PRIVACY'S CONSTITUTIONAL MOMENT AND THE LIMITS OF DATA PROTECTION

WOODROW HARTZOG
NEIL RICHARDS

PRIVACY'S CONSTITUTIONAL MOMENT AND THE LIMITS OF DATA PROTECTION

WOODROW HARTZOG[*]
NEIL RICHARDS[**]

Abstract: America's privacy bill has come due. Since the dawn of the internet, Congress has repeatedly failed to build a robust identity for American privacy law. But now both California and the European Union have forced Congress's hand by passing the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). These data protection frameworks, structured around principles for fair information processing called the "FIPs," have industry and privacy advocates alike clamoring for a "U.S. GDPR." States seem poised to blanket the country with FIPs-based laws if Congress fails to act. The United States is thus in the midst of a "constitutional moment" for privacy, in which intense public deliberation and action may bring about constitutive and structural change; and the European data protection model of the GDPR is ascendant. In this Article, we highlight the risks of U.S. lawmakers embracing a watered-down version of the European model as American privacy law enters its constitutional moment. European-style data protection rules have undeniable virtues, but they will not be enough. The FIPs assume data processing is always a worthy goal, but even fairly processed data can lead to oppression and abuse. Data protection is also myopic because it ignores how industry's appetite for data is wrecking our environment, our democracy, our attention spans, and our emotional health. Even if European Union-style data protection was sufficient, the United States is too different from Europe to implement and enforce such a framework effectively on its European law terms. Any U.S. GDPR would in practice be what we call a "GDPR-lite." Our argument is simple: in the United States, a data protection model cannot do it all for privacy, though if current trends continue, we will likely entrench it as though it can. Drawing from constitutional theory and the traditions of privacy regulation in the United States, we propose instead a "comprehensive approach" to privacy that is better fo-

[*] Professor of Law and Computer Science, Northeastern University.

[**] Koch Distinguished Professor of Law and Director, Cordell Institute, Washington University.

For helpful comments on prior drafts, the authors would like to thank Jared Bomberg, Jody Blanke, Julie Cohen, Mary Culnan, Nico van Eijk, Sarah Eskens, Robert Gellman, Chris Hoofnagle, Joe Jerome, Pauline Kim, Bill McGeveran, Susan Lyon-Hintze, Mike Hintze, Nicole Ozer, Ira Rubenstein, James Rule, Dan Solove, Olivier Sylvain, Gregory Voss, Ari Waldman, Kurt Wimmer, and Tara Whalen. The authors would also like to thank participants at the 2018 Amsterdam Privacy Conference, the 2019 Privacy Law Scholars Conference at Berkeley Law, and the 2020 Future of Privacy Forum's Privacy Papers for Policy Makers event.

cused on power asymmetries, corporate structures, and a broader vision of human well-being. Settling for an American GDPR-lite would be a tragic ending to a real opportunity to tackle the critical problems of the information age. In this constitutional moment for privacy, we can and should demand more. This Article offers a path forward to do just that.

INTRODUCTION

The General Data Protection Regulation (GDPR) is here, and America now faces an existential choice on privacy. The European Union's (EU) new comprehensive privacy law took effect in May 2018, and it is transforming American privacy law and practice.[1] Some effects of the GDPR were predictable. For example, because the GDPR protects the personal data of Europeans even when that data is processed in the United States, it was bound to affect how large American companies process the data of their European customers and employees. The extensive GDPR requirements have led many global technology companies to comply with GDPR requirements firm-wide, a compliance effect that was also relatively easy to predict.

Some effects of the GDPR were less obvious before the fact. The GDPR is the most prominent example of the governing framework for collecting, storing, and using personal data, commonly referred to as "data protection."[2] Data pro-

[1] *See, e.g.*, Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SECURITY REP. 508, 508 (2008) (noting the global impact of the EU's predecessor to the GDPR); Lillian Edwards, *Data Protection: Enter the General Data Protection Regulation*, *in* LAW, POLICY AND THE INTERNET 77, 77 (Lilian Edwards ed., 2019) (calling the GDPR the most important development in data privacy law's history); Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 75 (2012) (showing the EU's influence on other nations' data privacy laws); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 772–73 (2019) (noting that the new GDPR has caused U.S. corporations to spend billions of dollars on compliance, and that the European framework is making its way into discussions on data privacy throughout the United States); Lee A. Bygrave, *Transatlantic Tensions on Data Privacy* 12 (Transworld, Working Paper No. 19, 2013), http://transworld.iai.it/wp-content/uploads/2013/04/TW_WP_19.pdf [https://perma.cc/CTC8-X9LM] (claiming the "overwhelming bulk of countries that have enacted data privacy laws have followed, to a considerable degree, the EU model"); Ira Rubinstein & Bilyana Petkova, The International Impact of the General Data Protection Regulation 1 (Apr. 23, 2018) (unpublished chapter), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3167389 [https://perma.cc/EC4J-ZJNT] (arguing the GDPR's right to be forgotten, international adequacy standards, and large fines for noncompliant corporations are the most likely provisions to impact nations outside of Europe). *See generally* LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE (2014); Paul de Hert & Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 I/S: J.L. & POL'Y FOR INFO. SOC'Y 271 (2013).

[2] *See* Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65, 67 (2019) ("[T]he GDPR can be seen as a data governance framework. The GDPR encourages companies to think carefully about data and have a plan for the collection, use, and destruction of the data. The GDPR compliance process may cause

tection regimes that follow the GDPR typically follow what Margot Kaminski calls a "binary governance" approach that combines individual due process rights with a collaborative governance approach to follow and protect personal data to ensure it is always processed fairly.[3] Data protection regimes long predate the GDPR, but the GDPR has had the unexpected effect of turning European-style privacy protection into a global market norm, an example of what Anu Bradford has termed the "Brussels Effect," and what Paul Schwartz calls "global data privacy the EU way."[4] If you want to do business in the global data trade, regardless of where you are located, the GDPR sets the tone. Increasingly, this Brussels Effect is also influencing the conceptual design of privacy laws around the globe.

The United States, however, has yet to fully embrace the EU's data protection endeavor. The EU's omnibus approach to data protection is based on individual rights over data, detailed rules, a default prohibition on data processing, and a zealous adherence to the fair information practices (FIPs). In contrast, the patchwork approach of the United States is more permissive, indeterminate, and based upon people's vulnerabilities in their commercial relationship with companies.[5] William McGeveran draws upon these differences to distinguish between Europe's "data protection" and America's "consumer protection" frameworks for privacy. American and European regulators have, more or less, long tried to make the best of such differences.

But change is now on America's doorstep. The modern data industrial complex is facing a tidal wave of public support for a privacy law revolution.[6]

---

some businesses to increase the use of data in their activities, especially if the companies are not data-intensive, but the GDPR causes them to realize the utility of data."); Schwartz, *supra* note 1, at 775 ("'Data protection' is the accepted, standard term applied to Europe's body of law concerning the processing, collection, and transfer of personal data.").

[3] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1552–53 (2019).

[4] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3 (2012); Schwartz, *supra* note 1, at 775; *see* Greenleaf, *supra* note 1, at 75 (illustrating Europe's impacts on non-European data privacy laws); Bygrave, *supra* note 1, at 12 (saying that most of the countries that have promulgated data privacy laws have imitated the European framework); *see also* ASIA-PACIFIC ECON. COOPERATION, APEC PRIVACY FRAMEWORK 3 (2005), https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework [https://perma.cc/K8CK-NHKE] (claiming the APEC framework "is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data"); Anna von Dietze, *Australian Privacy Management Framework Launched*, INT'L ASS'N PRIVACY PROFS. (May 26, 2015), https://iapp.org/news/a/australian-privacy-management-framework-launched [https://perma.cc/3DE8-P4RM] (discussing principles of data protection laws that exist in many different nations). *See generally* BYGRAVE, *supra* note 1; GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (2014); de Hert & Papakonstantinou, *supra* note 1.

[5] WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 257–58 (2016).

[6] *See, e.g.*, Mark Scott, *In 2019, the 'Techlash' Will Go from Strength to Strength*, POLITICO (updated Apr. 19, 2019), https://www.politico.eu/article/tech-predictions-2019-facebook-techclash-

The Financial Times proclaimed that all of 2018 could be summarized by the word "techlash," which they defined as "[t]he growing public animosity towards large Silicon Valley platform technology companies and their Chinese equivalents."[7]

Yet the U.S. Congress has not updated its rules and permissive "notice and choice" approach to privacy in years.[8] Instead, states have taken the mantle and have begun creating their own data protection legislation.[9] At least partially as a result of the Brussels Effect, American state legislatures have started to pass state-level data protection statutes, such as the California Consumer Protection

---

europe-united-states-data-misinformation-fake-news/ [https://perma.cc/E5YS-HNA3] (claiming that public opinion is slowly beginning to turn against large tech companies and Congress is realizing it may need to enact new privacy laws); Matthew Sheffield, *Americans Overwhelmingly Want Congress to Restrict Sharing of Personal Data, Poll Finds*, THE HILL (Dec. 14, 2018), https://thehill.com/hilltv/what-americas-thinking/421384-opting-out-of-data-sharing-is-what-americans-want-most-from-a [https://perma.cc/PT7A-CP5B]. Apple CEO Tim Cook and others have used the term "data industrial complex" to describe the loose net of businesses that profit from data collection and processing or value personal data as a key aspect of their operations and business model. Natasha Lomas, *Apple's Tim Cook Makes Blistering Attack on the 'Data Industrial Complex,'* TECHCRUNCH (Oct. 24, 2018), https://techcrunch.com/2018/10/24/apples-tim-cook-makes-blistering-attack-on-the-data-industrial-complex/ [https://perma.cc/H5WC-HRAF]; *see* Steve Peace, *Data Industrial Complex: We Don't Destroy Our Enemies; We Change Them*, INDEP. VOTER NEWS (Apr. 12, 2018), https://ivn.us/posts/data-industrial-complex-we-dont-destroy-our-enemies-we-change-them [https://perma.cc/78V5-WXGX] (discussing companies like Facebook and Google and how they have been able to profit from user data). Julie Cohen, Ben Hayes, and others have discussed the "surveillance-industrial complex" as "a symbiotic relationship between state surveillance and private-sector producers of surveillance technologies." *See* Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, *in* THE PARTICIPATORY CONDITION IN THE DIGITAL AGE 207, 208 (Darin Barney et al. eds., 2016); Ben Hayes, *The Surveillance-Industrial Complex*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 167, 167 (Kirstie Ball et al. eds., 2012).

[7] Rana Foroohar, *Year in a Word: Techlash*, FIN. TIMES (Dec. 16, 2018), https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e [https://perma.cc/M2LZ-AJRH]; *see also* Ben Zimmer, *'Techlash': Whipping Up Criticism of the Top Tech Companies*, WALL ST. J. (Jan. 10, 2019), https://www.wsj.com/articles/techlash-whipping-up-criticism-of-the-top-tech-companies-11547146279 [https://perma.cc/N8N7-A8JM] (discussing citizen backlash against large technology companies and calls for increased regulation of those companies).

