The Redesign of the U.S. Privacy Policy Institutional Framework

William E. Kovacic[1]

September 23, 2020

Testimony Before the U.S. Senate Committee on Commerce, Science, and Transportation, Hearing on "Revisiting the Need for Federal Data Privacy Legislation"

Introduction

I thank the Senate Commerce Committee for the opportunity to discuss the future of privacy regulation in the United States. Data about consumer behavior is an increasingly valuable resource,[2] and privacy agencies are its most important regulators. Other policy domains – such as antitrust and consumer protection law – affect how commercial and non-commercial organizations gather and use data,[3] but privacy regulation today is paramount.

The ascent of privacy as focus for public policy in the United States since the early 1970s has inspired debate on two basic issues.[4] The first involves the substantive rules that dictate how private and public institutions can collect and use information about individuals.[5] Many commentators have offered approaches for developing optimal privacy rules,[6] including proposals is to codify and extend existing substantive law by adopting an omnibus federal privacy statute.[7]

The second focus of attention is policy implementation. The United States develops and applies

---

[1] Global Competition Professor of Law and Policy, George Washington University Law School; Visiting Professor, Dickson Poon School of Law, King's College London; Non-Executive Director, United Kingdom Competition and Markets Authority. The author served as General Counsel of the US Federal Trade Commission from 2001-2004 and was a member of the agency from 2006 to 2011. He chaired the agency from March 2008 to March 2009. This testimony is adapted in part from David A. Hyman & William E. Kovacic, *Implementing Privacy Policy: who Should Do What?*, 29 FORDHAM INTELLECTUAL PROPERTY, MEDIA & ENTERTAINMENT LAW JOURNAL 1117 (2019). I owe a great intellectual debt to Professor Hyman, who has taught me so much about the links between institutional design and the substantive outcomes achieved by public agencies. The views expressed here are the author's alone.

[2] *The world's most valuable resource is no longer oil, but data*, ECONOMIST (May 6, 2017), available at http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.

[3] *Digital Privacy Is Making Antitrust Exciting Again*, WIRED (June 4, 2017), available at http://www.wired.com/2017/06/ntitrust-watchdogs-eye-big-techs-monopoly-data/.

[4] The emergence of privacy as a central element of regulatory policy is traced in Peter P. Swire, The Administration Response to the Challenges of Protecting Privacy (Jan. 8, 2000) (mimeo).

[5] The legal systems that control the collection and use of information about individuals are sometimes called privacy law and sometimes called data protection. In this testimony, the term privacy encompasses both. See Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235 (2015) (hereinafter *FTC Data Protection*).

[6] A notable formative contribution along these lines is Dan Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 352.

[7] See, e.g., White House, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.*

privacy policy through a bewildering assortment of federal, state, and local governmental entities. The constellation of responsible public institutions deserves close attention, for the quality of substantive privacy policy depends greatly on which agency (or agencies) run the show.

In privacy and other areas of public administration, debates over the substance of policy tend to overshadow implementation.[8] In recent decades, academics, government officials, and practitioners have rebalanced the discussion by devoting greater attention to implementation issues.[9] Some scholars have examined how the Federal Trade Commission ("FTC") has become the closest US equivalent to a national privacy authority – a status owing to historical accident and the FTC's conscious efforts to occupy a significant unoccupied policy space.[10] Others have considered how the United States should allocate policy development and law enforcement among federal and state agencies.[11] Another line of commentary has used experience from foreign jurisdictions to suggest adjustments to the US privacy regime.[12]

My testimony builds upon these contributions and discusses institutional mechanisms the United States might use to design and implement privacy policy. Despite important achievements, the existing configuration of the US implementing institutions leaves a lot to be desired. Notably, authority over privacy is simultaneously murky and subdivided among multiple entities at the federal level (i.e., the FTC and sector-specific regulators), plus state and local governmental entities. The resulting horizontal and vertical dynamics create considerable inter-agency tension and prevent the US system, as a whole, from attaining desirable levels of coordination and shared learning.

The institutional deficiencies have at least two adverse consequences. First, the institutional status quo undermines the ability of the United States to develop coherent, effective substantive

---

[8] On the gap between the adoption of policy reforms and their successful sustained implementation, *see* Eric M. Patashnik, REFORMS AT RISK: WHAT HAPPENS AFTER MAJOR POLICY CHANGES ARE ENACTED 155 (2008) ("[W]hat is required to *initiate* policy reform should not be confused with what is required to *sustain* it.") (emphasis in original); Graham T. Allison, ESSENCE OF DECISION: EXPLAINING THE CUBAN MISSILE CRISIS 267-68 (1971) ("If analysts and operators are to increase their ability to achieve desired policy outcomes, . . . we shall have to find ways of thinking harder about the problem of 'implementation,' that is, the path between the preferred solution and actual performance of the government.").

[9] *See, e.g.*, Symposium, *Enforcing Privacy Rights*, 54 HASTINGS L.J. 877 (2003) (collecting various papers on privacy policy implementation).

[10] *See, e.g.*, CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016); Hartzog & Solove, *FTC Data Protection*, *supra*; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014). *See also* Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy* 21 (Washington University of St. Louis School of Law 2014) (noting the FTC's "entrepreneurial expansion of its jurisdiction" regarding privacy).

[11] *See, e.g.*, Danielle Keats Citron, *The Privacy Policymaking of States Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) (hereinafter *State Attorneys General*); Peter Swire, *Why the Federal Government Should Have a Privacy Policy Office*, 10 J. ON TELECOM. & HIGH TECH. L. 41 (2012); Peter Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime*, 7 J. ON TELECOM. & HIGH TECH. L. 107 (2009); Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183 (2003) (hereinafter *Privacy Protection Board*).

[12] *See, e.g.*, William McGeveran, *Friending the Privacy Regulators*, 58 ARIZONA L. REV. 959 (2016) (hereinafter *Friending*); Paul M. Schwarz, *The E.U.-U.S. Privacy Collision: A Turn to institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

privacy policies. Outwardly, the many public agencies with privacy duties at the national and state levels profess a common commitment to work collegially toward the development of a sound US privacy regime. To some degree, the expressed spirit of common cause is genuine, and it routinely manifests itself in helpful forms of policy coordination and enforcement cooperation. Nonetheless, in my capacities as a government official and as an academic, I have observed how parochialism and mistrust impede the development of a regime that exploits the full benefits of institutional diversity and experimentation while achieving needed levels of coherence.

