Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 4

Article 3

2019

Implementing Privacy Policy: Who Should Do What?

David Hyman
Georgetown University Law Center, dah137@georgetown.edu

William E. Kovacic
George Washington University Law School, wkovacic@law.gwu.edu

Implementing Privacy Policy: Who Should Do What?

Cover Page Footnote

David A. Hyman is a Professor at Georgetown University Law Center. From 2001– 2004, he served as Special Counsel to the Federal Trade Commission. William E. Kovacic is the Global Competition Professor of Law and Policy at the George Washington University Law School. He served as General Counsel at the FTC from 2001–2004, and was a Commissioner from 2006 to 2011, chairing the agency from March 2008 to March 2009. He currently is a Non-Executive Director of the United Kingdom's Competition and Markets Authority. The views expressed herein are the authors' alone. We received exceptionally helpful comments from Bob Gellman when this paper was presented at the 10th Annual Privacy Law Scholars Conference (May 2017). We also want to acknowledge the helpful comments we received from other attendees at the conference, including Aaron Burstein, Pam Dixon, Sharon Bradford Franklin, Zachary Goldman, David Gray, Lance Hoffman, Chris Hoofnagle, Cam Kerry, Siona Listokin, Bill McGeveran, Joanne McNabb, Terrell McSweeny, Whitney Merrill, Hannah Meyer, Ira Rubenstein, Jay Stanley, Peter Swire, and Omer Tene.

Implementing Privacy Policy: Who Should Do What?

David A. Hyman & William E. Kovacic*

Academic scholarship on privacy has focused on the substantive rules and policies governing the protection of personal data. An extensive literature has debated alternative approaches for defining how private and public institutions can collect and use information about individuals. But, the attention given to the what *of U.S. privacy regulation has overshadowed consideration of* ***how and by whom*** *privacy policy should be formulated and implemented.*

U.S. privacy policy is an amalgam of activity by a myriad of federal, state, and local government agencies. But, the quality of substantive privacy law depends greatly on which agency or agencies are running the show. Unfortunately, such implementation-related matters have been discounted or ignored—with the clear implication that they only need to be addressed after the "real" work of developing substantive privacy rules is completed.

---

* David A. Hyman is a Professor at Georgetown University Law Center. From 2001–2004, he served as Special Counsel to the Federal Trade Commission. William E. Kovacic is the Global Competition Professor of Law and Policy at the George Washington University Law School. He served as General Counsel at the FTC from 2001–2004, and was a Commissioner from 2006 to 2011, chairing the agency from March 2008 to March 2009. He currently is a Non-Executive Director of the United Kingdom's Competition and Markets Authority. The views expressed herein are the authors' alone.

We received exceptionally helpful comments from Bob Gellman when this paper was presented at the 10th Annual Privacy Law Scholars Conference (May 2017). We also want to acknowledge the helpful comments we received from other attendees at the conference, including Aaron Burstein, Pam Dixon, Sharon Bradford Franklin, Zachary Goldman, David Gray, Lance Hoffman, Chris Hoofnagle, Cam Kerry, Siona Listokin, Bill McGeveran, Joanne McNabb, Terrell McSweeny, Whitney Merrill, Hannah Meyer, Ira Rubenstein, Jay Stanley, Peter Swire, and Omer Tene.

As things stand, the development and implementation of U.S. privacy policy is compromised by the murky allocation of responsibilities and authority among federal, state, and local governmental entities—compounded by the inevitable tensions associated with the large number of entities that are active in this regulatory space. These deficiencies have had major adverse consequences, both domestically and internationally. Without substantial upgrades of institutions and infrastructure, privacy law and policy will continue to fall short of what it could (and should) achieve.

"The world's most valuable resource is no longer oil, but data."[1]

"In the '20s and '30s it was the role of government.
'50s and '60s it was civil rights.
The next two decades are going to be privacy."[2]

INTRODUCTION

For the past few decades, academics, government officials, and practitioners have debated the merits of privacy law and policy.[3] Most of the debate has focused on the substantive rules and policies that dictate how private and public institutions can collect and use information about individuals. Various commentators have offered frameworks, templates, and design principles for developing an optimal set of privacy rules.[4] The most popular approach appears to be codifying and extending existing substantive law by adopting an omnibus federal privacy statute—although there is considerable disagreement on the details of what such a statute should include.[5]

---

1 *The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [https://perma.cc/52PK-9LGL].

2 *The West Wing: The Short List* (NBC television broadcast Nov. 24, 1999).

3 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 paper, we use the term "privacy" to encompass both ideas. *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235 (2015). We define what we mean by privacy law and the institutions that carry out privacy functions below. *See* discussion *infra* Part II.

4 *See generally* Dan Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 352; ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf [https://perma.cc/V2YV-8DE3].

5 *See, e.g.*, *Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy*, WHITE HOUSE (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/D68Q-VHCT].

This emphasis on policy substance has overshadowed issues of administrative implementation—a problem that is certainly not unique to privacy policy.[6] That said, even casual observers of the U.S. system know that a bewildering assortment of federal, state, and local governmental entities are active in the privacy policy space. The hodgepodge of involved institutions deserves close attention, for the quality of substantive privacy policy depends greatly on which agency (or agencies) run the show.