[8] *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016) ("When the FTC first started to regulate privacy in the late 1990s, it adopted a basic notice and choice regime for businesses that was congruous with many of the FIPs."). Under the notice and choice regime, "[a]s long as companies notified people about their information collection, use, and disclosure practices and gave them a choice to opt out (usually by not using the service), then companies were free to act in any way consistent with the notice given to consumers." *Id.* Despite numerous critiques of the limitations of this model, it persists in U.S. privacy law proposals. *Id.* at 444–45.

[9] *See, e.g.*, Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N PRIVACY PROFS. (Apr. 18, 2019), https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/4Y4T-VYTB] (discussing an array of new privacy bills at the state level); *see also* Cameron F. Kerry, *Breaking Down Proposals for Privacy Legislation: How Do They Regulate?*, BROOKINGS (Mar. 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/ [https://perma.cc/U9MR-N6MB] (outlining federal bills).

Act (CCPA).[10] The CCPA applies in California, but because many companies are either headquartered in or do business in Silicon Valley's home state, it will have national consequences when it comes into effect in 2020.[11]

Other states like Washington have also begun to consider their own mini-GDPRs, and after years of opposition to regulation, big tech companies have started to call for a baseline privacy law.[12] These calls are often paired with arguments for federal preemption to avoid multiple state data governance regimes, particularly from more aggressive state regulators.[13] Although preemption advocates often claim that unification will help make U.S. privacy laws adequate in the eyes of the EU, any omnibus bill that is likely to be passed seems destined to be a watered-down version of the GDPR, given the trans-Atlantic differences in rights, cultures, commitments, and regulatory appetites.[14]

Congress now finds itself sandwiched between bottom-up momentum from the states, and top-down influence from emerging international norms and foreign law. At this critical juncture, Congress must now determine the trajectory of U.S. privacy law: To FIPs or not to FIPs? Preemption or federalism? Individual rights, governance obligations, or both? Protecting relationships or data? Europe has already made up its mind.[15] The states have their own ideas.[16] Even if Congress does nothing once again, this convergence of privacy federalism and the Brussels Effect will define America's privacy identity.[17] The GDPR has called the U.S. government's hand.

Privacy law in America thus faces what we might term a "constitutional moment." This is the idea derived from Bruce Ackerman's *We the People* that American constitutional law has been marked by a series of "constitutional mo-

---

[10] Jonathan G. Cedarbaum et al., *Privacy Legislation Continues to Move Forward in Many States*, WILMERHALE (Apr. 30, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20190430-privacy-legislation-continues-to-move-forward-in-many-states [https://perma.cc/Z5V7-RLP7] (surveying state privacy bills modeled after the CCPA); Noordyke, *supra* note 9 (same).

[11] *See* Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/ [https://perma.cc/7A8W-LFRA] (noting the CCPA will affect privacy law around the United States because it applies to companies with California customers, not just those based in California).

[12] *See* Kerry, *supra* note 9 (detailing a baseline privacy bill proposed by Intel Corporation); Noordyke, *supra* note 9 (detailing potential state legislation that share qualities with the GDPR).

[13] *See* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 890–99 (2009) (presenting an argument for when a federal preemptive privacy statute is preferable to conflicting state regimes).

[14] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160–62 (2004) (describing the different cultures of privacy found in the United States and in the EU).

[15] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (providing the new GDPR).

[16] *See* Noordyke, *supra* note 9 (showing proposed state privacy legislation).

[17] *See* Bradford, *supra* note 4, at 3 (noting "Europe's unilateral power to regulate global markets," including in the privacy law context).

ments": periods of constitutional transformation marked by intense public deliberation and participation.[18] In Ackerman's account, most people do not pay much attention to politics or constitutional law most of the time. But every once in a while (such as during the New Deal), "We the People" engage in politics in a way that changes the constitutional arrangements forever. In this Article, we suggest that something analogous is happening in privacy law in the United States—after decades of accommodating the internet and digital technologies into existing and often poorly fitting legal structures, we are on the cusp of a set of legal changes that will structure our emergent digital society for decades to come.[19]

It might seem at this point like there is not much of a decision to be made regarding the identity of U.S. privacy law. Although the GDPR and the states' proposals differ in important ways, each more or less adheres to the FIPs and seeks transparency and accountability from companies and control for data subjects. But the choice is far more profound than that. Lawmakers are facing pressure to fully enshrine the entire European data protection endeavor. Many of the proposals being considered, particularly those that seek to preempt state and other federal laws, zealously adhere to the FIPs. But a data protection identity for U.S. privacy law is not a fait accompli, nor is it the only option. Congress could do something different than bowing to privacy federalism, preemption, or the Brussels Effect. Instead, it could embrace a more holistic and nimble approach to privacy more closely rooted in relationships, power asymmetries, and a broader vision of human well-being.

This Article is about the fundamental dilemma of data protection in the United States, as American privacy law enters its constitutional moment. An EU-style data protection identity for American privacy law might bring interoperability, clarity, and data accountability. But it would entrench a regime designed for a sovereign with a different culture, structure, and commitments. It would also ossify rules based on the phenomenon of personal data that has risks and effects with which we have yet to fully reckon. Even at full strength, the GDPR and the state and sector-specific rules that embrace the FIPs fail to address significant harms that come from industry and governments' bottomless appetite for data. Because data protection regimes focus largely on information and are less sensitive to power disparities within relationships, they also fail to take advantage of critically important and established legal tools and justifications. Finally, data protection regimes seek to permit more ethical surveillance and data processing at the expense of foundational questions about whether that surveil-

[18] *See* 1 BRUCE ACKERMAN, WE THE PEOPLE: FOUNDATIONS 6–7 (1991) (describing "constitutional politics" as a "series of political movements" in which the American people become so heavily engaged in politics that they are able to transform the Constitution).

[19] *See infra* notes 27–136 and accompanying text.

lance and processing should be allowed in the first place. Our argument is simple: in the United States, a data protection approach cannot do it all for privacy, and we are on the precipice of entrenching it as though it can.[20] We can, and we should do better than a watered-down American version of the GDPR, regardless of whether that American version comes from market norms, privacy federalism, or a baseline preemptive federal statute.

We develop our claim in four steps. First, in Part I, we make the case that U.S. privacy law is in the midst of a "constitutional moment"—a period of unusual public engagement likely to result in a significant and durable settlement of the issues.[21] We explore how the Brussels Effect of the GDPR has forced American lawmakers to confront the long-deferred question of the identity of U.S. privacy law. And we show how EU law is substantively and fundamentally shaping U.S. privacy law around the concept of data protection. The GDPR has set global market norms that have created efficiencies for cross-border data flows with some notion of accountability. In our research we interviewed various high-ranking privacy officers at large and small companies, who affirmed that the global data protection movement, led by the GDPR, is driving industry practice and regulatory progress far more than traditional U.S. privacy law. Indeed, the lionizing of the FIPs has fundamentally altered the trajectory of U.S. torts, statutes, contracts, and administrative actions. In this Part we also explore how external pressure from Europe, as well as pressure from the states, has created this constitutional moment for U.S. privacy identity. And we explore the three possible options for U.S. lawmakers: do nothing, enact a preemptive "U.S. GDPR," or embrace what we're calling "the third way"—a more nimble, layered, and inclusive approach that protects personal data but also looks beyond it to account for things that data protection often fails to consider: power, relationships, abusive practices, and data externalities.

In Part II, we explore the compelling virtues of embracing an EU-style data protection identity for U.S. privacy law.[22] Data protection regimes are relatively refined and sturdy. Frameworks like the GDPR are the product of great wisdom, effort, and political compromise, and the substantive FIPs at their core have proven remarkably resilient. Data protection regimes are also formidable and empowering, at least when done properly. The GDPR has thus accomplished something quite difficult—motivating European and American companies to devote significant resources to privacy and creating structures to accommodate data subjects' rights. As a result, data protection could help the United States reclaim some of the moral authority on privacy that it generated in the 1960s and

[20] *See infra* notes 162–255 and accompanying text.
[21] *See infra* notes 27–136 and accompanying text.
[22] *See infra* notes 137–160 and accompanying text.

1970s but has long since abdicated with a self-regulatory approach centered on fictional "notice and choice." Finally, data protection offers conformity and interoperability if the United States assimilates into the global collective. The FIPs are the closest thing to a universal language of privacy.[23] This kind of efficiency is critical for a global data ecosystem.

In Part III, however, we make the case that notwithstanding data protection's virtues, data protection alone is not enough.[24] FIPs regimes conceive of fair data processing as an eternally virtuous goal, which has the consequence of normalizing surveillance, processing, and procedural rules at the cost of more substantive protections. Data protection regimes also fail to account for data externalities such as environmental harm, attention theft, and degradation of social interaction. This is a problem because we are only just beginning to see the human and societal costs associated with the massive scale of data processing and platform dominance. In addition to core privacy-related harms associated with data collection and data use, companies' insatiable hunger for personal information is negatively affecting our attention and how we spend our time, how we become educated and informed citizens, and how we relate to each other. Phenomena like "fake news," "deep fakes," non-consensual pornography and harassment, "sharenting," addiction by design, and lives spent staring blankly and bleakly into our phones are at least partially byproducts of or made worse by the human data industrial complex. This is to say nothing of the toll inflicted on our natural environment. We need broader frameworks for human data not just because it is personal to us, but because the incentive to exploit it creeps into nearly every aspect of our technologically mediated lives.

We also argue that data protection regimes are myopic. The fair information practices are too focused on individuals, control, and consent, and not focused enough on relationships and power. The control and informational self-determination sought by data protection regimes are essentially impossible in constructed environments where choices are constrained, engineered, and overwhelming. When privacy is thought of solely in terms of control over data, regulators risk becoming blind to the other values served by the broader notion of privacy and other mechanisms, such as design, that can be used to corrode people's autonomy. Privacy is about more than atomized decisions. It is about how power is distributed and wielded.[25]

---

[23] Paula Bruening, *Fair Information Practice Principles: A Common Language for Privacy in a Diverse Data Environment*, INTEL (Jan. 28, 2016), http://blogs.intel.com/policy/2016/01/28/blah-2/ [https://perma.cc/XBL5-F9F5].

[24] *See infra* notes 161–256 and accompanying text.

[25] *See, e.g.*, Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY?: WHAT LAW CAN AND SHOULD DO 131, 131–89 (Austin Sarat ed., 2015) (arguing, as the title suggests, that a focus on power is a better way of understanding privacy than consent or harm); Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIR-

We end Part III by observing that a U.S. GDPR is doomed to be watered down and ineffective because, to put it bluntly, the United States is not Europe. Specifically, the GDPR is powered by the fact that, in Europe, both data protection and privacy are treated as separate fundamental human rights. The United States does not have the same deep commitment to data protection, which can lead to diluted rules and placid regulators. The United States also differs regarding its ideological commitment to free expression. Aspects of a fully realized data protection vision, particularly provisions like the right to be forgotten, threaten censorship that is inconsistent with basic premises of the American constitutional order, and arguably with some of the fundamental rights protected by the European constitutional order as well. For these reasons, any version of the GDPR enacted in the United States in the near future is likely to be a "GDPR-lite."