The second adverse consequence involves the capacity of the United States to participate effectively in the development of global privacy standards. Our domestic institutional weaknesses hinder US efforts to encourage the development of superior international privacy standards and to achieve needed levels of cross-border cooperation in law enforcement.[13] The General Data Protection Regulation (GDPR),[14] which took effect in 2018, is the latest manifestation of the EU's preeminent role in setting what, in effect, are broadly applicable international privacy standards. In pressing ahead with their own reforms, data protection officials within the European Commission and the European Union's Member States often take a dismissive view of the US privacy regime and discount US preferences regarding the optimal design of privacy rules.[15] This dismissive perspective ignores valuable, effective aspects of the US regime (especially its enforcement mechanism), but it also reflects an understandable exasperation that comes from sometimes unavailing efforts to gain clarity with respect to the content of "US policy" and who is in charge of formulating it.

Basic reforms in the existing institutional arrangements are a necessary component of any improvement in substantive privacy policy. In previous work with Professor David Hyman, I have addressed the question of how to design regulatory mechanisms.[16] In this testimony, I draw upon that work to consider the future of privacy policy implementation in the United States My testimony assumes that the United States will enact a comprehensive national privacy law that consolidates, restates, and extends existing federal privacy commands. In this statement, I do not examine in depth what I believe to be the appropriate content of such an omnibus measure. As Congress defines the substantive commands of a new omnibus law, I suggest a close review of

[13] Professors Hartzog and Solove observe that "[a] more centralized and comprehensive approach to data protection is sorely needed in the United States, which is increasingly at odds with most other countries in the world with its more fragmented sectoral approach to data protection." Hartzog & Solove, *FTC Data Protection*, *supra* at 2271. They describe U.S. privacy law as "a fragmented mess of overlapping and inconsistent laws that make it nearly impossible for consumers to figure out how their privacy is protected." *Id*. at 2273. This position weakens the "soft power" that the US government otherwise would exercise in this policy domain. *Id*.

[14] Regulation 2016-678 of the European Parliament and of the Council of 27 April 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2018 O.J. (L. 119) 66.

[15] I base this observation on my experience at the FTC as General Counsel from 2001-2004, as an FTC member from 2006-2011, and as a Non-Executive Director of the United Kingdom's Competition and Markets Authority from 2013 to the present.

[16] See, e.g., David A. Hyman & William E. Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 GEO. WASH. L. REV. 1446 (2014) (hereinafter *Why Who Does What Matters*).

the FTC's experience in implementing the Telemarketing Sales Rule.[17] To my mind, this experience offers several insights into the design of privacy protections:

- In addition to unfair or deceptive acts and practices, the definition of forbidden behavior should encompass abusive conduct, as the FTC has developed that concept in the elaboration of the Telemarketing Sales Rule (TSR). I single out 2003 TSR amendments, which established the National Do Not Call Registry, popularly known as the Do Not Call Rule (DNC Rule). In applying the concept of abusive conduct, the DNC Rule used a definition of harm that reached beyond quantifiable economic costs of the challenged practice (i.e., the time lost and inconvenience associated with responding to unwanted telephone calls to the home). The DNC Rule's theory of harm focused on the fact that, to many citizens, telemarketing calls were annoying, irritating intrusions into the privacy of the home.[18] A new privacy regime could build on this experience and allow privacy regulators, by rulemaking and by law enforcement, to address comparable harms and to create standards that map onto common expectations for data protection and security.

- The coverage of the omnibus statute should be comprehensive. Privacy authorities should have power to apply the law to all commercial actors (i.e., with no exclusions for specific economic sectors) and to not-for-profit institutions such as charitable bodies and universities.

- The omnibus law should clarify that its restrictions on the accumulation and use of date about individuals apply to their status as consumers and employees. Since the late 1990s, the FTC at times has engaged in debatable interpretations of its authority under Section 5 of the Federal Trade Commission Act to assure foreign jurisdictions that it has authority to enforce promises regarding the collection and transfer by firms of information about their employees.[19]

With this general framework in mind, my testimony proposes that an omnibus privacy law should enhance the institutional arrangements for administering a new substantive privacy framework.[20] This statement:

---

[17] The FTC first promulgated the Telemarketing Sales Rule in 1995 pursuant to the Telemarketing and Consumer Fraud Abuse Prevention Act, which Congress enacted in 1994 and is codified at 15 U.S.C. §§ 6101-6108. The Telemarketing Sales Rule, as amended in 2003, 2008, and 2016, appears at 16 C.F.R. 310.

[18] The DNC Rule withstood formidable legal challenges by affected telemarketing companies. Mainstream Marketing Services, Inc. v. FTC, 358 F.3d 1228 (10th Cir. 2004).

[19] In discussions in the late 1990s and in the 2000s with foreign governments about the Safe Harbor mechanism, the FTC asserted that Section 5 of the FTC act permitted the agency to control transfers of data involving employees – a position not easily reconciled with traditional interpretations that view the law as protecting the interests of individuals as consumers. In my time as FTC general counsel from 2001 to 2004, I signed one letter assuring a foreign jurisdiction that, for the purpose of the Safe Harbor agreement, the Commission viewed its mandate as including the enforcement of promises that employers made about the collection and use of data about their employees.

[20] A number of observers had expressed doubts that the United States will adopt a comprehensive privacy bill in the foreseeable future. Professors Hartzog & Solove observe: "The chances of Congress passing a comprehensive federal data protection law are remote. The most practical way that the U.S. data protection regime will evolve into something more coherent and comprehensive is through FTC enforcement." Hartzog & Solove, *FTC Data*

- Sets out criteria to assess the performance of the entities implementing U.S. privacy policy, and to determine how to allocate tasks to institutions responsible for policy development and law enforcement.

- Suggests approaches to increase the coherence and effectiveness of the US privacy system and to make the United States a more effective participant in the development of international privacy policy.

- Considers whether the FTC, with an enhanced mandate, should serve as the national privacy regulator, or whether the FTC's privacy operations should be spun off to provide the core of a new privacy institution.

This statement concludes that the best solution is to take steps that would enhance the FTC's role by (a) eliminating gaps in its jurisdiction, (b) expanding its capacity to promote cooperation among agencies with privacy portfolios and to encourage convergence upon superior policy norms, and (c) providing resources necessary to fulfill these duties. The proposal for an enlarged FTC role considers two dimensions of privacy regulation. The first is what might be called the "consumer-facing" elements of a privacy. My testimony deals mainly with the relationship between consumers and enterprises (for-profit firms and not-for-profit institutions, such as universities) that provide them with goods and services.

My testimony does not address the legal mechanisms that protect privacy where the actors are government institutions. Thus, I do not examine the appropriate framework for devising and implementing policies that govern data collection and record-keeping responsibilities of federal agencies,[21] such as bodies that conduct surveillance for national security purposes. In light of the continued, significant role for privacy policy with respect to other government bodies; the proposals offered here for privacy reform therefore do not seek establish a single privacy policy maker and law enforcement body that would address all privacy questions involving behavior by private and public bodies. Giving the FTC an expanded role in consumer-facing privacy matters would leave in place the framework of controls that address other privacy concerns. At the same time, the proposals offered here do contemplate stronger mechanisms to ensure policy consultation and coordination among bodies with consumer-facing responsibilities and those with other privacy mandates.