In the past fifteen years or so, academics, government officials, and practitioners have devoted more attention to implementation issues.[7] Some scholars have examined how the Federal Trade Commission ("FTC") has become the closest U.S. equivalent to a national privacy authority—a status owing both to historical accident and to the FTC's conscious efforts to occupy a significant un-colonized policy space.[8] Others have considered how the

---

[6] 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."). *See also* David A. Hyman & William E. Kovacic, *Competition Agencies with Complex Portfolios: Divide or Conquer?*, CONCURRENCES REV. NO. 1-2013, ART NO. 50967, 1-2 (2013), https://www.concurrences.com/en/review/issues/no-1-2013/conferences/competition-agencies-with-complex-policy-portfolios-divide-or-conquer-chicago ("The specific amalgamation of policy tasks within a single government body has important consequences for how competition agencies define their goals, allocate resources, and select programs to fulfill their duties. The assignment of multiple regulatory tasks can deeply affect a competition agency's performance, just as it affects the performance of other agencies. This issue has attracted little attention in competition policy circles, although public administration scholars (and, to a far more limited extent, legal academics) have done important work on such issues in other areas.").

[7] *See, e.g.*, Symposium, *Enforcing Privacy Rights*, 54 HASTINGS L.J. 751 (2003) (collecting various papers on privacy policy implementation). Commentators before this period expressed concern with the adequacy of implementing institutions for privacy policy. But, our perception is that the attention to implementation has increased significantly in the more recent era.

[8] *See, e.g.*, CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 26–35 (2016); Hartzog & Solove, *supra* note 3, at 2232; *see generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114

development and enforcement of privacy policy should be allocated among federal agencies and across state governments.[9] Another line of commentary has compared U.S. privacy institutions to their counterparts abroad.[10]

In this paper, we build upon these contributions, and consider the optimal agency design with which to form and implement U.S. privacy policy. Despite important achievements, the existing configuration of implementing institutions leaves much to be desired. Authority over privacy is simultaneously murky and subdivided among multiple entities at the federal (i.e., the FTC and sector specific regulators), state, and local levels. The resulting dynamics (both horizontal and vertical) create considerable inter-agency tension and inconsistency.

In our experience at the FTC and working in Europe, we have seen that these institutional deficiencies have at least two distinct adverse consequences. First, the institutional status quo undermines the ability of the United States to develop coherent substantive privacy policy. Outwardly, the many public bodies at the national and state levels with privacy-related duties profess a common commitment to work collegially toward the development of sound privacy policies. To some extent, the expressed spirit of common cause is genuine, and it routinely manifests itself in helpful forms of policy coordination and enforcement cooperation. At the same time, in our roles inside and outside the government, we have observed a distressing tendency of participants to seek

---

COLUM. L. REV. 583 (2014). *See also* Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy*, *in* RESEARCH HANDBOOK OF RESEARCH ON DIGITAL TRANSFORMATIONS 21 (F. Xavier Olleros & Majlinda Zhegu eds., 2016) (noting the FTC's "entrepreneurial expansion of its jurisdiction" regarding privacy).

9 *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016); Peter Swire, *Why the Federal Government Should Have a Privacy Policy Office*, 10 J. TELECOM. & HIGH TECH. L. 41 (2012) [hereinafter Swire, *Privacy Policy Office*]; Peter Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime,* 7 J. ON TELECOMM. & 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).

10 *See generally* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959 (2016); Paul M. Schwarz, *The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

policymaking pre-eminence as an end in itself.[11] This (unfortunately quite predictable) impulse impedes the emergence of a privacy regime that exploits the benefits of institutional diversity and experimentation while also achieving needed levels of coherence.

The second adverse consequence involves the capacity of the United States to effectively participate in the formulation of global privacy standards. Our domestic institutional weaknesses hinder efforts by the U.S. government to encourage the development of superior international privacy standards and to achieve needed levels of cross-border cooperation in law enforcement.[12] At present, the European Union is the dominant influence in setting privacy standards that govern behavior by firms engaged in trans-Atlantic trade and, to a significant degree, in global commerce.[13] The General Data Protection Regulation, which took effect in May 2018, is simply the latest manifestation of the EU's preeminent role in setting international policy standards.[14] In pressing ahead with their own reforms, officials within the European Commission and the EU's member state data protection authorities often take a

---

[11] Most readers will be shocked to discover that this is going on. *See* CASABLANCA (Warner Bros. Productions 1942) ("I'm shocked—shocked—to find that gambling is going on in here.").

[12] *See* Hartzog & Solove, *supra* note 3, at 2271 (noting 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 and Solove 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 situation weakens the "soft power" that the U.S. government would otherwise have in this policy space. *See id.*

[13] *See* Sheera Frenkel, *Tech Giants Brace for Europe's New Privacy Rules*, N.Y. TIMES (Jan. 28, 2018), https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html [https://perma.cc/4UXC-H8DT] (describing the European Union's influence over information technology companies operating in Europe and in the United States).

[14] Regulation 2016/679, 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. *See generally* Ozan Karaduman, *The General Data Protection Regulation: Achieving Compliance for EU and Non-EU Companies*, 18 BUS. L. INT'L 225 (2017) (describing the General Data Protection Regulation).

dismissive approach to the U.S. privacy regime, and discount U.S. preferences regarding the optimal structure of privacy rules.[15]

The dismissive attitude of EU officials toward the U.S. partly derives from the EU's hope that it will be accepted as the world's foremost privacy regulator. One of us (Kovacic) has participated in many events in which European privacy officials lament the weakness of the U.S. system and assert that the U.S. regime is toothless. Recitals about the U.S. enforcement record—including cases prosecuted and fines collected—comes as a surprise, and occasionally seems to inspire a reconsideration of the inadequacy narrative. But come the next international meeting, and many of the same European officials will repeat the inadequacy narrative, and assert that the U.S. privacy regime is a paper tiger. Given these dynamics, it is not entirely clear how we should go about getting EU officials to take U.S. privacy regulation seriously, short of a complete transplant of the E.U. system (including its definition of privacy as a fundamental human right).

