities and more on grounds of its being either bad policy, in its 2012 incarnation, or unhelpfully codifying a status quo, in its 2013 iteration.[244] Though the Cybersecurity Act of 2012 was debated in the Senate, it failed two cloture votes.[245]

In desperation to pass a cybersecurity information-sharing bill, congressmembers and the president began pursuing novel tactics. Senator Rockefeller sent personal letters to the CEO of each Fortune 500 company asking about the companies' cybersecurity practices and their willingness to comply with a voluntary program comparable to the Cybersecurity Act of 2012.[246] Rockefeller also

---

[239] *See id.*

[240] *See* AM. C.L. UNION, *supra* note 223; *see also* Cybersecurity Act of 2012, S. 2105, 112th Cong., §§ 708(6)(A), 706(a) (2012).

[241] *See* Cybersecurity Act of 2012, S. 3414, 112th Cong., §§ 103(g)(1) (2012).

[242] *See* § 704(g)(2).

[243] *See id.*

[244] *See* Teplinsky, *supra* note 6, at 289, 292.

[245] *See* CONGRESSIONAL RESEARCH SERVICE, *supra* note 227, at 2.

[246] *See* Teplinsky, *supra* note 6, at 294. The questions were:

> 1. Has your company adopted a set of best practices to address its cybersecurity needs?
> 2. If so, how were these cybersecurity practices developed?
> 3. Were they developed by the company solely, or were they developed outside the company? If developed outside the

urged President Obama to issue an executive order to fill the gap, which he finally did in February of 2013.[247]

In terms of information-sharing, however, EO 13,636 did not provide the framework that congressmembers were seeking to establish. First, the EO confirmed the importance of cybersecurity information sharing, particularly with the private sector, to US policy.[248] Second, the EO rearticulated the need to expand communication within cyberinfrastructure and directed DHS and the Department of Defense (DOD) to expand their existing information-sharing procedures.[249] It adopted some pilot programs toward this goal.[250] Third, the EO called for government and

---

> company, please list the institution, association, or entity that developed them.
> 4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?
> 5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?
> 6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?
> 7. What are your concerns, if any, with the federal government conducting risk assessments, in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?
> 8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

[247] *See id.* at 295 ("Senator Rockefeller and others urged President Obama to address cybersecurity through an Executive Order . . . "); *see generally* Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,737, 11,739 (Feb. 19, 2013) .

[248] *See id.* at §§ 1, 4(a) ("We can achieve [cybersecurity] goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.").

[249] *See id.* at § 4.

[250] *See id.* at §§ 4, 7-9. *See also* Comments of Donna Dodson, Chief Cybersecurity Advisor, National Institute of Standards and Technology, to United States Senate Committee on Homeland Security and Governmental Affairs (Mar. 26, 2014), https://www.nist.gov/speech-testimony/strengthening-public-private-partnerships-reduce-cyber-risks-our-nations-critical [https://perma.cc/7SQF-YTLA] (remarking on NIST's role in EO 13,636's pilot programs and standards development efforts and emphasizing the role of voluntary participation).

industry to collaborate in setting appropriate industry standards to be voluntarily adopted within a year, returning to a theme of incentive-based voluntary policy.[251] It also included language encouraging private companies to come forward with cybersecurity information, but provided no clear inducements towards this end.[252]

Owing in part to the fact that it largely highlighted the importance of sharing information rather than overhauling policy, Obama's cybersecurity EO did not quench the desire for a major law. Commentators repeated the call to reverse ambiguity before it resulted in cyber disaster.[253] A few months later, the Senate again considered CISPA, but privacy advocates struck it down.[254] Similarly, the SECURE-IT Act was reconsidered in April of 2013, but it, too, failed.[255]

At long last, in 2015, the Cybersecurity Information Sharing Act (CISA) passed.[256] CISA's framework was voluntary, encouraging companies to monitor cyber threats on their own IT systems and in collaboration with other companies, and to share certain kinds of de-identified information with government agencies.[257] It mandated that agencies report threats to promote internal defense mechanisms, required government studies on certain kinds of device security, and made it easier for the government to apprehend cyber criminals even if they lacked assets within United States jurisdiction.[258] Finally, it exempted companies

---

[251] *See id.* at §8 ("The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities.").

[252] *See* Teplinsky, *supra* note 6, at 299 ("private sector companies may remain reluctant to share information with the government due to the EO"s lack of liability protections. The White House did not have the authority to provide liability protections through an executive order; an act of Congress is required.").