The benefits of adopting implementation reforms – notably, greater system-wide coherence and effectiveness – are likely to come about without regard to the substantive privacy commands that our nation adopts. Implementation-related reforms are desirable whether the conceptual basis for privacy protection is fair information practice principles (FIPPS),[22] a consequences-based theory

---

Protection, *supra* at 2271. Even if an omnibus statute is not adopted, there is considerable value in upgrading the mechanism for implementing, and extending, existing mandate

[21] At the federal level, the modern statutory foundation for privacy requirements that govern federal agencies is the Privacy Act of 1974, 5 U.S.C. §552a.

[22] *See* Department of Commerce Internet Policy Task Force, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 3-5, 23-30 (Dec. 2010) (hereinafter *Commercial Data*

of liability,[23] or some amalgam or these or other approaches.

II. U.S. Privacy Policy Development and Implementation

Privacy law in the United States is a stark example of a "regulatory thicket."[24] The discussion below highlights two aspects of the regulatory thicket: the collection of substantive commands that fall within the ambit of privacy regulation, and the myriad public institutions responsible for formulating or implementing privacy policy.

A. Privacy Law Commands: Functions and Forms

Privacy laws in the United States perform two basic functions. One set of controls seeks to restrict the *collection and use* of information about individuals. For commercial transactions, these controls define the circumstances under which service providers can (a) collect information about their customers; (b) retain and use such information; and (c) transfer customer information to third parties. Another set of controls establishes the conditions under which bodies such as credit rating services can assemble and use data on consumers.

A second core function is to ensure that information about consumers is *adequately protected* from unauthorized use. Some privacy policies require commercial bodies to establish safeguards against inadvertent disclosure of consumer information. Others punish those who misappropriate consumer information to steal an individual's identify or property, or damage an individual's reputation. A further category of controls prohibits unauthorized access to data systems for the purpose of stealing sensitive data or disabling a data network.

A complex, bewildering "jumble" of federal and state statutes seeks to perform these functions.[25] Unlike a number of other countries, the United States has no omnibus federal privacy law. Federal privacy law is a mosaic of controls that apply to specific categories of activity; to specific sectors; and to specific classes of individuals. The most scalable element of the federal privacy regime – the prohibition in the Federal Trade Commission Act against "unfair or deceptive acts and practices" (UDAP)[26] – is circumscribed by jurisdictional exclusions involving banks, common carriers, and not-for-profit institutions.[27] Nor does the FTC have responsibility to oversee data collection and protection by public institutions; a separate body of laws governs

---

Privacy) (describing FIPPs); *see also* Colin J. Bennett, REGULATING PRIVACY 101-11 (1992) (describing "core fair information principles").

[23] *See* J.. Howard Beales III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information 11-13 (June 15, 2007) (University of Chicago School of Law Conference on Privacy and Security) (presenting privacy policy approach based on proof of adverse consequences to consumers).

[24] Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1674, 1696-97 (2016) (using the concept of "regulatory thicket" to describe public regulation of software).

[25] Hartzog & Solove, *FTC Data Protection*, supra at 2267.

[26] 15 U.S.C. §45(a) (1).

[27] The scope of these exemptions is a regularly litigated matter. *See e.g.*, FTC v. AT&T Mobility LLC, 835 F.3d 993 (9th Cir. 2016) (interpreting scope of common carrier exemption). There are also frequently-expressed concerns about the FTC's authority to act to protect the interests of foreign citizens and thus to provide assurance to other jurisdictions (notably, the European Union) that their citizens are adequately protected when data about then is transferred to the United States. *See* Gellman, *Privacy Protection Board*, *supra* at 1213-14.

the duties of public agencies.[28] Finally, many elements of federal privacy law are enforceable with civil remedies only; other laws involving practices such as identity theft and hacking of computer systems are punishable as criminal offenses.

State law and policy provide a major second dimension in US privacy law.[29] The contributions of states, in many respects, equal or surpass the work of federal institutions in determining the privacy obligations of commercial actors. It is not a stretch to say that the California Consumer Privacy Act of 2018 (CCPA) is the most important piece of consumer-facing privacy legislation enacted in the United States in this century. The State of California has been especially influential in defining the privacy obligations of firms in the United States, but it is not alone among the states in playing an important policy making role. For example, at least 45 states have enacted laws that require firms to notify individuals when an unauthorized disclosure of consumer information has taken place.[30]

In this and other areas of privacy policy, state governments have spearheaded important experiments with different forms of privacy controls. As noted above, any listing of the most important sources of privacy law in the United States must include the State of California alongside the most significant of the federal institutions entrusted with privacy duties. One might argue that, measured by its power to shape national privacy norms, California deserves a place in any discussion about the institutions whose decisions determine privacy policy in the United States. If policymaking significance were the only criterion for selection (putting aside matters of protocols governing international relations), California might well be included (along with the FTC or other federal bodies) in delegations that represent the United States in international gatherings of privacy officials.

B. The Ecology of U.S. Privacy Institutions

An elaborate array of public bodies is responsible for formulating and implementing privacy policy. Institutional multiplicity, with concurrent or overlapping grants of authority, is hardly unusual in the U.S. legal system. Privacy law is an especially interesting case, due to the exceptional variety of public institutions that occupy some part of the policymaking and law enforcement space. Privacy stands out for study not just because of the complexity of the U.S. system considered in isolation, but also by comparison to many foreign privacy regimes, which use far fewer institutions to implement substantive privacy law.

The discussion below sketches out the regulatory ecosystem for the implementation of privacy policy. The term "ecosystem" captures several features of the US regime.[31] One element is the extraordinary diversity of institutional species/entities. Many public entities have developed

---

[28] *See* Alan Charles Raul, PRIVACY AND THE DIGITAL STATE: BALANCING PUBLIC INFORMATION AND PERSONAL PRIVACY 23-31 (2002) (describing the Privacy Act and other controls on the collection and use of information by public bodies).

[29] Professor Citron has written the preeminent account of the role of state law and policy in privacy. Citron, *State Attorneys General*, *supra*.

[30] Gregory James Evans, *Comment, Regulating Data Practices: How State Laws Can Shore UP the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187. 203 & n. 93 (2015).

[31] *See* Hyman & Kovacic, *Who Does What*, *supra* (describing the "regulatory ecosystem" of the federal government writ large).

programs and processes for devising privacy policy and enforcing privacy legal commands. A careful understanding of what each institution does, and knowledge of how it evolved, should precede decisions to uproot individual species or to plant new species within the ecology.

A second element of the privacy ecology is a relatively rapid adaptability that flourishes through decentralized decision making that does not depend on central direction as a predicate for policy development. Despite the lack of an omnibus US privacy law, institutions at the national and state levels have adjusted over time to the emergence of new commercial phenomena, many of which result from rapid technological change.