That said, one obvious strategy is for the U.S. to address the fragmented and convoluted framework of its domestic regulation of privacy. Foreign officials are understandably perplexed by the mélange of federal and state institutions—compounded by the patchwork of sector specific controls and the absence of any hierarchy of authority that would give one institution the "last word" on policy formation. We have seen the exasperation of foreign officials who fruitlessly seek clarity about who is in charge.

This state of affairs undermines U.S. efforts to shape the framework of global privacy standards. Until we improve policy coordination and establish a clear line of authority and responsibility, the U.S. will witness a further decline in its capacity to shape global privacy policy—which, at least in the technology sector, is arguably the single most important form of economic regulation currently in play. In sum, we believe reform of the

---

[15] The basis for this observation consists of conversations that one of us (Kovacic) has had with EU officials during his tenure as an FTC Commissioner (2006–11) and in subsequent meetings as a non-executive director of the United Kingdom's Competition and Markets Authority from 2013 to the present.

existing institutional arrangements are a necessary component if we want to improve substantive privacy policy—both at home, and in the effective participation of the U.S. in the formulation of global privacy standards.

In previous work, we explore the design of competition agencies and other regulatory bodies.[16] We draw upon this work to consider the future of privacy policy implementation in the U.S. To focus our discussion of institutional options, we assume that the U.S. will eventually undertake a fundamental retooling of substantive privacy policy—which seems likely to take the form of an omnibus privacy law that consolidates, restates, and extends existing federal privacy commands. But, as policymakers devise an omnibus privacy law, they should also simultaneously adjust the institutional arrangements through which the new substantive privacy framework will be administered. Indeed, even if an omnibus privacy statute is not adopted, there is considerable value in upgrading the mechanism for implementing and extending existing privacy mandates.[17]

We begin by describing the array of policy functions that fit under the privacy umbrella and identifying some of the principal public institutions that carry out these functions. We then set out seven criteria for judging the performance of the entities implementing U.S. privacy policy and for determining the optimal allocation of tasks to implementing institutions. We use this framework to propose several ways in which the U.S. should retool policy development and law enforcement in the privacy space. We present several options that will increase the coherence and effectiveness of the U.S. privacy system and enhance the influence of the U.S. in the development of international privacy policy. We focus chiefly on whether the FTC, with an enhanced mandate,

---

[16] *See generally* David A. Hyman & William E. Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 GEO. WASH. L. REV. 1446 (2014); Hyman & Kovacic, *supra* note 6.

[17] *See, e.g.*, Hartzog & Solove, *supra* note 3, at 2271 (noting that 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.")

should serve as the national privacy regulator, or whether a new dedicated privacy regulator should be created.

We conclude that the optimal strategy is to enhance the FTC's role, by eliminating gaps in its jurisdiction and expanding its capacity to promote cooperation among agencies with privacy portfolios. We expect that these steps will help rationalize privacy policy enforcement and encourage convergence on superior policy norms.

Our proposal for an enlarged FTC role focuses on two dimensions of privacy regulation. The first is what might be called the "consumer-facing" elements of a privacy. Our analysis 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. The second dimension involves the privacy of individuals as employees. Here we are concerned with laws and regulations that control what information employers can collect about their employees, and how such information can be distributed within the organization and shared with other bodies.[18]

We do not address the legal mechanisms that protect privacy where the actors are government institutions. Thus, we do not examine the appropriate framework for devising and implementing policies that govern data collection and record-keeping responsibilities of federal agencies.[19] We also do not address privacy questions that arise when government agencies conduct surveillance for national security purposes. We set aside these issues for another day, and we recognize there will be a continued, significant role for privacy policy makers in governmental entities other than the FTC. Thus, our suggestions for an expanded FTC

---

[18] In discussions with foreign governments about the EU-US Safe Harbor Privacy Principles, the FTC has taken the position that Section five of the FTC Act permits the agency to control transfers of data involving employees. This position is not easily reconciled with traditional interpretations that view the FTC Act as protecting the interests of individuals as consumers. *See* Hoofnagle, *supra* note 8, at 321–25 (describing the operation of the Safe Harbor mechanism). *See* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUSTON L. REV. 719, 738–46 (2001) (describing the soundness of the FTC's authority to enforce the Safe Harbor commitments).

[19] 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.

role with respect to consumer-facing privacy matters would leave in place the framework of controls that address other privacy concerns. Nonetheless, our proposal does contemplate stronger mechanisms to ensure policy consultation and coordination among governmental entities with privacy mandates—whether consumer-facing or not.

In addressing these issues, we generally do not take on the substance of U.S. privacy law. Our emphasis upon the benefits of system-wide coherence and effectiveness applies without regard to the specific privacy directives that our nation chooses to adopt. Thus, we do not address the debate over whether the conceptual foundation for privacy protection should be fair information practice principles ("FIPPs"),[20] a consequences-based theory of liability,[21] or some amalgam or these or other approaches. Of course, our views do reflect a judgment about which considerations ought to be taken into account in formulating substantive requirements. To the extent readers have different views or priorities, they may well reach different conclusions than we do about the optimal design of implementing institutions. Stated differently, your mileage (and preferred vehicle for getting to the destination) may vary.

I. U.S. PRIVACY POLICY DEVELOPMENT AND IMPLEMENTATION

Privacy law in the United States is a stark example of a "regulatory thicket."[22] We focus on two aspects of the regulatory thicket: the collection of substantive commands that fall within the

---

[20] *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) (describing FIPPs); *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101–11 (1992) (describing "core fair information principles"); GELLMAN, *supra* note 4, at 23.