In Part IV, we develop a comprehensive alternative, a "third way" for U.S. privacy that both moves beyond notice and choice and addresses the power dynamics ignored by GDPR-style data protection regimes.[26] First, we argue that U.S. lawmakers should develop their own privacy identity and frameworks built around four major regulatory landscapes: corporate structure and business incentives, power disparities within relationships, data collection and processing risks, and data externalities. If you look closely, the foundation for a pluralistic American theory of privacy based upon constraining corporate power and protecting vulnerable consumers has already been established. We must embrace it. Practically speaking, lawmakers, courts, and companies must embolden the doctrines and legal tools that advance this agenda. This means strengthening trust-based torts like the breach of confidence and theories of indirect liability, prohibiting more data practices outright, and being more skeptical of the role of consent in validating data practices. It also means both governments and organizations must leverage the concept of privacy to further the overall well-being of their citizens and customers.

The other key element in privacy's "third way" is a shift from focusing mainly on procedural rules to include substantive restrictions as well. Procedural requirements like obligations to get peoples' consent for data practices ultimately normalize the kinds of data collection and surveillance harms that they are supposed to mitigate. They are a recipe for companies to exploit and manipulate people in service of ever more data. The substantive shift we call for will require lawmakers to revisit some basic assumptions about when data collection and processing is desirable and entertains bolder obligations, such as outright bans

---

IES L. 1, 22 (2019) (same); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1426 (2001) (discussing privacy as a power struggle between humans and the entities that collect and process their data).

[26] *See infra* notes 257–358 and accompanying text.

and moratoria on certain technologies and practices. It also requires legislatures to be imaginative and go beyond the standard suite of procedural safeguards like transparency and data subject rights like access to data. Lawmakers have been remarkably creative in creating rules for other industries. They should leverage the power to tax, change business incentives, and pierce the corporate veil in going beyond standard data and consumer protection approaches to confront modern privacy risks.

We conclude by noting that if the United States is to take the modern privacy dilemma seriously, lawmakers must act urgently and be willing to expend political capital for effective rules. America's privacy reckoning is here, but its identity has yet to be defined. Congress has an opportunity to show leadership by embracing a comprehensive approach that addresses modern data and privacy problems, not those of the 1970s. But if it fails to embrace a comprehensive framework that addresses corporate power, vulnerabilities in information relationships, and data's externalities, America will be resigned to a weak and myopic approach as its constitutional moment passes. Settling for an American GDPR-lite would be a tragic ending to a real opportunity to tackle the critical problems of the information age.

I. THE PRIVACY BILL FINALLY COMES DUE

American privacy law is weird. Unlike other bodies of U.S. law, such as copyright or securities, American privacy law lacks a comprehensive statute that forms its core. American privacy law is instead a complicated hodge-podge of constitutional law, piecemeal federal statutes, state laws, evidentiary privileges, contract and tort law, and industry guidelines.[27] This weirdness is particularly striking, given that virtually all other industrialized democracies have a comprehensive overarching privacy statute. The European Union, for example, has had such laws since the passage of the EU Data Privacy Directive in 1995.[28] And that regime was recently updated by the comprehensive new GDPR.[29] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) has been in effect since the turn of the century.[30] Japan also recently passed an om-

[27] *See generally* MCGEVERAN, *supra* note 5; ANDREW B. SERWIN, INFORMATION SECURITY & PRIVACY (12th ed. 2018); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (6th ed. 2018).

[28] Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31, 45–46 (EC).

[29] Commission Regulation 2016/679, *supra* note 15.

[30] Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

nibus act for the protection of personal information, leading to a mutual adequacy agreement with the EU allowing data sharing.[31]

No doubt as a result of its weirdness, leading privacy law scholars have begun to document and explain American privacy law's frequently surprising features and sources. This body of work has, for example, shown how the Federal Trade Commission (FTC) operates as a de facto regulator of privacy in the United States,[32] how state attorneys general have played important roles as regulators and norm entrepreneurs,[33] and how privacy lawyers and the designers of technology have attempted (though sometimes failed) to provide "privacy on the ground" where they were not required by law to comply with "privacy on the books."[34]

In recent years, European law has come to have a substantial effect on American privacy law, both on the books as well as on the ground. Before the GDPR, James Whitman argued provocatively that, based on European ideals of dignity and American ideals of freedom, there were two distinct "cultures of privacy."[35] Even if such a distinction were true in the past, America and Europe are converging on a shared culture of data protection—one imposed directly and indirectly and based upon European norms rather than American ones.

This Part explains how Europe's data protection framework has influenced U.S. law to the point that American privacy law is facing its constitutional moment. Our story has three distinct elements. First, we show how the fair information practices, a fifty-year-old set of privacy rules created by the U.S. government, became the foundation of data protection regimes throughout the world.[36] Next we show how Europe's extraterritorial reach, a strong desire for regulatory harmony and global data flows, and a spate of high profile privacy scandals have created an inflection point for U.S. privacy law that is forcing regulators to confront America's privacy identity.[37] We end this Part by taking stock

---

[31] Press Release, European Comm'n, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019), https://europa.eu/rapid/press-release_IP-19-421_en.htm [https://perma.cc/8ZRT-PYNJ].

[32] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 73–80 (2016); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235–36 (2015); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–606 (2014).

[33] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748–51 (2016).

[34] KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 6–8 (2015); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249–51 (2011); Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 661–62 (2018).

[35] Whitman, *supra* note 14, at 1160–62.

[36] *See infra* notes 41–69 and accompanying text.

[37] *See infra* notes 70–111 and accompanying text.

of the three basic options on the table for Congress: (1) continue to do nothing for a "data protection patchwork"; (2) embrace EU-style data protection with preemptive, omnibus legislation; or (3) do something else.[38] In this Part, and in the rest of this Article, we build upon the work of Paul Schwartz and other scholars who have studied Europe's influence on American privacy law and the possibility of preemption to scrutinize the entire endeavor of data protection in the United States.[39]

A. The FIPs and the Birth of Data Protection

The story of data protection rules begins with the advent of computers. Throughout the 1960s and early 1970s, American anxiety about computers, privacy, and "data banks" gripped the public, regulators, and the Supreme Court.[40] Electric and electronic technologies began to transform society, disrupting settled expectations about surveillance, privacy, and government and corporate power. Scholars, popular authors, magazines, and news programs focused on the threats to privacy caused by new eavesdropping technologies and the creation of government and corporate "data banks," trying to understand these changes and calling for legal reform.[41] Courts, too, tried to respond to these new developments, most notably in a series of blockbuster Supreme Court cases holding that the Constitution protected privacy interests in areas as diverse as police wiretapping, political group membership, contraceptives, abortion rights, and the pos-

---

[38] *See infra* notes 113–136 and accompanying text.

[39] *See, e.g.*, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904–05 (2009) (explaining that a "broad coalition" of actors in the United States wants U.S. privacy regulation to align with the European Union's, but arguing against such overarching laws because they would preempt local decision making).

[40] A data bank is a "data repository accessible by local and remote users." Telecomm. Indus. Assoc., *Data Bank*, TELECOM GLOSSARY, https://standards.tiaonline.org/resources/telecom-glossary [https://perma.cc/QW44-A2BT].

[41] *See, e.g.*, MYRON BRENTON, THE PRIVACY INVADERS 85–109 (1964) (discussing telephone wiretapping in the context of monitoring employees and corporate espionage); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 54–89 (1971) (describing massive data collection efforts by the government and the private credit industry); VANCE PACKARD, THE NAKED SOCIETY 29–43 (1964) (decrying new electronic surveillance technologies and memory banks); ALAN F. WESTIN, PRIVACY AND FREEDOM 69–89 (1967) (arguing for the importance of privacy protections against the rise of information collection by governments and corporations); ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY 29–214 (1972) (discussing the creation of databanks by government entities at all levels, business corporations, and nonprofit organizations); Kenneth L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 342–43 (1966) (contending that the rise of computers has made it far quicker and easier to access others' personal data); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (highlighting the development of four types of privacy invasions recognized by tort law). *See generally* Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968); Symposium, *Privacy*, 31 LAW & CONTEMP. PROBS. 251 (1966).

session of obscene pornography.[42] The U.S. Congress reacted to these developments with important privacy legislation, including the Wiretap Act of 1968, which regulated public and private surveillance of telephone conversations.[43]

Perhaps the most important development from this period, however, was not a law but a report issued by a special advisory committee to the Secretary of the U.S. Department of Health, Education and Welfare (HEW) in 1973.[44] Entitled "Records, Computers, and the Rights of Citizens," the report proposed something called "the Fair Information Practices"—a set of "fundamental principles of fair information practice" meant to guide the protection of privacy in record-keeping systems,[45] and possibly influenced by a similar report commissioned by the British government a few years before.[46] As formulated by the HEW Report, the original Fair Information Practices protected a set of six substantive and procedural bedrock principles. First, they included a *prohibition on secret databases* ("There must be no personal data record-keeping systems whose very existence is secret.").[47] Second, they provided for *notice* of record-keeping ("There must be a way for an individual to find out what information about him is in a record and how it is used.").[48] Third, they gave rights to prevent data used for one purpose being used for another without *consent* ("There must be a way for an individual to prevent information about him that was ob-

---

[42] *See generally* Roe v. Wade, 410 U.S. 113 (1973); Stanley v. Georgia, 394 U.S. 557 (1969); Katz v. United States, 389 U.S. 347 (1967); Griswold v. Connecticut, 381 U.S. 479 (1965); NAACP v. Alabama, 357 U.S. 449 (1958).

[43] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. 3, 82 Stat. 197, 211 (1968) (codified as amended in scattered sections of 18 U.S.C. (2018)).

[44] SEC'Y ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEPT. OF HEALTH, EDUC. & WELFARE, DHEW PUBL'N NO. (OS) 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

[45] ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY 2–5 (2019), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf [https://perma.cc/TJ7E-SYLF].

[46] Although the dominant narrative is that the FIPs first appeared in the HEW Report, Chris Hoofnagle has argued that the HEW Report Chairman, Willis Ware, might have been influenced by Britain's Younger Committee for the handling of "information" by computers. Chris Jay Hoofnagle, *Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)*, BERKELEY L. (Jan. 13, 2016), https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/ [https://perma.cc/7Y7P-UZ9J] ("Ware's personal archive includes a memorandum that summarizes the Younger Committee report which was issued in June 1972; Ware appears to have been strongly influenced by it, and by principles underlying of the Freedom of Information Act."); *see* COMM. ON PRIVACY, REPORT OF THE COMMITTEE ON PRIVACY, 1972, HMSO, Cmnd. 5012, at 499 (UK) ("[I]ndividuals should have a legally enforceable right of access to the information held about them by credit rating agencies . . . ."); *see also* Robert Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices*, INST. ELECTRICAL & ELECTRONICS ENGINEERS SECURITY & PRIVACY, July–Aug. 2014, at 51, 52 (suggesting the Ware committee and Younger committee may have influenced each other).