The ecosystem metaphor can be misleading to the extent that it overlooks elements of intelligent design. The myriad of privacy institutions are, in key respects, interdependent. The effectiveness of the entire system of privacy controls depends on how well each institution accounts for these interdependencies. Through formal and informal means, the public agency participants in privacy regulation have formed mechanisms to coordinate their operations. Imperfect though it is, coordination has facilitated the development of common principles, and has reduced the smash-ups that one might expect from a multi-level regulatory regime with so many actors. Decisions about the redesign of institutions – such as by uprooting one regulator's duties and assigning them to another – should account for the operation and effectiveness of networks and policy synapses that may not be readily visible.

Federal agencies. The most important federal privacy institution is the FTC, which has become the leading US privacy body.[32] At present, the FTC is responsible for three distinct policy fields: competition, consumer protection, and privacy (which is situated within the agency's Bureau of Consumer Protection, but has acquired its own identity and prominence). The Commission's privacy work is grounded partly in statutes that, in whole or in part, are specifically designed as privacy measures. These include early measures, such as the Fair Credit Reporting Act ("FCRA"),[33] and more recent enactments such as the Gramm-Leach-Bliley Act[34] and the Children's Online Privacy Protection Act ("COPPA").[35] The FTC has built an extensive "common law" of privacy protection through settlements achieved in cases brought pursuant to its UDAP mandate.[36] A number of privacy scholars regard this process of common law elaboration as a useful instrument of policy making for privacy,[37] but this view is not universally accepted.[38] Some critics regard that FTC's privacy program not only to be inadequate, but also a

---

[32] Hoofnagle, FEDERAL TRADE COMMISSION PRIVACY, *supra* at 192 ("The Federal Trade Commission has emerged as the nation's top regulator of privacy."); Hartzog & Solove, FTC Data Protection, *supra* at 2267 ("In the current U.S. privacy regulatory system, the FTC has grown into the role of being the leading regulator of privacy . . . .").
[33] 15 U.S.C. §1681s (2000).
[34] 15 U.S.C. §§6804-05 (2000).
[35] 15 U.S.C. §6505 (2000).
[36] Solove & Hartzog, *Common Law*, *supra*. The FTC is not alone in using the administrative process to build legal norms. Gillian E. Metzger, *Embracing Administrative Common Law*, 80 GEO. WASH. L. REV. 1293 (2012).
[37] Positive assessments include Solove & Hartzog, *Common Law*, *supra* and Hoofnagle, FEDERAL TRADE COMMISSION PRIVACY, *supra*.
[38] For a negative assessment of the FTC's contributions to privacy policy, through law enforcement and other policy tools, see Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?* (Oct. 25, 2016) ("the FTC deserves low grades when it comes to protecting consumer privacy"), *available at* http://www.aclu.org/blog/free-future/can-consumers-trust-ftc-protect-their-privacy.

genuine barrier to the adopted of a much needed upgrade of the entire U.S. privacy regime.[39] The FTC has also used its rulemaking authority to build important elements of the national privacy architecture, including the DNC Rule.

The FTC also has important "soft power" tools with which to set privacy policy.[40] The FTC can examine industry trends by compelling companies to provide information. The FTC can also conduct studies, hold hearings, and prepare reports – a power it has used to examine privacy-related matters.[41] The FTC has also played a major role as a convenor of conferences, workshops, and seminars that have served to identify significant commercial trends and focus debate, among a range of interested groups, on key privacy issues.[42]

As noted above, the FTC's capacity to serve as the U.S. privacy regulator is hampered by several jurisdictional carve-outs. In 1914, Congress largely exempted banks, common carriers, and not-for-profit institutions from the Commission's oversight. Today thee exempted sectors assemble, use, and transmit massive amounts of data about individuals, yet they stand beyond the FTC's reach. Nor does the FTC have power to oversee the data collection practices of public institutions. It is difficult to envision the FTC serving as a truly effective national privacy regulator if these exemptions persist.

A variety of sectoral regulators occupy some of the policy terrain left open by the FTC's jurisdictional exclusions. A notable example is the Federal Communications Commission (FCC), which exercises privacy oversight for telecommunications providers. The boundary between what is and is not a telecommunications service has shifted over time, and has moved dramatically in recent years, in the face of technological change and court decisions that together have redefined the scope of the FCC's and FTC's authority.[43] As we are writing this piece, the FCC seems poised to revoke its recent net neutrality rule, which classified broadband as a telecommunications service. By bringing broadband within the ambit of the common carrier exemption, the FCC's rule would have ousted the FTC from privacy oversight in this technological space, while repudiation of the net neutrality rule would preserve the FTC's role.

Other federal agencies have responsibility for sector-specific privacy controls. For example, the

---

[39] At a privacy conference in the 2000s, while serving an FTC official, I was approached by a privacy advocate who scorned the FTC's role in the privacy field and berated its application of the agency's UDAP authority to address privacy issues. The advocate argued that the FTC's UDAP cases had created the illusion of effective law enforcement and had given the business community a useful argument to blunt demands for legislation that would upgrade the U.S. privacy framework dramatically. Only if the FTC stood down would the serious inadequacies of the status quo be revealed, and necessary support for reforms mobilized.

[40] *See* William E. Kovacic, *The Digital Broadband Migration and the Federal Trade Commission: Building the Competition and Consumer Protection Agency of the Future*, 8 J. TELECOMM. & HIGH TECH. L. 1 (2010).

[41] *See, e.g.*, FTC Privacy Report, at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report.; see also Remarks of FTC Chairwoman Edith Ramirez, *Protecting Privacy in the Era of Big Data*, International Conference on Big Data from a Privacy Perspective (Hong Kong, June 10, 2015).

[42] *See, e.g.*, FTC Announces Agenda for PrivacyCon, Dec. 29, 2015, at https://www.ftc.gov/news-events/press-releases/2015/12/ftc-announces-agenda-privacycon. On the FTC's role in convening events that provide fora for academics, advocacy groups, government officials, and practitioners to discuss privacy and other policy issues, see William E. Kovacic, *The FTC as Convenor: Developing Regulatory Policy Norms without Litigation or Rulemaking*, 13 COLO. TECH. L.J. 17 (2015).

[43] Ohm & Reid, *Regulating Software*, *supra* at 1674-75, 1697-98

Department of Education enforces the Family Educational Rights and Privacy Act (FERPA),[44] which imposes record-disclosure duties and limits on educational institutions and state educational bodies that receive federal funds. The Department of Health and Human Services (HHS) plays the lead role in enforcement of the Health Insurance Portability and Accountability Act (HIPAA),[45] which established data privacy obligations and security requirements to safeguard medical information.