[21] *See* J. Howard Beales III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 118–120 (2008) (presenting privacy policy approach based on proof of adverse consequences to consumers).

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

ambit of privacy regulation and the myriad public institutions responsible for formulating and 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.[23] 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.[24] Another set of controls establishes the conditions under which bodies such as credit rating services can assemble and use data on consumers.[25]

A second core function is to ensure that information about consumers is *adequately protected* from unauthorized use.[26] Some privacy laws require commercial bodies to establish safeguards against inadvertent disclosure of consumer information.[27] Others punish those who misappropriate consumer information to steal an individual's identify or property or damage an individual's reputation.[28] A further category of controls prohibits unauthorized access to data systems for the purpose of stealing sensitive data or disabling a data network.[29]

---

[23] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 491–547 (2006) (examining controls on the collection and use of information as elements of privacy policy).

[24] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 39–54 (2015) (describing the framework of controls).

[25] *See generally* HOOFNAGLE, *supra* note 8, at 268–305 (discussing legislation and controls that have impacted financial data privacy).

[26] *See id.* at 216–35 (discussing the FTC's standards for information security).

[27] *See generally* American Bar Association, *Antitrust Law*, *in* CONSUMER PROTECTION LAW DEVELOPMENTS 138–39 (2009) (describing legal obligations that require firms to safeguard consumer information).

[28] *See generally* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1246 (2003) (providing a review of protections against identity theft).

[29] *See generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010) (describing laws governing unauthorized access to computer databases).

A complex "jumble" of federal and state statutes seek to perform these functions.[30] Unlike a number of other countries, the United States has no omnibus federal privacy law.[31] Federal privacy law is a mosaic of controls that apply to specific categories of activity; to specific sectors; and to specific classes of individuals.[32] 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)[33]—is circumscribed by jurisdictional exclusions involving banks, common carriers, and not-for-profit institutions.[34] Nor does the FTC have responsibility to oversee data collection and protection by public institutions; a separate body of laws governs the duties of public agencies.[35] 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.[36]

State law and policy provide a major second dimension in U.S. privacy law.[37] The contributions of states, in many respects, equal or surpass the work of federal institutions in determining the privacy obligations of commercial actors. One impressive illustration of the significance of state policy making is the field of

---

30 Hartzog & Solove, *supra* note 3, at 2267.

31 *Id.*

32 *Id*.

33 15 U.S.C. § 45(a)(1) (2012).

34 The scope of these exemptions is a regularly litigated matter. *See generally* F.T.C. 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 them is transferred to the United States. *See* Gellman, *supra* note 9, at 1213–14.

35 *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).

36 *See generally* Stuart F. H. Allison et al., *Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics*, 33 J. CRIM. JUST. 19 (2005) (discussing the civil and criminal regimes for the prosecution of identity theft). On the criminal sanctions for unauthorized access to computer databases, see generally Kerr, *supra* note 29.

37 *See generally* Citron, *supra* note 9 (providing a comprehensive examination of the role of state law and policy in privacy).

data breach and notification legislation. At least forty-five states have enacted laws that require firms to notify individuals when an unauthorized disclosure of consumer information has taken place.[38]

In this and other areas of privacy policy, state governments have played an important role in devising and testing various forms of privacy controls. For example, any listing of the most important sources of privacy law in the United States would have to include the State of California.[39] Measured by its power to shape national privacy norms, California deserves a place in any discussion of which institution determines 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 the delegation that represents the United States in international gatherings of privacy officials.[40]

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 a routine feature of the U.S. system.[41] But 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.[42] Privacy stands out for study not just because of the complexity of the U.S. system considered in isolation, but

---

[38] *See* Gregory James Evans, *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, 203 n.93 (2015).

[39] On California's central role as a privacy regulator, see Citron, *supra* note 9, at 762.

[40] Indeed, one could reasonably argue that California has an active foreign policy portfolio—and not just on privacy. *See* David Freeman Engstrom & Jeremy M. Weinstein, *What if California Had A Foreign Policy? The New Frontier of States' Rights,* 41 WASH. Q. 27 (2018) ("[Governor Jerry] "Brown eagerly positioned California at the forefront of global efforts to confront climate change. . . Because California prides itself on its global reach, the idea of a distinctively Californian foreign policy has been kicking around for a while.")

[41] *See* Hyman & Kovacic*, supra* note 6, at 9.

[42] For a discussion of the complexity of the regulatory framework for privacy policy in the United States, *see supra* notes 23–28 and accompanying text.

also by comparison to many foreign privacy regimes, which use far fewer institutions to implement substantive privacy law.

Below, we sketch out the regulatory ecosystem for the implementation of domestic privacy policy. We use the term "ecosystem" to capture several distinctive features of the U.S. regime.[43] One element is the extraordinary diversity of institutional species/entities. A large number of these institutions have developed programs and processes for devising privacy policy and enforcing privacy legal commands.[44] A careful understanding of what each institution does, and knowledge of how it evolved, should precede decisions to uproot individual species, or to introduce new species into the ecosystem.

A second element of the privacy ecosystem is a relatively rapid adaptability that flourishes through a process of decentralized decision making and does not depend on central direction as a predicate for policy development. Despite the lack of an omnibus privacy law, institutions at the national and state levels have adjusted over time to the emergence of new commercial phenomena and to rapid technological change.[45]

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

---

[43] *See supra* notes 23–28 and accompanying text (describing the "regulatory ecosystem" of the federal government). In fairness, our ecosystem metaphor obscures the degree of "intelligent design" in the system, as well as the extent to which dumb luck plays a role. *See, e.g.,* SAMUEL ELIOT MORISON, THE OXFORD HISTORY OF THE UNITED STATES 1783–1917, at 413 (1927) ("Prince Bismarck is said to have remarked, just before his death, that there was a special providence for drunkards, fools, and the United States of America.").