[47] SEC'Y ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., *supra* note 44, at xx.

[48] *Id.*

tained for one purpose from being used or made available for other purposes without his consent.").[49] Fourth, they contemplated rights of *data access and correction* ("There must be a way for an individual to correct or amend a record of identifiable information about him.").[50] Finally, they provided for protections of *data reliability* and against *data misuse* ("Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.").[51]

The Fair Information Practices have been highly influential and are now typically referred to just as the "FIPs." Beginning in the 1970s, the FIPs enshrined in the HEW report spread throughout the world. The Organization for Economic Cooperation and Development (OECD) revised the FIPs in 1980. After that, they became the building blocks for data protection laws around the world.[52] The FIPs did not, however, inspire the first data protection statute—the German Province of Hesse had passed a data protection statute in 1970 that influenced Germany's Federal German Data Protection Act (Bundesdatenschutzgesetz, or BDSG) of 1977, for example.[53] And the global FIPs evolved over time from the 1970s formulation by the United States government. In 2013, the OECD once again revised the FIPs to take into account the extent to which the "profound change of scale in terms of the role of personal data in our economies, societies, and daily lives" has changed the need for the FIPs since the 1970s and 1980s.[54] Nevertheless, the FIPs-based data protection model has been the foundation of a series of data protection laws around the world. For example, they are enshrined in privacy laws as far apart in time and space as Sweden's privacy law of 1973, the EU Data Privacy Directive of 1995, and the new Japanese privacy standards of 2018.[55]

Europe's new GDPR further refines the FIPs model, providing for new data protection rights such as the "right to be forgotten" and the "right to an explana-

---

[49] *Id.*

[50] *Id.*

[51] *Id.* at xxi.

[52] *See* GELLMAN, *supra* note 45, at 1–11 (documenting how the FIPs serve as the basis for many national privacy laws and tracing their development from the HEW committee and through the OECD guidelines).

[53] Schwartz, *supra* note 39, at 908–09.

[54] ORG. FOR ECON. COOPERATION & DEV., THE OECD PRIVACY FRAMEWORK 3 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/RPT3-MPVZ].

[55] *See* GELLMAN, *supra* note 45, at 8–13 (documenting the global influence of the FIPs); Kensaku Takase, *GDPR Matchup: Japan's Act on the Protection of Personal Information*, INT'L ASS'N PRIVACY PROFS. (Aug. 29, 2017), https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/ [https://perma.cc/PJH3-BMYY] (highlighting key provisions of Japan's new privacy law, many of which reflect principles found in the FIPs).

tion."[56] As we explain further below, the GDPR represents the fullest embodiment of the FIPs in a sovereign privacy law, the extraterritorial effect of which is having a substantial regulatory effect in the United States. Today, it is fair to say that the FIPs model of privacy regulation has been adopted by virtually every country in the world that has decided to take data protection seriously. The FIPs have certainly not been without their critics (including the authors of this paper).[57] But for privacy lawyers and scholars around the world, "the FIPs have been with us so long that in many ways they have become synonymous with privacy."[58]

Yet despite their global development and influence, the FIPs and the data protection model of privacy regulation they represent have been far less influential in the United States than in the rest of the developed world. The United

---

[56] Commission Regulation 2016/679, *supra* note 15, at 12, 43–44, 46 (EU). The right to be forgotten gives individuals the right to have their data "erased and no longer processed." *Id.* at 12. The right to an explanation refers to the rights of individuals to receive an explanation of and "meaningful information about the logic involved" in automated decision making. *Id.* at 14, 41–43.

[57] *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341, 341–42 (Jane K. Winn ed., 2006) (characterizing FIPs-based regimes as difficult to enforce and as failures in practice); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1218–19 (2013) (arguing that the updated version of the FIPs "fails to update the definition of personal data," exacerbates the problematic "central role of consent," "remains rooted on a linear approach to [data] processing," and problematically continues to view information as "residing" in a jurisdiction); *see also* DANIEL J. WEITZNER ET AL., MASS. INST. OF TECH., INFORMATION ACCOUNTABILITY 1–2 (2007) (arguing that the current online privacy paradigm is inadequate); Austin, *supra* note 25, at 132–33; Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425, 489 (2011) (noting the FTC's difficulties with enforcing the FIPs); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 499–500 (1995) ("[I]nstead of minimizing the manipulation of citizens and their thinking through unfettered flows of information, the private sector has established a 'smoke screen' that in effect enables subtle, yet significant, manipulation of citizens through hidden control of personal information."). *But see* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 12–17 (defending the FIPs); Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 745 ("I propose an approach to Internet privacy centered around fair information practices (FIPs), which are rules for the fair treatment of personal information."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1670–71 (1999) (praising the FIPs for their flexibility and enforceability); Paula Bruening, *Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy*, INTEL (Oct. 19, 2014), http://blogs.intel.com/policy/2014/10/19/rethink-privacy-2-0-fair-information-practice-principles-common-language-privacy/ [https://perma.cc/8Y5Q-92NZ] (commenting on the FIPs' international acceptance, their ability to "measure compliance," and their enforceability).

[58] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 953 (2017); *see* GREENLEAF, *supra* note 4, at 6–7 (documenting the expansion of FIPs-based privacy laws since Sweden passed the first one in 1973 to today when 101 countries have them). *See generally* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION (2d ed. 2007).

States occasionally flirted with the idea of taking data protection seriously, but it has never fully enshrined the FIPs in a robust, omnibus framework.[59] Paul Schwartz has opined that the best explanations for why the United States and the EU struck different paths with respect to data protection are "(1) initial choices followed by path dependency, and (2) the usefulness of omnibus laws in multination systems that wish to harmonize their regulations."[60] As a result, the United States abdicated the moral authority on privacy and left massive gaps in the U.S. framework, ripe to be filled by others.[61] Specifically, Schwartz focuses on the road not taken by Congress in 1974 with Senate Bill 3418, which would have regulated public and private databases but was eventually scaled back to what we now know as the Privacy Act, which only regulates federal agencies.[62]

To be fair to U.S. policymakers, Congress passed the Fair Credit Reporting Act of 1970 and, following the Richard Nixon surveillance tapes scandal, the Privacy Act of 1974 applied a version of the FIPs to personal data held by the U.S. government.[63] Yet even though the U.S. federal government helped develop

---

[59] *See* GELLMAN, *supra* note 45, at 13 ("The HEW Advisory Committee's recommendation for a federal privacy statute resulted in the first statutory implementation of FIPs anywhere in the world. The Privacy Act of 1974 applies FIPs to federal agencies in the United States. Massachusetts enacted a Fair Information Practices chapter to its general laws in 1975. Minnesota enacted a Minnesota Government Data Practices Act implementing fair information practices in 1974. It was not until 2002 that the U.S. Congress first formally referenced FIPs in a statute. In establishing a privacy office at the Department of Homeland Security, the Congress assigned the office responsibility for 'assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974.'" (footnotes omitted)).

[60] Schwartz, *supra* note 39, at 912.

[61] *See id.* (stating that while the United States has continued to lack an omnibus privacy law bill, European nations have developed their own omnibus frameworks and then built law off of those foundations).

[62] *See id.* at 911 (discussing the proposed Senate bill). Schwartz wrote:

> S. 3418 would have required public and private entities to "collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization." . . . The bill would also have required organizations to "maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject"—a data quality requirement. As a final example, the bill would have placed restrictions on onward transfers. . . . In other words, the organization transferring personal data would be obliged to determine that the entity receiving the information followed FIPs, including drawing a line against further transfers.
>
> From a contemporary perspective, one of the most interesting aspects of the proposed bill from 1974 is that it would have conditioned international transfers of information on either subject consent or equivalent protections abroad for the personal data. This proposed requirement of "equivalency" would have exceeded the protections later found in the European Data Protection Directive . . . .

Id. (footnotes omitted) (quoting S. 3418, 93d Cong. § 201(a)(1), (a)(4) (1974)).

[63] Privacy Act of 1974, 5 U.S.C. § 552a (2018); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2018); *see* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Con-*

the first version of the FIPs, it has never fully applied them to the data in its control or in interstate commerce over which it possesses regulatory power under the Constitution. As Robert Gellman put the point succinctly in 2017, before the effective date of the GDPR, "[i]n the United States, occasional laws require some elements of FIPs for specific classes of record keepers or categories of records. Otherwise, private sector compliance with FIPs' principles, while increasing, is mostly voluntary and sporadic."[64] Despite the introduction of countless pieces of proposed legislation, Congress has failed since the mid-1990s to pass a law governing the personal information traded in internet-based commerce, much less a commercial privacy law of general applicability.[65] Outside of the few sectoral federal FIPs-based laws such as the Health Insurance Portability and Accountability Act (HIPAA) (health privacy), Family Educational Rights and Privacy Act (FERPA) (educational records), and the Fair Credit Reporting Act (FCRA) (credit reports), federal privacy law in the United States often requires little more than (1) not engaging in unfair or deceptive trade practices as defined by the FTC; (2) not causing substantial harm to consumers; and (3) following a very thin version of the FIPs known as "notice and choice."[66] As we have argued elsewhere, under this permissive version of the Fair Information Principles, "notice" often means little more than burying data practices in the fine print of a dense privacy policy, while "choice" means choosing to use a service with its non-negotiable data practices as a take-it-or-leave-it option.[67] Indeed, even though the FTC has become the default privacy regulator in the United States, during the critical period of internet development in the late 1990s and early 2000s, the FTC adhered to this thin version of the FIPs, a fact that the FTC appeared to concede in a preliminary 2010 report.[68] Still, this concession was not present in its final issued report.[69]

---

stitution, 86 MINN. L. REV. 1137, 1164–69 (2002) (noting the timing of the Privacy Act's passage and how the FIPs made their way into the legislation).

[64] GELLMAN, *supra* note 45, at 22–23 (citations omitted).

[65] Robert Gellman, *The Long and Difficult Road to a U.S. Privacy Law: Part 1*, INT'L ASS'N PRIVACY PROFS. (Aug. 3, 2018), https://iapp.org/news/a/the-long-and-difficult-road-to-a-u-s-privacy-law-part-1/ [https://perma.cc/5Z3H-JNZR] (discussing failed attempts at a comprehensive commercial privacy law and describing how only a hodgepodge of narrower privacy laws currently exist).

[66] *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT 15 (2018) (describing most privacy laws today as having three basic commands: "follow the Fair Information Practices, do not lie, and do not harm"); *see also* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1899–1900 (2019) (highlighting other sectoral federal laws, including the Children's Online Privacy Protection Rule, the Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and others).

[67] Richards & Hartzog, *supra* note 8, at 434; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019).

[68] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 8–10 (2010) (acknowledging that in

This, then, is the cruel irony of the FIPs: the most generally accepted mechanism for regulating and protecting personal data in the world was significantly developed by the U.S. government, but the FIPs have been more influential outside the United States than inside its borders. The U.S. government sketched the blueprint for our international privacy regime, but then failed to build the structure it had planned. That structure has been built, but it has been built by others. And in the United States, just a thin remnant of the FIPs remains as a minimal basis for general commercial privacy protection.