Another notable participant in federal privacy policy implementation is the U.S. Department of Justice (DOJ). The Department is responsible for enforcing a collection of criminal statutes, such as the Computer Fraud and Abuse Act,[46] which fall within the general heading of cybersecurity.[47] DOJ also has the power to enforce general anti-fraud provisions (e.g., statutes involving mail fraud and wire fraud) that can be used to attack such cyber-crimes as hacking and identify theft.

Consistent with the regulatory ecosystem theme, there have been numerous efforts to coordinate the work of these entities, in order to develop national privacy policy objectives and work with foreign governments to establish international policy norms. The FTC, the Department of Commerce, and various ad hoc bodies established by the Office of the President have all contributed to this broader policy development and coordination process.

State and Local Governments. As mentioned above, state governments are also prominent sources of privacy law in the United States.[48] States typically enforce their own laws through privacy units contained within the office of the state attorney general. Some enforcement functions are performed at the municipal level. In many instances, local police departments are the focal point for reports about identity theft, although they usually lack the capacity to pursue the matter.

Non-Government Organizations. Non-government organizations (NGOs) also play an important role in the creation of norms and in policy coordination. Academic institutions and professional societies (such as the American Association of Privacy Professionals) provide networks in which the full spectrum of groups with an interest in privacy policy (e.g., academics, companies, consumer advocates, consultancies, government officials, legislators and their staff members, and practitioners) meet to discuss privacy policy issues.

Such meetings can help build consensus about the content and implementation of privacy policy. For this reason, NGOs are an important ingredient in the creation of privacy norms. These organizations also provide a forum in which policymakers can meet each other and discuss matters of common concern. These engagements supplement the more formal arrangements

---

[44] 20 U.S.C. §1232g (2000).
[45] 42 U.S.C. §1320d.
[46] Computer Fraud and Abuse Act of 1986, Pub. L. No. 98-474, §2, 100 Stat. 1213-16 (codified as amended at 18 U.S.C. §1030 (2012)).
[47] Patricia Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442 (2016); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statues*, 78 N.Y.U. L. Rev. 1596 (2003). The expanding significance of this area of enforcement is reported in *Why everything is hackable*, THE ECONOMIST, Apr. 8, 2017, at 73.
[48] The framework of state controls is examined comprehensively in Citron, *State Attorneys General*, *supra*.

through which public officials discuss shared or collateral responsibilities. The academic institutions and professional societies also function as educational hubs through which the U.S. privacy community and its foreign counterparts meet to learn about international developments. In combination, these interactions help crystallize shared understandings about the substance and process of privacy norms that can inform the development of international standards.

III. U.S. Privacy Law Implementation Design: Some Basic Principles

The discussion below approaches the question of institutional design for privacy policy implementation from two perspectives. First, what considerations should guide the design of the system as a whole? Second, what criteria should inform the allocation of tasks to specific institutions within the larger system framework?

A. System-wide Design Criteria

U.S. privacy policy implementation should satisfy five basic criteria: policy coherence, well-defined lines of authority, cost-minimization, adaptability, and diversification.

Policy Coherence. The implementation framework should foster the development of clear and consistent commands. Affected operators should not to have to reconcile conflicting obligations with respect to the same activity. Similarly situated operators should be subject to the same obligations. Industry-specific variations should be justified by the distinctive needs of the sector. And individual regulators should be attuned to the spillover effects of their own decisions upon other regulators and other industries.

Well-Defined Lines of Authority. Affected operators, citizens, and foreign data protection officials should have a clear view of the responsibilities of each implementation institution.

Cost-Minimization. Regulatory objectives should be achieved at the lowest possible cost to operators and citizens – meaning that needless institutional complexity should be avoided.

Adaptability. The regulatory system should be designed so it can adapt to changing conditions, including the ability to address new phenomena and technological developments. To do so, the system should have the resources and policy tools to stay abreast of new developments and reasonably elastic mandates – for example, by rulemaking – to adjust legal commands over time.[49]

Diversification. Overlapping or parallel authority can serve as a useful safeguard against failure by any single institution, and can facilitate policy experimentation that produces good solutions to new problems.

Tensions inevitably can arise among these goals. For example, the diversification that can promote useful experimentation and adaptability can come at the cost of systemwide coherence

[49] See Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 Geo. Wash. L. Rev. 1703, 1714-22 (2016) (discussing how administrative agencies can use rulemaking and other policy tools to adapt to changing conditions).

(more regulators taking different approaches to solving the same problem). The purpose of focusing on these criteria is to recognize design tradeoffs and identify areas for possible improvement.

B. Allocation of Regulatory Tasks

Seven criteria should guide the assignment of responsibilities to individual agencies.[50]

Policy Coherence. At the agency level, one must ask whether the privacy mandate fits within the agency's existing portfolio of duties. The issue is relatively simple when privacy is the agency's only responsibility – but that really does not apply to our current regulatory framework. The key participants in privacy regulation – the DOJ, the FCC, the FTC, and state attorneys general – all have diversified mandates. The wisdom of placing privacy within a multi-function agency, or giving a privacy role to an agency that presently does something else, depends principally on whether privacy and the other functions are policy complements rather than policy substitutes.

Branding and Credibility. Agencies develop reputations or "brands" that convey information about their aims and effectiveness. A good brand is an asset when the agency appears before other governmental bodies (e.g., courts or legislatures), deals with affected operators, or interacts with foreign authorities. The assignment of unrelated functions to an agency can diminish its brand, even if the functions are not policy substitutes. Excessive diversification can reduce the agency's ability to define its role clearly and to build a reputation for competence and effectiveness.

Capability and Capacity. Capability refers whether the agency has the statutory powers, organizational structure, and processes to perform its assigned role effectively. Capacity focuses on whether the agency has the resources – human capital and physical infrastructure – to fulfill its responsibilities. Legislators routinely give regulators too little power and too few resources to meet the goals set out in the law. Some degree of mismatch between ends and means is inevitable, but serious imbalances will cause policy failures.

Adaptability. Regulators must be able to adapt to technological development and other unforeseen circumstances. In many respects, adaptability is a function of the agency's capability (grant of authority) and its capacity (human and physical resources).

Internal Cohesion. A major determinant of agency effectiveness is the successful integration of its internal operating units.[51] For a single-purpose agency with law enforcement duties, this requires joining up the work of case-handling units, the general counsel's office, and other relevant operating units. For a body with a multi-member governance system, the attainment of internal cohesion also involves the formulation, to the greatest extent possible, of a common

[50] These criteria are derived from Hyman & Kovacic, *Why Who Does What Matters*, supra at 1468-83.
[51] *See, e.g.*, Jennifer Nou, *Intra-Agency Coordination*, 129 Harv. L. Rev. 421 (2015). *See also* Bijal Shah, Toward an Intra-Agency Separation of Powers, 92 N.Y.U. L. Rev. 101 (2017); Jon D. Michaels, Of Constitutional Custodians and Regulatory Rivals: An Account of the Old and New Separation of Powers, 91 N.Y.U. L. Rev. 227 (2017); Daniel Carpenter, *Internal Governance of Agencies: The Sieve, the Shove, the Show*, 129 Harv. L. Rev. F. 189 (2016)

vision on the part of board members and the development of techniques for communicating that vision inside and outside the agency. For a multi-function agency, internal cohesion requires mechanisms to ensure that conceptual policy synergies are realized in practice.