[253] *See* Kathleen B. Rice, Mary Bono and Robert J. Ehrich, *Congress Must Pass Cyber Legislation Before Next Attack*, LAW360 (Oct. 31, 2014), https://www.law360.com/articles/590230/congress-must-pass-cyber-legislation-before-next-attack [https://perma.cc/GC6G-J67K].

[254] *See* Gerry Smith, *Senate Won't Vote On CISPA, Deals Blow To Controversial Cyber Bill*, HUFFINGTON POST (Apr. 25, 2013), https://www.huffpost.com/entry/cispa-cyber-bill_n_3158221 [https://perma.cc/NS4J-8MD8].

[255] *See* H.R. 1468 (113th); SECURE IT (2013) GovTrack.us (relating the bill's history).

[256] *See* CISA, 6 U.S.C. §§ 1501-1510; *see also* Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 578-79 (2016) (describing the law's provisions).

[257] *See* Johnson, *supra* note 256, at 578 (describing CISA's design as voluntary); CISA, *supra* note 256, at 580 (describing the process for de-identifying information).

[258] *See* Johnson, *supra* note 256, at 578-80 (describing CISA's provisions at length).

from antitrust suits and other causes of action for participating in the voluntary information exchange, so long as they acted in accordance with the rules of the exchange.[259] This included a specific exemption for antitrust, providing that "it shall not be considered a violation of any…antitrust laws for 2 or more private entities to exchange or provide [cybersecurity information] for cybersecurity purposes under this title."[260]

XI. REFLECTIONS: ANTITRUST SOFT LAW AS A VEHICLE FOR CYBERSECURITY POLICY

A. Predictions for the Future of Soft Law

As one pair of legal commentators observed, reflecting contemporaneously on the 2014 DOJ-FTC Joint Policy Statement's release, "[I]t does not appear likely that cybersecurity legislation will become law any time soon."[261] Thus, although the statement's content "[wa]s not new,"[262] the Policy Statement was still "significant…[for] clearly establishing that properly designed and executed cyberthreat information-sharing does not raise antitrust concerns."[263] Indeed, clarity, and hence market certainty, has been touted as one of the main benefits that soft law can provide.[264] Soft law also promotes legitimacy, flexibility, and transparency.[265] All of these virtues emanate from the examples of soft law discussed throughout this paper, especially the 2000 and 2014 Joint Policy Statements, as well as from the collaborations between the government and groups like H-ISAC and IGSC.[266]

---

[259] *See* CISA, *supra* note 249, at § 1505(a) ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 1503(a) of this title that is conducted in accordance with this subchapter.").
[260] CISA, *supra* note 256, at § 1503(e)(1).
[261] Padua Ferris & Tiao, *supra* note 216, at 2.
[262] *Id.* at 2.
[263] *Id.*
[264] *See* Hagemann et al., *supra* note 29, at 106 (discussing clarity and market certainty as benefits of soft law).
[265] *See id.* at 107 (discussing transparency), 111 (discussing legitimacy), 103 (discussing flexibility).
[266] *See id.* at 43-45 ("Some soft law actions such as standards or guidelines come from the private sector"); *see also* Kenneth W. Abbott, *Introduction: The Challenges of Oversight for Emerging Technologies*, in INNOVATIVE GOVERNANCE MODELS FOR EMERGING TECHNOLOGIES 1, 7 (Gary E. Marchant et al. eds., 2013) (noting that such soft governance approaches "rely on decentralizing regulatory authority among public, private and public-private actors and institutions," and that the advantage of such arrangements is that they "can be adopted and revised more rapidly than formal regulations").

What other benefits does soft law provide, and where can we expect to see it used? First, we should expect to see government agencies gap-filling via soft law wherever a deeply felt need exists for some sort of policy that is struggling to achieve the status of law. Adaptable, incentive-driven soft law can solve problems where the brute force of "hard law" cannot. The use of soft law will likely coexist with traditional "hard law," taking such forms as enforcement actions and both formal and informal agency rulemaking. This is because agencies fulfill their mandates to pave the way for policies that cannot otherwise get past congressional gridlock using every tool they have, both soft law and more traditional legal actions.

Sure enough, during the same time period when the FTC was issuing soft law policy statements, it also, for the first time, brought suit under the FTCA §45(a) against prominent companies in federal court for not securing customer information. In these suits, the FTC claimed that the failures to secure customer information were unfair trade practices that substantially injured consumers and that the companies' privacy policies were misrepresenting their practices.[267] The FTC continued bringing these cases even after CISA passed in 2015.[268] This is to be expected; the FTC was fighting for cybersecurity policy on all fronts, not just with soft law as chronicled here, but also with innovative legal theories in traditional modes of agency action.