B. The Internal and External Pressures for Action

Congress, it seems, is finally feeling the heat to act decisively on privacy.[70] In any given day in 2019, if you tuned into the news, you were likely to come across a story about a congressional privacy hearing, a new privacy failure demonstrating the ineffectiveness of our rules, or even industry asking to be regulated in the style of the EU.[71] From 2018 to 2019 alone, a series of privacy bills were introduced into Congress, and more are on the way.[72] In this Part, we describe how Congress is facing two separate pressures for action on privacy. First, there is an external pressure from the EU and all similarly styled data protection regimes around the world, and second, an internal pressure from the states, industry, privacy advocates, and the voting populace.

As noted above, the FIPs have had a profound influence around the world, particularly in Europe. These guidelines were highly influential in Europe's first major attempt at a data protection framework, which began the export of EU

---

the early 2000s, the FTC had to shift from its notice-and-choice FIPs approach and develop a more harm-based approach).

[69] *See* GELLMAN, *supra* note 45, at 23–24 (documenting the FTC's inconsistent track record with the FIPs).

[70] *See* Cameron F. Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation?*, BROOKINGS (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/ [https://perma.cc/YH37-B6PH] (discussing stakeholder engagement with Congress on issues of privacy and major events—such as the Cambridge Analytica scandal—that have placed privacy on Congress's radar).

[71] *See* Kerry, *supra* note 9 (discussing Senate privacy hearings, draft privacy legislation from corporations such as Intel, and flaws in the current U.S. privacy law framework).

[72] *See* Jeffrey Atteberry, *A Survey of Proposed Federal Privacy Legislation and the Year Ahead*, LAW.COM (Feb. 4, 2019), https://www.law.com/corpcounsel/2019/02/04/a-survey-of-proposed-federal-privacy-legislation-and-the-year-ahead/?slreturn=20190402095708 [https://perma.cc/H5UY-6K9Z] (detailing a slew of congressional privacy proposals from 2018); Jerry Barbanel, *A Look at the Proposed Algorithmic Accountability Act of 2019*, INT'L ASS'N PRIVACY PROFS. (Apr. 29, 2019), https://iapp.org/news/a/a-look-at-the-proposed-algorithmic-accountability-act-of-2019/ [https://perma.cc/J87Y-Z4XS]; Taylor Hatmaker, *Proposed Bill Would Forbid Big Tech Platforms from Using Dark Pattern Design*, TECHCRUNCH (Apr. 9, 2019), https://techcrunch.com/2019/04/09/dark-pattern-bill-senate-warner-detour/ [https://perma.cc/TN3U-KNP6] (highlighting the introduction of the Deceptive Experiences to Online Users Reduction (DETOUR) Act in 2019).

privacy norms across the world. In 1995, the EU adopted "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[73] Perhaps the most important law in the global spread of privacy norms, the European Union's Data Protection Directive ("Directive") made FIPs the governing legal standard for all data in the European Union and required each member state to enact a national law based on the FIPs for virtually all personal information in Europe.[74]

The Directive applied from 1998 until it was superseded by the similar but more robust GDPR in 2018. The Directive sought to operationalize Article 8 of the Charter of Fundamental Rights of the European Union, which provides that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
3. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
4. Compliance with these rules shall be subject to control by an independent authority.[75]

To accomplish this goal, the Directive laid out prescriptive rules regarding the processing—including collection, storage, use, and disclosure—of all personal data.[76] The EU enacted the Directive in large part to harmonize its member states' laws to permit the free transfer of personal data among member states while also ensuring that each member state protected that data at similar levels.

The first hint of Europe's intentions to apply its data protection regime extraterritorially can be found in its refusal to allow data to be exported and processed to places that did not offer the level of protection offered in Europe. The Directive generally prohibited the export of personal information outside the EU, subject to a series of exceptions, the most important of which is where the non-EU country had been determined to ensure an "adequate level of protection."[77]

---

[73] Council Directive 95/46, *supra* note 28.

[74] *See* GELLMAN, *supra* note 45, at 13 (claiming the Directive promoted the dispersion of FIPs all over Europe).

[75] Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border E.U.-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227, 231–32 (2013); *see* Charter of Fundamental Rights of the European Union 2012/C 326/02, art. 8, 2012 O.J. (C 326) 391, 397 (EU), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN [https://perma.cc/T35A-3NY9].

[76] Council Directive 95/46, *supra* note 28, at 38.

[77] *Id.* at 45–46.

This framework caused a number of countries outside the EU to directly adopt the FIPs that lie at the foundation of the Directive.[78]

The U.S. Congress, of course, refused to pass any general data protection law, whether in the style of the FIPs or otherwise. But there remained a vital commercial pressure to allow EU data into the United States for processing. Articles 25 and 26 of the Directive required that the personal data of Europeans could not be sent to foreign countries (like the United States), unless that country ensured an "adequate level of data protection," or the transaction satisfied another exception to the rule.[79] Because there was no general privacy law on par with the Directive in the United States, there was little to no chance that European regulators would declare U.S. law "adequate." This rule was a huge problem for American tech companies like Google who wanted to process Europeans' data (for example to deliver email, generate personalized web search results, or provide mapping services) in the United States (where their servers were). It was also a problem for traditional multinationals headquartered in the United States who wished to continue processing the human resources data of their foreign employees at their head offices. To resolve this problem, the EU and U.S. governments negotiated the "Safe Harbor Agreement" of 2000.[80] Under the "Safe Harbor," a U.S. company wishing to import European personal data merely had to self-certify to the Department of Commerce that it had complied with the seven FIPs principles considered to represent the essence of the Directive's "adequacy" requirement: essentially a modified version of the FIPs.[81] They required the companies to process the data of Europeans with (1) notice; (2) choice; (3) compliance with the Safe Harbor Principles for any onward transfer of data to other entities; (4) data security; (5) data integrity, meaning that the data must be relevant and reliable for the purposes it was collected for; (6) access to individuals of their data; and (7) effective enforcement of these promises.[82] In practice, this meant that (at least for data about Europeans) the United States companies agreed to abide by the fundamental requirements of European data protection law.[83] Violations of certifications were policed by the FTC under its unfair and deceptive trade practice authority.[84] The entire system, under which hundreds of

---

[78] GELLMAN, *supra* note 45, at 13; *see, e.g.*, Schwartz, *supra* note 39, at 933 (claiming that Canada's new data privacy law was partly motivated by the EU's "adequacy" requirement).

[79] Council Directive 95/46, *supra* note 28, at 45–46.

[80] Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7 (EC).

[81] *Id.* at 15.

[82] *Id.* at 11–12.

[83] *See Federal Trade Commission Enforcement of the U.S.-E.U. and U.S.-Swiss Safe Harbor Frameworks*, FED. TRADE COMMISSION (Dec. 2012), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor [https://perma.cc/3GY7-HDCH].

[84] Commission Decision 2000/520/EC, *supra* note 80, at 7.

U.S. companies had to declare that they were complying with the essence of European law, had a significant effect on "privacy on the ground" at U.S. companies.[85] In many instances, the emerging cadre of privacy professionals in the United States who facilitated the compliance regime sought to build the requirements of EU law into the internal governance structures of their own, American-based companies.[86]

Elements of these cross-border rules became encoded into United States domestic law. For example, because both the Safe Harbor and Privacy Shield were explicitly enforceable against participating U.S. companies by the FTC, the requirements of the EU's FIPs became enforceable under U.S. privacy law. Thus, when Google launched its ill-fated Buzz social network by signing up Gmail users automatically and without their consent, the FTC charged Google with violating not only the FTC's statutory authority over deceptive trade practices, but also for violating the Safe Harbor, of which Google was a participant.[87] Google settled the case, agreeing to a 2011 consent decree with the United States government that continues to bind it to both U.S. and EU privacy principles to this day.[88] In this way, FTC jurisdiction was asserted to enforce the violation of a foreign legal standard, and to extend the scope of that standard going forward. Similarly, some companies chose to satisfy the requirements of Article 25 by enacting standard EU-approved contracts or more stringent "binding corporate rules" whose terms required that data sent to the United States for processing would be handled according to the Directive and then the GDPR.[89] In these additional ways, substantive EU privacy law came to have direct application in the U.S.

But European data protection norms were not finished with the United States. In the now-famous 2015 case *Schrems v. Data Protection Commission*,

---

[85] *See, e.g.*, Bamberger & Mulligan, *supra* note 34, at 261–62 (chronicling the creation of the role of corporate chief privacy officer (CPO) as one privacy change "on the ground," and how "companies' motivations for creating CPO positions" included "smoothing interactions with European regulators under the Safe Harbor Agreement").

[86] *See id.* at 295 (explaining how the emergence of the FTC and rise of privacy professionals within U.S. companies have increased corporate focus on privacy for customers); *see also* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 784–85 (2020) (noting the creation of internal privacy policies by company employees).

[87] *See* Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz [https://perma.cc/C52P-SA95] (discussing the "U.S.-E.U. Safe Harbor," problems with Google's Buzz project, and the resulting consent agreement between Google and the FTC).

[88] *Id.*

[89] *See* Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH., no. 1, 2018, at 101–03 (discussing "model contract clauses" and "binding corporate rules" as alternative ways of meeting the EU's adequacy standards).

the Court of Justice for the European Union (CJEU) invalidated the Safe Harbor Agreement because it did not conform with the Data Protection Directive in light of the Charter of Fundamental Human Rights, particularly given the allegations by Edward Snowden about the National Security Agency's access to personal data held by U.S. tech companies.[90] The Safe Harbor was replaced by a second, allegedly stronger FIPs-based certification regime known as the "Privacy Shield," whose legal future remains uncertain and dependent on the outcome of another ruling by the CJEU.[91]

In addition to the external Brussels Effect of EU privacy imperialism, U.S. law at the national level is being affected by an internal force of state privacy regulation. State governments have of course regulated privacy for many years, whether through common law, statutory or state constitutional law rules, or the regulatory entrepreneurship of state attorneys general.[92] But there is a new trend in state privacy regulation occasioned by our great privacy awakening of 2018. Tech companies have been approaching a privacy reckoning for years, driven on by data breaches, the Snowden revelations, and untrustworthy data practices in general. But the final straw appears to be the debacle involving Facebook and the disgraced data firm Cambridge Analytica, which illicitly gathered personal data on millions of American Facebook users to be deployed for manipulation of their votes and other electoral meddling.[93] This is to say nothing of the ceaseless run of stories about a high-profile data breach or concern about a "creepy" new technology or data practice. The cumulative effect is that people have grown wearier and more skeptical of digital tech, and social media in particular. John Gramlich of the Pew Research Center wrote:

> A little over half of adult Facebook users in the U.S. (54%) have adjusted their privacy settings in the past 12 months, according to a separate Center survey conducted in May-June 2018. The survey followed revelations that former consulting firm Cambridge Analytica

---

[90] Case C-362/14, Schrems v. Data Prot. Comm'n, 2015 E.C.R. I-650 ¶¶ 30, 104–06.