Relationship to the Larger Regulatory Ecosystem. In many settings, two or more public agencies exercise the same or related policy making duties or law enforcement functions. The assignment of concurrent or parallel authority to two or more institutions is usually a source of tension, as the relevant agencies understandably regard one another as rivals rather than partners.

Despite antagonisms, agencies recognize the need for cooperation and develop a range of mechanisms, some formal (e.g., the execution of an interagency memorandum of understanding) and some informal (e.g., regular discussions among agency leaders and case-handlers), to achieve policy coherence across the system and reduce conflict. Decisions about whether to move policy functions from one agency to another, or to situate new duties in an existing agency, should be undertaken with awareness of these policy synapses.

Political Support. The effectiveness of a design for a single institution requires that the design be politically sustainable. Does the agency's substantive mandate and organization enable it to gain the assent of elected officials (e.g., in the form of adequate appropriations) for the successful performance of its duties? The decision in Dodd-Frank to insulate the new Consumer Protection Financial Bureau (CFPB) so extensively from political interference reflected the belief that only a truly autonomous regulator would take bold action to avoid another collapse of the financial system.[52] Yet the full collection of safeguards – notably governance by a single director appointed for a fixed term, and funding through fees collected by the Federal Reserve Board – exposed the new institution to assault in the courts about whether it possessed a necessary degree of accountability.[53]

IV. Applying Our Criteria: Who Should Do What?

An overhaul of the framework of substantive privacy policy ought to be accompanied by a reexamination of the framework of implementing institutions. From a system-wide perspective, measured by the criteria set out in Section III, the U.S. regime for implementing privacy policy has serious weaknesses. Perhaps the most noteworthy is a lack of coherence. The heavy reliance on an accumulation of sector specific and activity specific statutory measures has established a mosaic that contains potent controls but lacks unifying principles and has important gaps. The FTC has used its UDAP authority to fill some of the gaps, but the agency's jurisdictional limitations are a serious disability. Coherence also suffers from the ability of individual regulators – state and federal – to establish new interpretations or requirements without the need to coordinate their choices with other regulators or to consider the impact of new initiatives on the larger ecosystem of privacy regulation.

The fragmentation of responsibility also denies the United States coherence and credibility in the eyes of its foreign counterparts. Some foreign privacy regulators downgrade the U.S. privacy

[52] Arthur E. Wilmarth, *The Financial Service Industry's Misguided Quest to Undermine the Consumer Financial Protection Bureau*, 31 REV. BANKING & FINANCIAL L. 881 (2011-2012).
[53] Seila Law LLC v. CFPB, 140 S. Ct. 2183 (2020).

regime on substantive grounds, often pointing to the lack of an omnibus statutory foundation with universal applicability. Others score the U.S. system poorly for the absence of a simplified implementation framework overseen by a single national privacy regulator with broad powers and supplemented by state-level enforcement pursuant to clearly delegated lines of authority. Simplification of the U.S. implementation regime, anchored by the establishment of a national privacy regulator, and a better clarification of authority among its regulators would give the United States more influence in global privacy policymaking.[54]

What might such a simplified, clarified framework look like? There are a number of possible approaches for ordering the relationship of public agencies in policy domains occupied by multiple authorities.[55] For the national privacy authority, I single out two options. One is to enhance the powers of the Federal Trade Commission, which, as noted above, is the closest equivalent to a U.S. national privacy agency.[56] The other is to create a new free-standing national privacy agency.

A. Make an Enhanced the FTC the Principal National Privacy Regulator

Under the first option, Congress would eliminate the FTC's jurisdictional limitations and give it authority to enforce privacy in every domain of U.S. commerce and with respect to not-for-profit institutions. Other government agencies (e.g., the Department of Health and Human Services) would retain concurrent powers to enforce privacy laws, but only pursuant to rules and other guidance set by the FTC, and under a regular process of consultation involving the FTC and its federal counterparts. Such a concurrency regime could be modeled along the lines of the United Kingdom's competition policy framework by which the Competition and Markets Authority (CMA) and sectoral regulators such as OFGEN and OFCOM share authority for the enforcement of the nation's competition laws. The CMA and the sectoral regulators engage in regular consultations through the United Kingdom Competition Network (UKCN), which serves to coordinate competition policy implementation and ensure cooperation in the application of the CMA's law enforcement and other policymaking tools.

The case for making an enhanced FTC the national regulator is straightforward. Of all U.S. privacy implementation institutions, the FTC has unequaled capacity in the form of expert case handling and policy teams and physical resources (including the development, over the past decade, of an internet laboratory to do high-quality forensic work). The agency's capacity also is the product of extensive experience in applying its UDAP authority and enforcing statutes such as the FCRA and COPPA. The FTC has a broad portfolio of policy instruments (litigation, rulemaking, consumer and business education, data collection, the preparation of reports, the convening of conferences), and it has demonstrated its ability to use all of them to good effect in the privacy domain. The FTC's stature as an independent agency gives it additional credibility in the eyes of foreign officials, who tend to distrust the vesting of privacy powers in an executive

[54] See Gellman, *Privacy Protection Board*, *supra* at 1187 ("[W]ith the international critical mass of data protection agencies that now exists, a country without an agency is at a disadvantage.").

[55] These options are analyzed in Alejandro E. Camacho & Robert L. Glicksman, *Functional Government in 3-D: A Framework for Evaluating Allocations of Government*, 51 HARV. J. LEGIS. 19 (2014).

[56] Several scholars have proposed that the FTC, using its existing grants of authority, could expand its role in developing coherent nationwide privacy standards. See Hartzog & Solove, *FTC Data Protection*, *supra*; Hoofnagle, FEDERAL TRADE COMMISSION PRIVACY LAW, *supra*.

department.