[44] *See supra* notes 23–28 (describing the "regulatory ecosystem" of the federal government).

[45] *See, e.g.*, David C. Vladeck, *Charting the Course: The Federal Trade Commission's Second Hundred Years*, 83 GEO. WASH. L. REV. 2101, 2102–11 (2015) (describing the modern evolution of FTC's role in developing privacy policy standards).

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 U.S. privacy body.[46] 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).[47] The Commission's privacy work is grounded partly in laws that, in whole or in part, are specifically designed as privacy measures. These include early measures, such as the Fair Credit Reporting Act ("FCRA")[48] and more recent enactments such as the Gramm-Leach-Bliley Act[49] and the Children's Online Privacy Protection Act ("COPPA").[50] The FTC has built an extensive "common law" of privacy protection through settlements in cases brought pursuant to its UDAP mandate.[51]

Most privacy scholars regard this process of common law elaboration as a useful approach,[52] but this view is not universally accepted.[53] The FTC has also used its rulemaking authority to

---

[46] *See* HOOFNAGLE, *supra* note 8, at 192 ("The Federal Trade Commission has emerged as the nation's top regulator of privacy."); Hartzog & Solove, *supra* note 3, at 2267 ("In the current U.S. privacy regulatory system, the FTC has grown into the role of being the leading regulator of privacy . . .").

[47] For a discussion on the ascent of privacy as a distinct focus of FTC policymaking and on the possibilities for future elaboration of the Commission's role in this field, *see* Hoofnagle, *supra* note 8; Hartzog & Solove, *supra* note 3; Vladeck, *supra* note 44, at 2102–11

[48] 15 U.S.C. § 1681 (2012).

[49] 15 U.S.C. §§ 6804–05 (2012).

[50] 15 U.S.C. § 6505 (2012).

[51] The FTC is not alone in using the administrative process to build legal norms. *See* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 958 (2016).

[52] Positive assessments include Solove & Hartzog, *supra* note 8, and HOOFNAGLE, *supra* note 8.

[53] For a negative assessment of the FTC's contributions to privacy policy, see Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?*, ACLU (Oct. 25, 2016), http://www.aclu.org/blog/free-future/can-consumers-trust-ftc-protect-their-privacy

build important elements of the national privacy architecture, including the Do-Not-Call rule, which was promulgated pursuant to the Telemarketing Sales Act.

Some critics view the FTC's privacy program as a barrier to the adoption of an improved privacy regime. One of us (Kovacic) attended a privacy conference as an FTC official, and was approached by a privacy advocate who condemned the FTC and its use of 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 dramatically upgrade the U.S. privacy framework. Only if the FTC stood down, he said, would the serious inadequacies of the status quo be revealed, and the necessary support for needed reforms materialize.

The FTC also has important "soft power" tools with which to set privacy policy.[54] 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.[55] The FTC has also played a major role as a convener of conferences, workshops, and seminars that have served to identify significant commercial trends and focus debate on key privacy issues.[56]

[https://perma.cc/UNV9-EGU9] ("[T]he FTC deserves low grades when it comes to protecting consumer privacy.").

[54] *See* Adam D. Thierer, Ryan Hagemann, and Jennifer Skees, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, COLO. TECH. L. J. (forthcoming 2019); *see also* 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, 2–3 (2010).

[55] *See, e.g.*, *Protecting Consumer Privacy and Security*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report [*https*://perma.cc/4QHA-6SLC] (last visited Feb. 12, 2019); s*ee also* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, *Protecting Privacy in the Era of Big Data*, Remarks at the International Conference on Big Data from a Privacy Perspective (Hong Kong, June 10, 2015), https://www.ftc.gov/public-statements/2015/06/protecting-privacy-era-big-data-remarks-ftc-chairwoman-edith-ramirez [https://perma.cc/3E43-8SXK].

[56] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Announces Agenda for PrivacyCon (Dec. 29, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/ftc-announces-agenda-privacycon [https://perma.cc/U6ZQ-CV32]. On the FTC's role in

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 FTC's oversight.[57] The exempted sectors assemble, use, and transmit massive amounts of data about individuals, yet they stand beyond the FTC's reach. It is difficult to envision the FTC serving as a truly effective national regulator of the consumer-facing elements of privacy policy 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.[58] 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, court decisions, and the FCC's adoption (2016) and revocation (2017) of the "net neutrality" rule.[59] By classifying broadband as a telecommunications service (bringing it within the ambit of the common carrier exemption), the FCC's net neutrality rule would have ousted the FTC from privacy oversight in this technological space. The revocation of the net neutrality rule preserved the FTC's role in this policy space.

The FCC is not the only federal agency with sector-specific privacy oversight. The Department of Education enforces the Family Educational Rights and Privacy Act (FERPA),[60] 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

---

convening events that provide fora for academics, advocacy groups, government officials, and practitioners to discuss privacy and other policy issues, see generally William E. Kovacic, *The FTC as Convenor: Developing Regulatory Policy Norms without Litigation or Rulemaking*, 13 COLO. TECH. L.J. 17 (2015).

57 These jurisdictional limitations are described in *Antitrust Law Developments*, AMERICAN BAR ASS'N, 658–59 (7th ed. 2012).

58 *See* HOOFNAGLE, *supra* note 8, at 335–37 (describing FCC's role in privacy regulation).