[91] *See* Case C-311/18, Data Prot. Comm'n v. Facebook Ire. Ltd. & Schrems, 2019 EUR-Lex CELEX LEXIS 1145 ¶¶ 33–38 (Dec. 19, 2019); *The Schrems Saga Continues: Schrems II Case Heard Before the CJEU*, HUNTON ANDREWS KURTH (July 10, 2019), https://www.huntonprivacyblog.com/2019/07/10/the-schrems-saga-continues-schrems-ii-case-heard-before-the-cjeu/ [https://perma.cc/CBX5-6RLL] (detailing the facts of the case that will decide the validity of the "Privacy Shield"). In full disclosure, one of the authors of this paper (Richards) served as an independent expert in this case retained by the Irish Data Protection Commissioner.

[92] *See, e.g.*, Citron, *supra* note 33, at 748–49 (discussing the efforts of state attorneys general to regulate privacy); Solove & Hartzog, *supra* note 32, at 587 (mentioning state constitutions and statutes as well as state tort law).

[93] *See* Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, WIRED (Mar. 17, 2019), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ [https://perma.cc/52CH-836M] (detailing the Cambridge Analytica scandal and how it is now spurring state and federal regulation).

> had collected data on tens of millions of Facebook users without their knowledge or permission.
>
> About four-in-ten adult Facebook users (42%) have taken a break from checking the platform for several weeks or more, and about a quarter (26%) have deleted the app from their phone at some point in the past year. Combined, 74% of adult Facebook users say they have taken at least one of these three actions.[94]

Even though Congress has yet to meaningfully act on the public's general unease with personal data and surveillance ecosystems, states, particularly California, have taken up the banner.[95] This is the other major pressure on Congress in addition to the Brussels Effect. State governments have started to impose privacy regulations with national effects from the bottom up.[96]

Apparently, the rising tide of states' privacy efforts started with a casual conversation over dinner.[97] Alastair Mactaggart, a successful California real estate developer and investor, had some friends over for the evening, including a software developer at Google.[98] Nicholas Confessore of *The New York Times* wrote:

> As evening settled in, Mactaggart asked his friend, half-seriously, if he should be worried about everything Google knew about him. "I expected one of those answers you get from airline pilots about plane crashes," Mactaggart recalled recently. "You know—'Oh, there's nothing to worry about.'" Instead, his friend told him there was plenty

---

[94] John Gramlich, *10 Facts About Americans and Facebook*, PEW RES. CTR. (May 16, 2019), https://www.pewresearch.org/fact-tank/2019/02/01/facts-about-americans-and-facebook [https://perma.cc/XFP3-RHDQ]; *see* Andrew Perrin, *Americans Are Changing Their Relationship with Facebook*, PEW RES. CTR. (Sept. 5, 2018), https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook [https://perma.cc/WNU2-RKU4] (providing the same data and a similar quote); *One Year After Cambridge Analytica, Survey Reveals Strong Consumer Privacy Fears Remain*, SLICKTEXT (2019), https://www.slicktext.com/blog/2019/02/survey-consumer-privacy-fears-after-cambridge-analytica [https://perma.cc/3TPY-E57W] (summarizing survey results following the Cambridge Analytica scandal indicating that most consumers are worried about how large companies use their data).

[95] Low income populations in particular generally express greater concern about industry and government surveillance and data practices. JOSEPH TUROW ET AL., UNIV. PA., DIVIDED WE FEEL: PARTISAN POLITICS DRIVE AMERICANS' EMOTIONS REGARDING SURVEILLANCE OF LOW-INCOME POPULATIONS 6–7 (2018), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1563&context=asc_papers [https://perma.cc/69KN-BT35].

[96] *See* Mathews & Bowman, *supra* note 11 (showing the CCPA's potential to have effects outside of California).

[97] Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/7VTK-4D59].

[98] *Id.*

> to worry about. If people really knew what we had on them, the Google engineer said, they would flip out.[99]

Mactaggart subsequently became passionate about improving California's privacy rules and devoted time and resources to getting a privacy initiative put forth as a ballot measure for California voters that ultimately met the requirements for a vote.[100] He devoted substantial resources to the initiative, and Californians were open to legal reform in the wake of the Cambridge Analytica scandal.[101] After working with industry and government, Mactaggart agreed to withdraw the measure if California passed and signed similarly effective legislation. The result is the California Consumer Privacy Act of 2018 (CCPA).[102]

The CCPA in its current form has many similarities with the GDPR, but it would be inaccurate to call it merely a GDPR clone.[103] Kristen Mathews and Courtney Bowman have described the act as revolving around four basic rights for Californians involving their personal information:

1. the right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
2. the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent's, opt-in);
3. the right to have a business delete their personal information, with some exceptions; and
4. the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.[104]

Although the CCPA certainly obligates businesses, it is relatively limited in scope compared to the GDPR.[105] It largely targets third-party advertisers and

---

[99] *Id.*

[100] *Id.*

[101] *Id.* ("[I]t was suddenly easy to get people to sign the ballot petition. After the Cambridge Analytica scandal, all we had to say was 'data privacy,' [Rick Arney, who helped draft the measure,] told me.") (internal quotations omitted).

[102] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2020).

[103] *See, e.g.*, Anupam Chander et al., *Catalyzing Privacy Law*, MINN. L. REV. (forthcoming 2020), SCHOLARSHIP @ GEO. L. 4 (Feb. 6, 2020), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3208&context=facpub [https://perma.cc/92CQ-N3PD] (arguing, upon a close look at both laws, that the CCPA and GDPR differ in significant ways).

[104] Mathews & Bowman, *supra* note 11.

[105] *Id.*

other data brokers and imposes some but not all of the traditional "data subject rights" outlined in FIPs-based regimes like the GDPR.[106] Although the act purportedly aimed to move away from the dominant U.S. "notice and choice" model, the rights granted to Californians still center around industry transparency and individual notions of consent, control, and choice.[107] The act does not change the default status of data processing in California, nor does it tackle thorny data practices beyond sales, such as algorithmic accountability.[108] But the act is certain to have a national effect because many technology companies covered by the act are either headquartered in or do business in California and thus fall within its scope.[109] Following the CCPA, at least eighteen states have passed or introduced similarly styled data protection bills.[110] Although not all of these bills will be successful, it seems as though this trend will continue, particularly as the CCPA itself becomes refined and entrenched.[111]

C. Data Protection Three Ways

Given pressures from Europe, the states, the tech industry, and the American public, what options does Congress now have? The way we see it, Congress can react to this constitutional moment in three general ways: do nothing, attempt a national data protection law, or attempt a more creative third way for privacy.[112]

Option one would thus be to do nothing, a regulatory skill that Congress has been honing for decades. But even if Congress does nothing on privacy, America's privacy identity is about to be set regardless of whether Congress acts.[113] This is because many states seem keen to pursue FIPs-style data protection regimes as long as Congress remains inert.[114] The CCPA has energized state legislatures across the United States.[115] As other states introduce privacy legisla-

---

[106] *See id.* (focusing on the act's provisions regarding selling data to third parties and noting that the GDPR contains more rights for data subjects).

[107] *See* Chander et al., *supra* note 103, at 20 (arguing that the CCPA still focuses on transparency rather than adopting the more substantive requirements that the GDPR has imposed).

[108] *See id.* at 19–21 (noting the CCPA's permissive stance toward data processing and arguing that it takes a less holistic regulatory approach than the GDPR does, including on the issue of algorithmic accountability).

[109] *See* Mathews & Bowman, *supra* note 11 (discussing the CCPA's broad impact because it applies to all companies with California customers, regardless of whether or not they are based there).

[110] Noordyke, *supra* note 9.

[111] *See id.* (updating over time as additional states propose bills similar to the CCPA).

[112] *See infra* notes 113–136 and accompanying text.

[113] *See* Bradford, *supra* note 4, at 3 (arguing that the EU has the ability to set global market rules regarding privacy).

[114] *See* Noordyke, *supra* note 9 (claiming the appetite for comprehensive state privacy laws to protect consumers has reached a high point, with many proposed bills containing the FIPs).

[115] *Id.*

tion, they are likely to seek at least some kind of conformity with it, as creating conflicting state privacy rules is more likely to cause Congress to pass a national law that preempts state law.[116] So even the first and easiest option for Congress, doing nothing, will mean an inevitable march toward transparency, consent, and control mandated from the outside by the increasing creep of the GDPR and from the inside by state laws with national effect. If Congress does not act, states are likely to follow the CCPA's lead and pass mini-GDPRs at the state level.[117] Mitchell Noordyke recently analyzed twenty-four of the most recent state privacy bills (or enacted laws).[118] He found sixteen common privacy provisions, all of which are based on the FIPs and reflected EU-style data protection regimes.[119] These include data subject rights of access, rights against solely automated decision making, rights to rectification, deletion, data portability, restriction of processing, and a right to opt out of the sale of personal information.[120] These bills and laws also commonly include standard GDPR-like business obligations, such as notice and transparency requirements, data breach notifications, mandated risk assessments, purpose and processing limitations, and prohibitions on discrimination against a consumer for exercising a right.[121] So if Congress does nothing, we will likely get a flood of state mini-GDPRs.

Option number two would be to pursue a U.S. GDPR. In its fullest form, this approach would entail an omnibus data protection law that would entrench the FIPs as the dominant identity for American privacy law. This is certainly a popular option. Federal and state law and policymakers have argued in favor of a U.S. version of the GDPR.[122] So have privacy advocates and the press.[123] Even large, powerful tech companies like Apple, Cisco, Facebook, and Brave have requested to be regulated by a U.S. version of the GDPR.[124] Many of the bills

---

[116] *See* Chander et al., *supra* note 103, at 41–43 (putting forth theories as to why state legislatures are following California's example on privacy regulation).

[117] *See* Noordyke, *supra* note 9 (documenting the introduction of many state bills similar to the CCPA after its passage).

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *See* Savia Lobo, *GAO Recommends for a U.S. Version of the GDPR Privacy Laws*, PACKT (Feb. 18, 2019), https://hub.packtpub.com/gao-recommends-for-a-us-version-of-the-gdpr-privacy-laws/ [https://perma.cc/E6JP-7U59]; Casey Newton, *Congress Just Showed Us What Comprehensive Regulation of Facebook Would Look Like*, THE VERGE (July 31, 2018), https://www.theverge.com/2018/7/31/17632858/facebook-regulation-mark-warner-policy-paper-congress [https://perma.cc/4D5Y-Q6Q4] (detailing a U.S. Senator's call for a U.S. version of the GDPR).

[123] *See* Editorial, *Facebook Is Not the Problem. Lax Privacy Rules Are.*, N.Y. TIMES (Apr. 1, 2018), https://www.nytimes.com/2018/04/01/opinion/facebook-lax-privacy-rules.html [https://perma.cc/ZR6F-4G44] (calling for GDPR-like rules to be established in the United States).