Within an enhanced FTC, privacy policy implementation also would be informed by the Commission's larger experience with consumer protection. The FTC's privacy unit is one part of its Bureau of Consumer Protection, rather than being a self-contained bureau. This reflected the institution's reasonable view that the effort to safeguard consumer interests in "privacy" was one dimension of "consumer protection," rather than a wholly distinct policy realm. Our impression is that many matters that involve privacy issues also raise problems that fit within other areas of the FTC's consumer protection program. The analysis of the "privacy" issue often benefits from perspectives developed in the course of applying the agency's deception and unfairness authority in other cases. The intertwining of privacy issues with other consumer protection concerns in many scenarios has important implications for how the mandate of a privacy agency should be defined. In whatever setting one ultimately might place a "privacy" mandate, I anticipate that the host agency would have a mandate that incorporates powers that traditionally have been associated with the FTC's broader consumer protection program.[57]

The implementation of privacy policy also can benefit from the Commission's work as an antitrust agency. The latter experience has provided a deeper knowledge of about the relevant commercial operators and an understanding of how competition can be a valuable force to press companies to provide better privacy protection. In all its work, the Commission draws upon a Bureau of Economics with over 80 Ph.D. economists in industrial organization economics. This bureau has developed considerable skill in sub-disciplines (such as behavioral economics) with special application to privacy issues.

Of course, inputs are not the same thing as outputs. The FTC has not always achieved the full integration of perspectives that the combination of these institutional capacities would permit. And, although there are policy complementarities across the domains of antitrust, consumer protection, and privacy, this combination of functions is not an unmixed blessing. An agency with all three functions might seek to use its position as a gatekeeper with respect to one policy domain to leverage concessions from firms over which it exercises oversight in another domain.[58] Such temptations have been present when the FTC has applied its antitrust powers to review mergers involving companies in the information services sector.[59] Finally, there is the possibility that any one of these functions might be diminished if all three are contained in the same agency. An agency focused solely on privacy will make privacy policy its single concern. An agency responsible for antitrust, consumer protection, and privacy is likely to find itself making tradeoffs as it sets priorities for how to use its resources.

A decision to give the FTC an expanded privacy role would also require some reevaluation of the FTC's portfolio. More privacy powers (and a larger privacy budget) would make antitrust a comparatively smaller element of the FTC's program. Consumer protection (including privacy)

[57] The interconnections between the domains of privacy law and consumer protection law are explored in one context in Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).
[58] William E. Kovacic & David A. Hyman, *Regulatory Leveraging: Problem or Solution?*, 23 Geo. Mason L. Rev. 1163 (2016)
[59] Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 Antitrust L.J. 121 (2015).

now consumes about 55 percent of the agency's budget. An expanded privacy role would reduce the overall percentage of resources devoted to antitrust policy still further. The augmentation, or possible augmentation, of the FTC's privacy role could well trigger a larger debate about whether the FTC should retain its antitrust mandate, or instead divest its antitrust functions to the Antitrust Division of the DOJ.[60] If this path is followed, the long term result of making the FTC the nation's top privacy cop may to transform the agency into a consumer protection/privacy regulator, rather than a consumer protection/antitrust regulator.

For international relations, the enhanced FTC solution likely would make the FTC an more effective participant in international policy discussions and deliberations on international standards. With the jurisdictional loopholes closed, the FTC properly could claim to speak with respect to all matters affecting commerce. The independent agency configuration gives the agency sufficient distance from the executive branch to avoid concerns that would occur abroad if the U.S. data protection authority were an executive department.

B. A New National Privacy Regulator

The second option for creating a national privacy regulator would be for the FTC to spin off its privacy functions to a newly formed independent commission, which also might absorb privacy-related functions of other federal bodies.[61] Compared to a multi-function agency, an independent, privacy-only commission would have internal policy cohesion and greater ability to develop a well-understood policy brand.[62] These conditions potentially would improve the agency's ability to function effectively within the U.S., and to engage with foreign authorities, who no longer would have concerns that the U.S. regulator's privacy program was diluted by attention to non-privacy policy duties. This cohesiveness and clarity would come at the cost of losing connection to relevant experience assembled in the fulfillment of the FTC's antitrust and consumer protection missions. On the other hand, the powers of the new institution could be defined in a way that enables the agency to address privacy issues with consumer protection powers akin to those now exercised by the FTC.

The independent privacy agency also would be untethered from the discipline provided by the work of the FTC's Bureau of Economics, which has pushed the FTC's antitrust and consumer protection lawyers to apply economic analysis in the development of cases and rules. Of course, it would be possible to give the new privacy agency a similar analytical capacity. As with the FTC, the actual application of that capability would depend heavily on the training and

---

[60] Similar questions would arise if Congress disbanded the Consumer Financial Protection Bureau, and assigned the FTC a large part of its duties. The FTC's current headcount is about 1200, and the CFPB's is roughly 2000. If the FTC absorbed all, or even half, of these employees, the share of agency resources dedicated to antitrust would fall to under a third of the agency's budget – posing the same question about whether an agency whose duties are so heavily weighted toward consumer protection should retain antitrust responsibilities.

[61] This would not be the first time that the FTC served as an incubator for a new federal institution. The FTC performed this role in the creation of the Securities Exchange Commission in the 1930s. Similarly, the establishment of the Consumer Product Safety Commission in the 1970s and the CFPB both involved the absorption of programs developed within the FTC.

[62] Compare Yoon-Ho Alex Lee, *Beyond Agency Core Mission*, 68 ADMIN. L. REV. 551 (2016) (discussing approaches that can enable an agency to effectively perform policy functions that lie beyond what might be considered to be its "core mission").

preferences of the new agency's leadership. One function we would expect the FTC or a new stand-alone privacy agency to perform is to evaluate the effects of individual privacy initiatives at the federal and state levels, and periodically to assess the impact of the U.S. privacy system as a whole.

In setting out this option, I recognize all of the difficulties that arise in the creation of a new institution that absorbs many of its functions and personnel from other agencies. No one should underestimate the lost productivity that occurs during the period of transition. Nor can one ignore the costs of knitting new functions and personnel into a new institution. Bringing a variety of disparate mandates and teams under a single roof does not mean that they automatically will function as an integrated whole. These changes are the equivalent of major surgery, and recovery time for the new organization can be substantial.

C. Suggested Approach

I recommend the first approach set out above: to denominate the FTC as the principle U.S. data protection authority for consumer-facing privacy matters. As suggested above, a necessary legislative foundation for this approach would involve (a) eliminating the jurisdictional exclusions from the FTC's mandate, (b) creating the FTC concurrent enforcement authority with respect to all consumer-facing federal statutes, and (c) giving the FTC an express mandate to perform the coordination functions among federal and state agencies.

This approach would not divest other government agencies of the privacy policy functions they now perform, nor would it involve the FTC's absorption of staff now resident in other government agencies. Other governmental institutions will continue to have important privacy responsibilities. The DOJ will retain an important role, prosecuting cybercrimes and other grave infringements of privacy laws. The Department of Commerce and the other ad hoc bodies within the Office of the President will continue to be active in the privacy space, given the prominence of privacy issues in domestic economic policy, in international trade negotiations, and in foreign relations generally.[63]

What about the states? Some commentators have argued that a full-scale renovation of the U.S. privacy framework should preempt the ability of states to pursue initiatives inconsistent with national policy.[64] I think an alternative pathway holds greater promise. Federal and state privacy regulators currently cooperate in a variety of ways, but there is no systematic mechanism for policy coordination, let alone promoting convergence on shared norms. I envision an extension of existing cooperation and coordination efforts through the establishment of a domestic privacy network (DPN).[65] Such a network could encourage individual privacy regulators to converge upon superior policy norms.