59 Ohm & Reid, *supra* note 22, at 1674–75, 1697–98.

60 20 U.S.C. § 1232(g) (2012).

lead role in enforcement of the Health Insurance Portability and Accountability Act (HIPAA),[61] 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,[62] which fall within the general heading of cybersecurity.[63] 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.[64]

Consistent with our 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.

Finally, we note that our focus on consumer-facing privacy obscures the reality that multiple public entities collect information on citizens and residents of the U.S. Although we have already described the FTC as the "closest U.S. equivalent to a national privacy authority," the FTC does not have the statutory authority to oversee the privacy practices of executive branch departments and agencies—and any attempt to give it that power would raise

---

61 42 U.S.C. § 1320d-5 (2018).

62 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)).

63 *See* Patricia Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act,* 84 GEO. WASH. L. REV. 1442, 1443 (2016); *see generally* 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 addressed in *Why Everything is Hackable*, ECONOMIST, Apr. 8, 2017, at 73.

64 For example, DOJ plays a significant role in prosecuting instances of identity theft. *See Combating Identity Theft: A Strategic Plan*, PRESIDENT'S IDENTITY THEFT TASK FORCE 52–71 (2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf [https://perma.cc/WUJ4-WXY6].

serious constitutional issues. Currently, many of these departments—including the Department of Justice and the Department of Homeland Security—have their own privacy offices.[65]

State and Local Governments. State governments are prominent sources of U.S. privacy law.[66] The states typically enforce their own laws through privacy units contained within the office of the state attorney general.[67] Some enforcement functions are performed at the municipal level.[68] In many instances, local police departments are the focal point for reports about identity theft, although they usually lack the authority or information sharing mechanisms to pursue these matters effectively.[69]

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 through

---

65 *See, e.g.*, *Privacy*, DEP'T OF HOMELAND SEC. PRIVACY OFF., https://www.dhs.gov/topic/privacy [https://perma.cc/XR3S-H47M] (last visited Feb. 12, 2019); *Office of Privacy and Civil Liberties*, DEP'T JUST., https://www.justice.gov/opcl [https://perma.cc/5YNH-AQLU] (last visited Feb. 12, 2019).

66 *See generally* Citron, *supra* note 9 (comprehensively examining the framework of state controls).

67 *See generally id*. (describing such mechanisms).

68 *See generally id.*

69 *See, e.g.*, PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 64, at 40–41 (describing measures to enhance cooperation across federal, state, and local law enforcement agencies to share information about instances of identity theft and to facilitate prosecution).

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.

II. U.S. PRIVACY LAW IMPLEMENTATION INSTITUTIONAL DESIGN: SOME BASIC PRINCIPLES

We approach 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.[70]

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.[71]

We note that tensions inevitably arise among these goals. For example, the diversification that can promote useful experimentation and adaptability can come at the cost of system-wide coherence (more regulators taking different approaches to solving the same problem) and greater administrative costs. The purpose of focusing on these criteria is to recognize design tradeoffs and identify areas for possible improvement.

B. Allocation of Regulatory Tasks

Based on our prior work, we offer seven criteria that should guide the assignment of regulatory responsibility to governmental agencies.[72]

Policy Coherence. At the agency level, one must ask whether a 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.[73]

---

70 *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).

71 *See generally* Hyman & Kovacic, *supra* note 6.

72 *See* Hyman & Kovacic, *supra* note 16, at 1468–83.

73 *See id.*

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 to 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.[74] For a single-purpose agency with law enforcement duties, this requires joining up the work of case-handling teams, 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 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,

---

[74] *See, e.g.*, Jennifer Nou, *Intra-Agency Coordination*, 129 HARV. L. REV. 421, 429 (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, 192 (2016).

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.[75] 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 Financial Protection 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.[76] 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—has exposed the new institution to assault in the courts and in Congress about whether it has the necessary degree of accountability.[77]

---

[75] *See* Hyman & Kovacic, *supra* note 16, at 1454–60 (collecting examples of shared policymaking functions).

[76] *See* Arthur E. Wilmarth, *The Financial Service Industry's Misguided Quest to Undermine the Consumer Financial Protection Bureau*, 31 REV. BANKING & FIN. L. 881, 884 (2012).

[77] *See generally* PHH Corp. v. CFPB, 881 F.3d 75 (D.C. Cir. 2018) (en banc). *See also* Hyman & Kovacic, *supra* note 16, at 1504–08.

If political support for an agency is absent entirely, or exists but only on a partisan basis, there will be concrete consequences for the perceived legitimacy of the agency. It is not an accident that President Trump named an individual to head the CFPB (OMB Director Mick Mulvaney) who had previously stated that the agency was a "joke, in a sick, sad kind of way" and had co-sponsored legislation that would have eliminated the CFPB.[78] Nor was it an accident that the CFPB was the only agency in the federal government at which there was a lawsuit over who was actually in charge of the bureau—with the (ultimately unsuccessful) claims to the throne by Leandra English, the just-named Deputy Director of the CFPB, enthusiastically backed by Congressional Democrats, and dismissed or ignored by Republicans.[79]

III. APPLYING OUR CRITERIA: WHO SHOULD DO WHAT?

Any overhaul of substantive privacy policy should be accompanied by a reexamination of the framework of implementing institutions. Even if we do not overhaul substantive privacy policy, it is past time for the institutional arrangements through which privacy policy is developed and administered to be overhauled as well. Measured by the criteria set out in Section III, the U.S. regime for implementing privacy policy has serious weaknesses. Perhaps the most noteworthy weakness 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

---

[78] *See* Abigail Tracy, *What the Hell is Going on at the CFPB?*, VANITY FAIR (Nov. 27, 2017), https://www.vanityfair.com/news/2017/11/donald-trump-mick-mulvaney-consumer-finance-protection-bureau [https://perma.cc/L5FE-3E7F]; Gillian B. White, *The Dismal Future of Trump's Least Favorite Agency*, ATLANTIC (Nov. 17, 2017), https://www.theatlantic.com/business/archive/2017/11/cfpb-mulvaney-trump/546131/ [https://perma.cc/8G57-VWR2].