[124] Ellen Daniel, *Could the US Adopt Its Own Version of GDPR?*, THE VERDICT (Jan. 3, 2019), https://www.verdict.co.uk/us-gdpr-laws-facebook/ [https://perma.cc/8GMZ-66EQ]; Johnny Ryan, *Bren-*

and frameworks proposed in the past few years by lawmakers, industry, and civil society seem to mimic aspects of the GDPR.[125] For example, most of these proposals involve some combination of transparency, choice, and consent obligations with purpose limitations and data subject rights.

But as we will explore in Part III, it is not as though the United States will be able to simply cut and paste the GDPR into a bill.[126] The question here is what a U.S. version of an omnibus data protection law would likely turn out to be as enacted. There are reasons to be concerned, and it is likely that any U.S. version of the GDPR would be significantly weaker than its European counterpart. Any movement towards a preemptive national omnibus bill is likely to be seen as an opportunity for industry to lower the floor of privacy protections by watering down key provisions. Alvaro Bedoya, formerly chief counsel to the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, noted:

> [L]obbyists paid by Facebook are working with Illinois lawmakers backed by Facebook to gut the state's face recognition privacy law, the strongest in the nation.
>
> This should make us very skeptical about any calls for a broad, European-style privacy law that would apply across technologies and platforms. We cannot underestimate the tech sector's power in Congress and in state legislatures. If the United States tries to pass broad rules for personal data, that effort may well be co-opted by Silicon Valley, and we'll miss our best shot at meaningful privacy protections.[127]

---

dan Eich Writes to the US Senate: We Need a GDPR for the United States, BRAVE (Oct. 1, 2018), https://brave.com/us-gdpr-senate/ [https://perma.cc/7YZR-RU7C]; Andreas Sandre, *Mark Zuckerberg and Europe's GDPR*, HACKER NOON (Apr. 11, 2018), https://hackernoon.com/mark-zuckerberg-and-europes-gdpr-9b76adebf8bd [https://perma.cc/V5WM-NLP4]; Elena Souris & Hollie Russon Gilman, *Data Rights Are Civic Rights: A Participatory Framework for GDPR in the US?*, VOX (Apr. 12, 2018), https://www.vox.com/polyarchy/2018/4/12/17229354/data-rights-civic-rights-gdpr [https://perma.cc/WWW6-XUYE]; Mark Wyciślik-Wilson, *Cisco Joins Apple in Calling for a US Version of GDPR Data Protection and Privacy Laws*, BETANEWS (Feb. 4, 2019), https://betanews.com/2019/02/04/cisco-us-gdpr/ [https://perma.cc/5JQJ-4B5M].

[125] *See* Kerry, *supra* note 9 (highlighting recent draft legislation proposed by many different actors, some of which shares key characteristics with the GDPR).

[126] *See infra* notes 161–256 and accompanying text.

[127] Alvaro M. Bedoya, *Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html [https://perma.cc/B63N-7DAK]; *see also* Louise Matsakis, *As Zuckerberg Smiles to Congress, Facebook Fights State Privacy Laws*, WIRED (Apr. 12, 2018), https://www.wired.com/story/despite-zuckerberg-pledge-facebook-fights-state-privacy-laws/ [https://perma.cc/4AHQ-8GTY] (explaining Facebook and other large technology companies' extensive lobbying and campaign donation efforts to weaken state privacy laws).

Cameron Kerry, who led the Obama administration's drafting of legislation based on its Consumer Privacy Bill of Rights, lamented how after he left the government, "draft Obama administration legislation was diluted in an unsuccessful effort to broaden business support, lost civil society support in the process, and so fell flat when it was released publicly."[128] The dilution of privacy laws in the U.S. political process has a long history, including the rejection of an omnibus FIPs-based bill in 1974 when the Privacy Act was limited to federal databases and not the privacy sector, and the repeated failure by two decades of Congresses to pass a general internet privacy bill despite dozens of opportunities to do so.[129] Indeed, at the time of writing, there are similar efforts afoot in California to water down the CCPA through legislative amendment.[130]

In other words, given different systems, value commitments, and political realities, it seems likely that any version of a U.S. GDPR will, in effect, be a GDPR-lite. Although preemptive federal legislation could, in theory, be more robust than state laws, it would be a risky proposition.[131] Therefore, in this paper, our criticisms of data protection are largely based on what form we believe such a regime would take in the United States. We do not specifically take issue in this Article with Europe's commitment to privacy or data protection except insofar as we argue that all FIPs-based regimes have built-in limitations.

The third option, an inclusive and layered privacy law that goes beyond the FIPs, is going to require two key things: imagination and forbearance. First, legislators, regulators, and judges will need to be more creative when tackling privacy problems by being willing to look beyond the FIPs and the standard data protection playbook. As we will explain in Part III, legislators and policymakers will need to look to relationships and power differentials, design and externalities, and manipulation and market power.[132] We have already seen flashes of this legislative imagination in a few pending bills. The Data Care Act of 2018 introduced by Senator Brian Schatz looks to relational duties of care, loyalty, and

---

[128] Kerry, *supra* note 70.

[129] *See* GELLMAN, *supra* note 45, at 13, 22–23 (noting that the 1974 act only applied to federal agencies and that today the United States has no complete FIPs-based regime that requires compliance from companies collecting data).

[130] *See, e.g.*, Kartikay Mehrotra et al., *Google and Other Tech Firms Seek to Weaken Landmark California Data-Privacy Law*, L.A. TIMES (Sept. 4, 2019), https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law [https://perma.cc/KP7U-R5AG] (documenting large tech companies' efforts to push amendments to the CCPA to create new exemptions that cover their activities).

[131] *See* Cameron F. Kerry, *A Federal Privacy Law Could Do Better than California's*, BROOKINGS (Apr. 29, 2019), https://www.brookings.edu/blog/techtank/2019/04/29/a-federal-privacy-law-could-do-better-than-californias/ [https://perma.cc/YEE6-YV5J] (claiming that a federal law could protect privacy better than the CCPA).

[132] *See infra* notes 161–256 and accompanying text.

confidentiality.[133] A discussion draft of the Consumer Data Protection Act circulated by Senator Ron Wyden looks to tackle automated decision systems and hold executives personally liable for certain privacy lapses.[134] The Deceptive Experiences to Online Users Reduction (DETOUR) Act introduced by Senators Mark Warner and Deb Fischer targets so-called "dark patterns": user interfaces that attempt to manipulate users into making decisions they would not otherwise do or are in ways adverse to their interests.[135] Although we are under no illusions of the likelihood that any of these bills will be passed given the sorry history of congressional privacy regulation, or not watered down given the power of the tech sector, they remain a good start in directing us towards the kind of third way we propose here.

The third way we envision would also require Congress to largely avoid preemption. There are of course many different ways Congress might preempt some but not all areas of privacy law while maintaining a flexible and layered approach to privacy federalism, but generally, limited or no preemption will be the key to an inclusive and adaptive regime. Other scholars have explored the virtues and vices of privacy preemption, and our purpose here is merely to note that this third approach should be built to resist ossification of privacy rules and to accommodate a broad range of privacy concerns beyond data by virtue of its personal nature.[136]

If we make no other contribution in this paper, we hope to convey that regardless of the merits of EU-style data protection regimes, now is the time for lawmakers, industry, advocates, and the public to rethink the trajectory of America's privacy identity. We must not proceed as though FIPs-style data protection regimes are the only way. Privacy's current constitutional moment might be our last meaningful opportunity to collectively interrogate and modify our first principle privacy values, goals, and strategy without a revolution. Our inevitable next step should be made bravely and carefully rather than merely following the path of least resistance.

---

[133] Data Care Act of 2018, S. 3744, 115th Cong. (2018). In the interest of full disclosure, both authors of this Article provided feedback on drafts of the bill.

[134] Consumer Data Protection Act, SIL18B29, 115th Cong. (2018) (discussion draft).

[135] Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019).

[136] For more detailed explorations on the role of preemption and federalism in American privacy law, see generally Bellia, *supra* note 13; Citron, *supra* note 33; Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIR. 57 (2013); Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 LEWIS & CLARK L. REV. 595 (2016); Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018); Schwartz, *supra* note 39.

II. THE VIRTUES OF DATA PROTECTION

There are of course many advantages to lawmakers taking the path of least resistance and fully assimilating the European vision for data protection. Adopting the FIPs would build upon a refined and remarkably sturdy tradition that is formidable and empowering (in a sense) to data subjects while also offering industry efficiency benefits gained through conformity and interoperability of international regimes. In this Part, we highlight these advantages in order to help better illuminate the calculus facing lawmakers.[137]

A. Refined and Sturdy

EU-style data protection was not a rush job. It is the fruit of decades of careful thought based upon actual experience. The GDPR is the product of mountains of collective wisdom, negotiation, and experience, including twenty years of experience with the Directive, and twenty years of the development of the FIPs before that.[138] The GDPR itself took years to formulate.[139] As one recent study explains:

> European policy makers started a process that involved a multitude of expert consultation and deep sophistication about how information practices can be manipulated to evade regulatory goals.
>
> Consultation began in 2009 and the European Commission published a proposal text in 2012. Two years later, the European Parliament adopted a compromise text, based on almost 4,000 proposed amendments. The Council of the European Union published its proposal for the GDPR in 2015, to start negotiations with the European Parliament. In December 2015, the Parliament and Council reached agreement on the text of the GDPR. The GDPR was officially adopted in May 2016, and [went into effect in] May 2018.[140]

This steady and careful process helped make the GDPR internationally attractive as a model because as a refined extension of many elements of the Directive, it was relatively time-tested. Paul Schwartz explains that "[b]eyond the force of EU market power and its negotiating prowess, the widespread influence of EU data protection reflects a success in the marketplace of regulatory ideas."[141]

As a result, one reason an EU-style FIPs regime might be attractive for lawmakers is that much of the heavy lifting has already been done. Concepts

---

[137] *See infra* notes 140–160 and accompanying text.
[138] Hoofnagle et al., *supra* note 2, at 70–71.
[139] *See id.* at 71 (detailing the process of drafting and passing the GDPR).
[140] *Id.* (citations omitted).
[141] Schwartz, *supra* note 1, at 774–75.

from the GDPR like "data controllers," "data processors," and "legitimate interests" are being constantly refined through a kind of international crowdsourcing. The longer this goes on, the sturdier FIPs-based regimes around the world will become. If U.S. lawmakers do not follow the rest of the world on privacy, they will lose some of the collective wisdom that could help quickly refine the rough parts of any new laws.