---

[63] *See, e.g.*, Swire, *supra*.

[64] The debate over preemption of the states' role in privacy policy is reviewed in Citron, supra note xx, at 798-803. See also Robert A. Mikos, *Making Preemption Less Palatable: State Poison Pill Legislation*, 85 GEO. WASH. L. REV. 1 (2017).

[65] For a discussion of the possible creation of such a network to deal with competition law, *see* William E. Kovacic, *Toward a Domestic Competition Network*, in COMPETITION LAWS IN CONFLICT 316 (Richard A. Epstein & Michael S. Greve eds., 2004).

Among other tasks, the DPN could use the accumulated experience of state regulators to devise model laws – for example, a law dealing with data breaches – that could provide focal points for convergence. Here the DPN would play a role akin to that performed by American Law Institute and the National Council of Commissioners on Uniform State Laws in the drafting of the Uniform Commercial Code, which supplied an influential focal point for the reform of state codes.[66]

In general terms, this approach to improving the institutional framework for privacy seeks to improve policy formation and implementation by contract across existing agencies rather than by a merger that places all relevant functions within a single institution. The integration-by-contract approach involves greater costs of coordination, but it has several major benefits. It avoids the disruption that takes place when responsibilities and personnel are reallocation across agencies. I believe such reorganizations are difficult to justify unless the benefits are compelling.

D. Resources

The development of a full-scale national privacy regulatory body, as a stand-alone agency or as part of an enlarged FTC, will not come cheaply. I do not have a precise estimate for the Committee's consideration, but a substantial expansion in resources will be necessary to fulfill the ambitions of a new omnibus law.

Measures to upgrade the US privacy regime will require a considerable boost in capacity of the federal privacy regulators responsible for promulgating rules and enforcing rules and statutes.[67] Not only is the drafting of strong rules difficult, but enforcement will encounter arduous opposition from the affected businesses. The targets of rules and enforcement will marshal the best talent that private law firms, economic consultancies, and academic bodies can offer to oppose the government in court.

For privacy reforms to be effective, it is necessary that ambitious policy commands be backed up with ambitious funding. An enhanced privacy program therefore will go only as far as the talent of the agencies will carry it. We propose three steps to build and retain the human capital – attorneys, economists, technologists, and administrative managers – to undertake a more ambitious litigation program.

To accomplish the desired privacy upgrade, I see a need for more resources, but not simply to build a larger staff by hiring more people. It is also to attract and retain a larger number of elite personnel who are equal to the tasks that the ambitious reform agenda will impose. I would use an increase in resources to boost compensation substantially, which means taking the federal privacy agencies out of the existing civil service pay scale. I do not see how the public agencies can recruit and retain necessary personnel without a significant increase in the salaries paid to case handlers and to senior managers.

---

[66] Compare Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1903 (2013) (using the UCC analogy to discuss the development and broad adoption of privacy norms).

[67] For a comparable proposal to upgrade the quality of the federal competition policy program, see Alison Jones & William E. Kovacic, The Institutions of US Antitrust Enforcement: Comments for the US House Judiciary Committee on Possible Competition Policy Reforms (Apr. 17, 2020).

Consider two possibilities for compensation reform. The first is to align privacy agency salaries with the highest scale paid to the various U.S. financial service regulators. Here the model would be the compensation paid to employees of the banking regulatory agencies; the salary scale for these bodies exceeds the General Schedule (GS) federal civil service wage scale by roughly twenty percent.[68] In adopting the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010,[69] Congress concluded that the importance of the mission of the new Consumer Financial Protection Bureau (CFPB) warranted higher salaries for the agency's personnel. If the higher salary scale made sense for the CFPB, we see no good reason why a more generous compensation schedule is not appropriate for the privacy agencies.[70] Are the duties entrusted to the federal privacy agencies any less significant? If the answer to these questions is "no," Congress should allow the privacy agencies to pay at least the same wages as the CFPB does.

A second alternative requires a more dramatic change, which I would implement in the first instance at the FTC. I would triple the FTC's existing budget of about $330 million per year and use the increase mainly to raise salaries and partly to add more employees. This experiment might be carried out for a decade to test whether a major hike in pay would increase the agency's ability to recruit the best talent, retain the talent for a significant time, and apply that talent with greater success in a program that involves prosecuting numerous ambitious cases and devising other significant policy initiatives.

I see a major increase in compensation, either by adopting the CFPB model or trying our more dramatic alternative, to be a crucial test of our national commitment to improved privacy protections. If fundamental privacy policy reforms are vital to the nation's well-being, then the country should spend what it takes to get the best possible personnel to run the difficult cases (and carry out other measures, such as the promulgation of trade regulation rules) that will be the pillars of a new, expanded program. Such steps will become even more important if new political leadership seeks to close the revolving door, which has operated as a mechanism to encourage attorneys and economists to accept lower salaries in federal service in the expectation of receiving much higher compensation in the private sector at a later time.

V. Conclusion

The improvement of the U.S. privacy system requires as much attention to implementation as it does to the appropriate content of substantive privacy standards. A top to bottom review of implementing institutions ought to accompany the development of an omnibus U.S. privacy act. The existing fragmentation of policymaking and enforcement duties, coupled with significant

[68] See Paul H. Kupiec, The Money in Banking: Comparing Salaries of Bank and Bank Regulatory Employees (American Enterprise Institute, April 2014), https://www.aei.org/wp-content/uploads/2014/04/-the-money-in-banking-comparing-salaries-of-bank-and-banking-regulatory-employees_17170372690.pdf.

[69] Pub. L. No. 111-203, 124 Stat. 1376 (2010).

[70] As a member of the FTC, one of us (Kovacic) observed firsthand how the disparity in salaries between the CFPB and the FTC resulted in a significant migration after 2010 of the Commission's elite consumer protection attorneys and economists to the CFPB. Many of these individuals were major contributors to the FTC's consumer protection programs because they combined outstanding intellectual skills with decades of experience (much of it in middle-level and senior management positions) at the Commission. It was impossible to replace them with individuals of comparable skill and experience, and the FTC's performance suffered as a consequence.

gaps in coverage, denies the U.S. system policy coherence at home and diminishes the influence of the U.S. in international deliberations about global privacy norms.

This testimony has offered two options for the development of a next-generation national privacy regulator: the enhancement of the powers and role of the Federal Trade Commission, or the creation of a new, independent privacy commission whose core would consist of privacy functions previously performed by the FTC. The establishment of a national privacy regulator would be supplemented by expanded reliance on policy networks to link implementation at the federal and state levels.