[79] Tracy, *supra* note 77. *See also* Doyle McManus, *It's High Noon at the CFPB*, L.A. TIMES (Nov. 29, 2017), http://beta.latimes.com/opinion/op-ed/la-oe-mcmanus-cfpb-elizabeth-warren-trump-20171129-story.html [https://perma.cc/6KZ6-2SS2]; Kelsey Tamborrino, *Graham, Durbin Disagree on New CFPB Director*, POLITICO (Nov. 26, 2017), https://www.politico.com/story/2017/11/26/graham-durbin-consumer-protection-agency-259969 [https://perma.cc/L7WF-73VN].

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 for domestic privacy policy also denies the U.S. coherence and credibility in the eyes of its foreign counterparts. In our experience, some foreign privacy regulators downgrade the U.S. privacy 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. Most foreign privacy regulators have doubts about the benefits of simultaneous federal and state-level enforcement in the absence of clearly delegated lines of authority. Simplification of the U.S. privacy regime, anchored by the establishment of a national privacy regulator and clarification of zones of authority among the various regulators, would give the U.S. more influence in global privacy policymaking.[80]

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.[81] For the national privacy authority, we focus on two distinct options. One approach 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.[82] The other approach is to create a new free-standing national privacy agency. We consider each of these strategies in turn.

---

[80] *See* Gellman, *supra* note 9, at 1187 ("[W]ith the international critical mass of data protection agencies that now exists, a country without an agency is at a disadvantage.").

[81] *See* Alejandro E. Camacho & Robert L. Glicksman, *Functional Government in 3-D: A Framework for Evaluating Allocations of Government*, 51 HARV. J. LEGIS. 19, 21 (2014).

[82] *See supra* text accompanying note 8. *See also* Hartzog & Solove, *supra* note 3, at 2294–300; Solove & Hoofnagle, *supra* note 4, at 368–82 (proposing that the FTC, using its existing grants of authority, could expand its role in developing coherent nationwide privacy standards).

A. Enhanced FTC as National Privacy Regulator

Under the first option, Congress would eliminate the FTC's jurisdictional limitations and give it the authority to enforce privacy across the board—including against 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 privacy 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, and the hiring of technology experts to assist in that effort). 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 generally distrust the vesting of privacy powers in an executive 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, we would expect that the host agency would have a mandate that incorporates powers that traditionally have been associated with the FTC's broader consumer protection program.[83]

The FTC's expertise in antitrust should also help it develop and enforce privacy policy. Enforcing antitrust law has given the FTC ongoing involvement in multiple high-tech markets—as well as an understanding of how competition can motivate companies to offer better privacy protections. The FTC's work in both consumer protection and antitrust draws upon a Bureau of Economics with over 80 PhDs in economics.[84] The Bureau of Economics has developed considerable skill in sub-disciplines (including 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

---

[83] 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, 1043 (2014).

[84] *See* Paul A. Pautler, *A History of the FTC's Bureau of Economics* 136 (Am. Antitrust Inst., Working Paper No. 15-03, 2015) (reporting that, as of 2012, the FTC had eighty-two economists with doctorates in economics).

over which it exercises oversight in another domain.[85] Such temptations have been present when the FTC has applied its antitrust powers to review mergers involving companies in the information services sector.[86]

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.

Giving the FTC an expanded privacy role is likely to prompt 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. In the FTC's budget request to Congress for Fiscal Year 2019, the funds proposed for consumer protection (including privacy) functions constituted nearly fifty-four percent of the agency's budget.[87] An expanded privacy role would reduce the overall percentage of resources devoted to antitrust policy still further. Any 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.

Similar questions would arise if Congress dissolved the CFPB and assigned its duties to the FTC. From Fiscal Year 2010 through Fiscal Year 2017, the FTC's headcount ranged between 1132 and 1165; the CFPB's is roughly 1800.[88] Even if the FTC absorbed

---

[85] *See* William E. Kovacic & David A. Hyman, *Regulatory Leveraging: Problem or Solution?*, 23 GEO. MASON L. REV. 1163, 1168 (2016).

[86] *See* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 123 (2015).

[87] *Fiscal Year 2019 Congressional Budget Justification*, 2 FED. TRADE COMM'N (2018), https://www.ftc.gov/reports/fy-2019-congressional-budget-justification [https://perma.cc/BS6F-25JM].

[88] On the FTC's data, see *FTC Appropriation and Full-Time Equivalent (FTE) History*, FED. TRADE COMM'N (2018), https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation [https://perma.cc/73DM-QXM4]. The CFPB's FTE headcount estimate for Fiscal Year 2018 was 1792. *See The CFPB Strategic Plan, Budget, and Performance Plan and Report*, 11–12 CONSUMER FIN. PROT. BUREAU (2017),

only half of the CFPB's 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.

If this path is followed, the long-term result of making the FTC the nation's top privacy cop may transform the agency into a consumer protection/privacy regulator, rather than a consumer protection/antitrust regulator. Reasonable people can disagree on whether that transformation is a net positive development.