Innovative industries will likely continue to resist easy regulation by conventional means. Thus, we can expect to continue to see soft law in innovation markets. As discussed above, the 2000 Joint Guidelines described innovation markets as "consist[ing] of the research and development directed to particular new or improved goods or processes and the close substitutes for that research and development."[269] These sectors are characterized by rapid-fire change, relative portability into different jurisdictions, and a tendency to straddle surprising areas of law. Soft law is much more apt to keep up with innovation markets than the comparatively plodding hard law mechanisms. Moreover, where the government is

[267] *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (2014), *supra* note 49.
[268] *See In re* LabMD Inc., 2015 FTC LEXIS 272 (2016), *supra* note 49.
[269] 2000 Joint Guidelines, *supra* note 106, at 17.

widely perceived as incompetent,[270] such as in cybersecurity,[271] it is to the government's benefit to recruit industry actors to behave based on their own incentives, just as the government pivoted to public-private partnerships from the beginning of its cybersecurity discussions.

Moreover, we will likely continue to see soft law at work where regulation slows down owing to a contentious topic, such as that of cybersecurity and privacy.[272] This may particularly be the case for soft law interventions by antitrust agencies, as antitrust has the wonkish veneer of economics grounding and a public reputation for preventing companies from abuses of power. Perhaps because of this, antitrust regulations may slip through unnoticed by civil liberties activists concerned about the rights of the less powerful. Moreover, soft law-style interventions by antitrust agencies, by motivating private technology companies to alter their behavior rather than imposing poorly designed policies, might achieve more favorable outcomes.

Nevertheless, one must not hasten to draw inferences from a narrative so full of redundancy and coincidence. The 2014 FTC-DOJ Joint Policy Statement reiterated previous laws and guidelines and seemed to intervene when Congress could not pass a law, but it evidently did not negate (at least the Congressional) demand for CISA, passed a year after the Joint Policy Statement. Was CISA meant to be expressive as much as effective? Was the 2014 Joint Policy Statement meant to be permanent or a stop along the way to a legislative overhaul? Is this another example of Congressional glut and removal from other aspects of governance?

B. Need for Further Academic Attention: Cybersecurity Governance

Because cybersecurity is woefully undertheorized as a field,[273] it comes as no surprise that its regulation also requires scholarly attention. For instance, in cybersecurity governance, as in

---

[270] *See, e.g.,* Sen. Tom Coburn, *A Review of the Department of Homeland Security's Missions and Performance,* SENATE HGSAC 12 (2015) ("The Department of Homeland Security is struggling to execute its responsibilities for cybersecurity, and its strategy and programs are unlikely to protect us from the adversaries that pose the greatest cybersecurity threat.").

[271] *See id.; see also supra* Sections IV and V (describing industry's outsize role in cybersecurity compared to government).

[272] *See supra* Section XI(i) (describing legislative and regulatory context of soft law chronicled in this paper).

[273] *See* Johnson, *supra* note 256, at 547 ("Indisputably, cyber threats are simply under-theorized.").

emerging soft law discourse, the importance of voluntary, industry-driven standards is accepted as a given. Section I chronicled how, from its very nascence, officials touted the idea of cybersecurity governance as voluntary, not mandated.[274] This may well be a good idea, but it is an idea laden with political baggage, including the undying big-government-versus-invisible-hand debates.[275] As discussed above, this zeal for collaboration seems to be driven by a near-universal sentiment that industry experts are more competent than the government. Still, more scholarship should investigate whether a voluntary structure is preferable and why it is so universally accepted, at least in the area of technology governance.[276]

C. Antitrust in Search of Itself: Mergers vs. Joint Ventures and the Per Se Rule vs. the Rule of Reason

This article's narrative dramatizes the impact of confusion in classifying an entity as a joint venture versus a merger and when to use the per se rule versus the rule of reason for joint ventures. The NCRA statutorily defines joint ventures and specifies when each rule should be used, and the 2000 and 2014 Joint Policy Statements distinguish between joint ventures and mergers. Nevertheless, one aspect of the Policy Statements' definition clashes with the joint ventures we have seen: the short and often self-limited duration of partnerships. Both H-ISAC and the IGSC seem to be collaborating for an indeterminate period of time with no plans of stopping, and the government does not seem interested in intervening.

Moreover, the Toyota/GM collaboration was found to be a joint venture although it lasted for twelve years, the same amount of time that the 2000 Policy Statement used in its hypothetical as being impermissibly long and requiring merger treatment.[277] To

---

[274] *See supra* Section I (describing how stakeholders agreed that cybersecurity government should be voluntary).

[275] *See generally* Kelly, *supra* note 35, at 1671 ("[E]lements of each [cybersecurity bill from each party] represent (popularly believed, but perhaps cliched) normative tendencies of the two parties: Democratic-favored direct regulation versus Republican-favored market incentives. Therefore, due to the proposals' links to incentivized party leaders, the final version of cybersecurity reform will likely embody major elements from one of these two proposals.").

[276] *Compare id.* At 1681-1695 (chronicling differences in proposals put forth by the Democrats and the Republicans) with Teplinsky, *supra* note 6, at 281 ("Despite differences between the Administration's legislative proposal and the task force recommendations, in December 2011, Senate Majority Leader Harry Reid (D-NV) described the House Republican cybersecurity task force recommendations as 'fully consistent with our efforts.'").

[277] *See 2000 Joint Guidelines*, *supra* note 110, at 28 (finding that twelve years was too long to be considered a joint venture).

contemporary antitrust commentators, indeed, twelve years may seem unacceptably long. It will be interesting to see whether a collaboration's duration will ever run afoul of the government's interests enough to be challenged and clarified, or if the duration requirement given in the definitions will be quietly dropped.

Finally, narratives about the development of the per se rule and rule of reason are the genesis stories of antitrust, revealing the field's self-conception and motivations. Early Supreme Court cases seemed firmly to distinguish between the two, using them to articulate American antitrust principles.[278] Later decisions gave rise to a third test, the "quick look," which lower courts and commentators quickly hailed as another monolithic test, although the Court seemed reluctant to fully credit it as a test unto itself.[279] In subsequent cases, however, the Court seemed to endorse the view that all of the antitrust tests could be conceived of as lying along a continuum, differing in degree rather than in kind.[280] Scholars have noted that a sliding scale approach is the natural way to conceive of "what courts have always done"[281] in the face of weaker or stronger cases, even if it can create confusion in terms of how to apply the rules.[282]

If antitrust tests are best conceptualized as existing along a continuum, the policy interventions discussed in this paper—both legislation and soft law—betray this schema by their depictions of the two main analyses. In different ways, they minimize the per se rule and present it as an entirely different category than the rule of reason. The 2000 guidelines spare only a few sentences for the per se rule, presenting it as used in only a vanishing subset of cases, while devoting pages to the rule of reason.[283] The 2014 statement

[278] *See* United States v. Trenton Potteries Co., 273 U.S. 392, 397–98 (1927); Board of Trade of City of Chicago v. United States, 246 U.S. 231 (1918); *see also* Hovenkamp, *supra* note 151, at 122 (describing our evolving understanding of the antitrust tests).

[279] *See* Hovenkamp, *supra* note 151, at 122-23 ("Lower courts, the FTC, and commentators have often suggested that antitrust analysis in fact occupies three silos: the rule of reason, per se illegality, and an intermediate 'quick look,' which has been described in different ways by different courts . . . . The Supreme Court has never embraced a three-silo quick look. While the Court has not rejected the idea categorically, its various statements have been quite critical. Only three Supreme Court decisions have explicitly acknowledged the quick look, and then only to reject it under the circumstances.").

[280] *See id.* at 123 (presenting evidence for how the Court seems to have "embraced" this view).

[281] *Id.* at 125.

[282] *See id.* at 125-28.

[283] *See 2000 Joint Guidelines*, *supra* note 110, at 3.

does not acknowledge the per se rule at all.[284] The guidelines certainly do not mention a sliding scale or quick look, even if their examples may implicitly invoke some of the tests' logic.

Changemakers in fast-moving sectors like science and technology lack scholarly patience; they need to know the consequences of their actions. Soft law methods of governance can provide the rough and ready reassurance they need. In so doing, though, they can undersell nuances in how courts and scholars are thinking about live issues and force developments in practice on a shorter timeline, or perhaps even a different direction, than traditional governance might have. For better or worse, soft law has made itself indispensable as a gap-filling tool in ever-changing and highly-politicized innovation sectors. In an environment where not just technology, but also judiciary-agency relationships, are in flux, soft law will surely continue to cushion the transfer of long-standing antitrust theories into the contemporary economy.

[284] *See generally* 2014 Joint Policy Statement, *supra* note 208.