From an international relations perspective, an enhanced FTC would be a more effective participant in policy discussions and deliberations on privacy standards. With the jurisdictional loopholes closed, the FTC could properly claim to speak with respect to all matters affecting consumer-facing privacy in the U.S. The FTC's status as an independent agency also gives it sufficient distance from the executive branch—avoiding concerns that would otherwise be inevitable 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 commission, which also might absorb the privacy-related functions of other federal bodies.[89] Compared to a multi-function agency, an independent, privacy-only commission would have internal policy cohesion and greater ability to develop a well-

http://files.consumerfinance.gov/f/documents/201705_cfpb_report_strategic-plan-budget-and-performance-plan_FY2017.pdf [https://perma.cc/HX2T-6W2G].

[89] 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. For an early proposal to create a new free-standing privacy agency, see JAY STANLEY, ACLU, ENFORCING PRIVACY: BUILDING AMERICAN INSTITUTIONS TO PROTECT PRIVACY IN THE FACE OF NEW TECHNOLOGY AND GOVERNMENT POWERS (2009), https://www.aclu.org/files/assets/ACLU_Report_-_Enforcing_Privacy_2009.pdf [https://perma.cc/FP4V-JPC9].

understood policy brand.[90] It would also be less subject to the path-dependent constraints that would inevitably be associated with turning all consumer-facing privacy matters over to an enhanced FTC.

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 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, we 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

---

[90] *But see* Yoon-Ho Alex Lee, *Beyond Agency Core Mission*, 68 ADMIN. L. REV. 551, 593–603 (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").

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

We suggest the adoption of the first approach set out above: the FTC should become the principal U.S. data protection authority for consumer-facing privacy matters. A necessary legislative foundation for this approach would involve (a) eliminating the jurisdictional exclusions from the FTC's mandate, (b) giving the FTC concurrent enforcement authority with respect to all consumer-facing federal statutes, and (c) giving the FTC an express mandate to coordinate national privacy policy.

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.[91] And, as noted previously, our proposal only covers consumer-facing privacy regulation—leaving in place the existing infrastructure for all other matters.

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.[92] We 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 or convergence on shared norms. We propose

---

[91] *See generally* Swire, *Privacy Policy Office*, *supra* note 9.

[92] Citron, *supra* note 9, at 798–803 (discussing the debate over preemption of the states' role in privacy policy). *See generally* Robert A. Mikos, *Making Preemption Less Palatable: State Poison Pill Legislation*, 85 GEO. WASH. L. REV. 1 (2017).

the extension of existing cooperation and coordination efforts through the establishment of a domestic privacy network (DPN)—analogous to the International Competition Network for antitrust enforcers.[93] A DPN will help encourage privacy regulators within the U.S. to converge on superior policy norms.

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 will 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.[94]

From a theoretical perspective, one can improve the institutional framework for U.S. privacy policy either by merger (i.e., by placing all relevant functions within a single institution) or by contract (i.e., by creating and strengthening the ties that allow existing entities to better coordinate their efforts). Our "integration-by-contract" approach involves greater costs of coordination, but it has several major benefits. Most importantly, it avoids the disruption that takes place when responsibilities and personnel are reallocated across agencies. We believe that reorganizations are difficult to justify unless the benefits are compelling. As a practical matter, reorganization proposals also face daunting political headwinds, since they disrupt settled practices and expectations (including the flow of campaign contributions to members of Congress).

CONCLUSION

For nearly two decades, a growing collection of commentators has called for fundamental reform of the U.S. privacy regime.[95] Recent developments—including the implementation of the

---

[93] 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 316–17 (Richard A. Epstein & Michael S. Greve eds., 2004).

[94] *Cf.* 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).

[95] *See supra* note 4, and accompanying text.

GDPR,[96] and disclosures about apparent lapses in data protection by leading information services firms[97]—may be creating a political environment in which Congress undertakes a basic redesign of U.S. privacy law. Concerns about the adequacy of the U.S. privacy system have led the leaders of major American high technology firms to call for adoption of a new omnibus U.S. law that resembles the GDPR.[98]

Should these developments catalyze basic change, improvements in U.S. privacy policy will require as much attention to implementation as it does to the appropriate content of substantive privacy standards. Currently, domestic privacy policymaking and enforcement are fragmented. This state of affairs precludes policy coherence at home and diminishes the influence of the U.S. in international deliberations about global privacy norms.

We offer two options for the development of a next-generation national privacy regulator: the enhancement of the powers and role of the FTC or the creation of a new, independent privacy commission whose core would consist of privacy functions previously performed by the FTC. In addition, we suggest the creation of a policy network that links implementation at the federal and state levels. Although we believe the former solution (enhanced FTC) is better than the latter solution (new privacy regulator), either solution would be an improvement on the status quo.

---

96 *See supra* notes 15–16 and accompanying text.

97 *See, e.g.*, Kadhim Shubber, *Facebook Leak Puts US Regulator's Reputation in Play*, FIN. TIMES (Apr. 3, 2018), https://www.ft.com/content/bcc01464-36c1-11e8-8b98-2f31af407cc8 [https://perma.cc/96GQ-XV25] (discussing revelations suggesting that Facebook may have violated the terms of a data protection settlement reached with the FTC in 2011–2012).

98 *See, e.g.*, *Tim Cook Calls for US Federal Privacy Law to Tackle 'Weaponized' Personal Data*, GUARDIAN (Oct. 24, 2018, 2:24 PM), https://www.theguardian.com/technology/2018/oct/24/tim-cook-us-federal-privacy-law-weaponized-personal-data [https://perma.cc/UD7W-2F3B].