Margot Kaminski has held the GDPR up as a model for modern tech regulation because it balances both individual rights and industry accountability through what she refers to as "binary governance."[142] Kaminski argues that the "GDPR is both a system of individual rights and a complex compliance regime that, when applied to the private sector, is constituted through collaborative governance. The GDPR relies on both formal and informal tactics to create public-private partnerships in governing algorithmic decision-making."[143] This kind of collaborative approach is essential to ensure regulatory regimes are grounded in and informed by multiple perspectives.[144]

B. Conformity and Interoperability

It is remarkable that a concept as vague, contested, and culturally dependent as privacy has any meaningful areas of consensus. Yet, amazingly, the FIPs represent what Paul Bruening has called the "common language for privacy."[145] The global dominance of the FIPs now means that the European Union, Canada, Australia, Japan, Singapore, and many other Asian countries all speak substantially similar languages when it comes to data protection.[146] Even in "FIPs-lite" countries like the United States, the FIPs provide a starting point for finding common ground.[147]

---

[142] Kaminski, *supra* note 3, at 1537 (calling the GDPR's approach "binary").

[143] *Id.* at 1583.

[144] *See also* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 1025 (2016) (discussing the idea of "responsive regulation" in which public agencies work collaboratively with private actors to create a more effective compliance regime for privacy and data protection).

[145] Bruening, *supra* note 57; *see also* Bruening, *supra* note 23.

[146] *See generally* GELLMAN, *supra* note 45; GREENLEAF, *supra* note 4. A related version of the FIPs was incorporated into the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. *See* GREENLEAF, *supra* note 4, at 33–37 (outlining the main principles contained in the APEC framework and relating them to the principles articulated by the EU).

[147] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 & 42 U.S.C.) (relying on the FIPs to govern privacy law for health information); DIV. OF FIN. PRACTICES, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 1 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf [https://perma.cc/59TM-7S3Y] (calling for more regulation to ensure the FIPS govern online data and privacy).

This international conformity opens up all kinds of benefits. For example, it enables diplomatic solutions like Japan and Europe's mutual adequacy decision and the EU-United States Privacy Shield.[148] A common language of privacy was key in the creation of the Asian-Pacific Economic Cooperation's (APEC) cross-border privacy rules.[149] Even in federalist regimes like the United States, the common language helps avoid conflicting language and obligations among states and the federal government.[150] As one of this Article's authors wrote elsewhere: "[A] common language of privacy provides interoperability, relative harmony, and incremental change. It helps avoid lurches that deviate too far from established understandings of privacy. Without the FIPs, countries and states would risk talking past each other every time they needed to cooperate on privacy issues."[151]

C. Formidable and Empowering

The United States has lost the moral thread in the privacy debate. The GDPR has claimed the moral authority in privacy abdicated by U.S. lawmakers' continued deference to notice and choice, self-regulation, and a sectoral approach to privacy regulation in which some sectors of the economy have privacy statutes but others do not. For example, under the GDPR (or an equivalent omnibus data protection law) all health data would be protected because all personal data would be protected. But in the United States, only personal health information held by specific parties—like "covered entities" and "business associates"—is protected by HIPAA.[152] In an interview for this Article, the eminent FIPs scholar Robert Gellman had this to say to the question of whether Europe's approach to privacy clashed with the American approach to privacy:

> If we look at privacy alone, then the answer must be that the EU approach is not consistent with what we do here. We don't have an approach. The sectoral approach is not a policy or a plan. It's just a de-

[148] *See Federal Trade Commission Enforcement of the U.S.-E.U. and U.S.-Swiss Safe Harbor Frameworks*, *supra* note 83 (discussing the new Privacy Shield); *see also* Press Release, *supra* note 31 (discussing Europe's mutual adequacy decision for Japan).

[149] *See* GREENLEAF, *supra* note 4, at 537 (recognizing that APEC's Cross Border Privacy Rules System's mandate that corporations meet basic standards related to the notions of "'harm,' 'consent,' and 'accountability'" that are also found in the FIPs).

[150] *See* Citron, *supra* note 33, at 749 (noting that "[i]n the 1990s, while the Federal Trade Commission . . . was emphasizing self-regulation, state attorneys general were arguing that consumer protection laws required the adoption of Fair Information Practice Principles").

[151] Hartzog, *supra* note 58, at 960–61.

[152] 45 C.F.R. § 160.103 (2019); *see* Health Insurance Portability and Accountability Act of 1996.

> scription. Power over privacy policy and law is so spread out that there is no central driver here as there is in the EU.[153]

Quite simply, the United States has not taken privacy seriously, despite its industry giving rise to the personal data universe.

Although the GDPR is not perfect, one undeniable virtue of the law is that it has compelled companies to pay attention to it and, as a result, take a deep assessment of their own data practices. One study found:

> The GDPR awakened [U.S.] lawyers and the business community because it calls for minimum 8-figure fines and creates both internal and external mechanisms to bolster enforcement efforts.
>
> As a result, the GDPR is the most consequential regulatory development in information policy in a generation. The GDPR brings personal data into a complex and protective regulatory regime.[154]

In an interview for this Article, one scholar posited that one of the greatest virtues of the GDPR is that it caused many U.S. companies to take privacy seriously for the first time.[155] Consumers received a "barrage of updated privacy notices" in May 2018, but while that effect of the GDPR may have been the most visible, it was not the most important.[156] Although companies in a GDPR compliance cycle must always update their privacy policy, the key effect of the GDPR is "under the hood."[157] GDPR compliance thus requires privacy lawyers to:

- Perform a data mapping
- Identify a legal basis for possessing the data in the mapping, including how the firm minimizes the retention of data
- Review all vendor contracts to ensure that downstream data uses are consistent with the legal basis, meaning that downstream processors who were using the data to monetize it all of a sudden can no longer do so without becoming a co-controller
- Think through cross-border and data export issues (i.e., Privacy Shield)
- Develop process flows for data subject rights (these may be manual for companies that do not anticipate many requests)
- Develop procedures for breach notification

---

[153] E-mail from Robert Gellman to Woodrow Hartzog, Professor of Law & Comput. Sci., Northeastern Univ. (Aug. 14, 2018, 08:17 EST) (on file with authors).

[154] Hoofnagle et al., *supra* note 2, at 66.

[155] E-mail from Chris Hoofnagle, Adjunct Professor of Law, Univ. of Cal. Berkeley, to Woodrow Hartzog, Professor of Law & Comput. Sci., Northeastern Univ. (Aug. 12, 2018, 12:17 EST) (on file with authors).

[156] *Id.*

[157] *Id.*

- Figure out if one needs a DPIA; if one is needed, implement risk-mitigation procedures
- Figure out the DPO issue, and many companies need a DPO because behavioral advertising is "high risk"
- Start employee training
- Register with a lead European DPA
- Implement "state of the art" security[158]

These steps cumulatively force companies to balance people's privacy with firms' interests, with, according to our research, "a thumb on the scale for consumers. The result is at least a more considered approach."[159]

The data protection model that undergirds the GDPR thus has many virtues as a model for comprehensive privacy regulation. It is the product of many years of thought and it has proven resilient in the face of technological change up to this point. It forms the basis of a global system of personal data regulation that allows information to flow across national borders and remain protected at the same time. And it forces companies to take their internal governance structures for personal data seriously, while attempting to protect individual rights to empower humans in the control of their data. When done well, as in the GDPR, data protection is an effective model for the regulation of personal data. But as we will explore in the next Part, data protection law, particularly the kind of data protection law we might expect in the United States, has serious defects as well.[160]

III. WHY AMERICAN DATA PROTECTION WILL NOT BE ENOUGH

Although an EU-style data protection regime has many virtues, federal lawmakers should pause before adopting a European-style privacy identity for the United States. Even though the United States could end up with a European approach to privacy through federal inaction or through federal preemption, an EU-style data protection regime is not an inevitability for the United States. American lawmakers have a moral and strategic decision to make about the future direction and future identity of U.S. privacy law.

In this Part, we argue that U.S. lawmakers should resist the easy path of an EU-style data protection identity for America.[161] Even data processing that is fair to an individual is not always a good thing for the individual or for society.[162] Industry and governments' appetite for data has many costs that data protection

[158] *Id.*
[159] *Id.*
[160] *See infra* notes 161–256 and accompanying text.
[161] *See infra* notes 166–256 and accompanying text.
[162] *See infra* notes 167–191 and accompanying text.

regimes based on the FIPs cannot comprehend or counteract. In our emergent personal data-driven society, privacy involves structural questions about relationships and power differentials that the FIPs do not and cannot answer.[163] Moreover, even if the FIPs could answer some of these questions, what works well in Europe is unlikely to work as effectively in the United States.[164] It is highly probable that under any kind of U.S. GDPR likely to be enacted, data protection will get watered back down to the level of mere notice and choice because unlike the EU, the United States lacks a commitment to data protection as a distinct right, and because data protection regimes in the United States are likely to raise both spurious and real First Amendment objections from regulated industries. If Congress were to embrace omnibus, preemptive EU-style data protection, it would almost certainly wind up with a model that would fail to foster a full account of privacy and human well-being as well as fall short of its espoused protection and fair processing goals.[165] We thus should not blindly copy Europe and adopt the weak and myopic data protection model we are terming "GDPR-lite."

A. FIPs Assume Data Processing Is Always a Worthy Goal

The goal of data protection regimes like the GDPR has always been to encourage fair data processing and balance competing interests, rather than to prevent data processing entirely.[166] In other words, the entire endeavor of modern FIPs-based data protection is built around the idea that as long as data processing is fair to the data subject, the law should not just regulate it, but rather create a legal structure to enable it. The EU Data Protection Directive, for example, had the dual goals of providing for personal data rights as well as allowing for data to "flow freely" across the EU.[167] Similarly, although the GDPR is designed to advance "economic and social progress," bring EU economies closer together, and improve people's well-being, the function of the GDPR is to create a system that facilitates fair data processing at an unprecedented scale.[168] One of the three objectives announced by Article 1 of the GDPR is to ensure that "the free movement of personal data within the Union shall be neither restricted nor prohibited

[163] *See* Austin, *supra* note 25, at 131 (saying that privacy encompasses power dynamics); Cohen, *supra* note 25, at 22 (same).

[164] *See infra* notes 192–219 and accompanying text.

[165] *See infra* notes 220–256 and accompanying text.

[166] *See, e.g.*, Commission Regulation 2016/679, *supra* note 15, at 2 ("The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.").

[167] Council Directive 95/46, *supra* note 28, at 31.

[168] Commission Regulation 2016/679, *supra* note 15.

for reasons connected with the protection of natural persons with regard to the processing of personal data."[169]

Critics have long observed that the FIPs have their limitations. In the 1980s as they became widely adopted, James Rule and his colleagues criticized the FIPs because they posed no major obstacle to surveillance systems.[170] They conceived of the FIPs as "efficiency" principles that endeavored to improve information systems to operate better for both data controllers and data subjects, instead of substantively limiting data collection against the interests of data controllers.[171]

Rule and his colleagues were critical of this FIPs efficiency goal because it legitimized surveillance systems and also gave them moral privacy cover. They wrote that under the FIPs' criteria, "organisations can claim to protect the privacy of those with whom they deal, even as they demand more and more data from them, and accumulate ever more power over their lives."[172] Graham Greenleaf noted that this fundamental tension in the FIPs remains today, with lawmakers rarely asking "to what extent do and should data privacy principles and laws go beyond attempting to ensure the 'efficiency' of personal information systems, and provide means to limit and control the expansion of surveillance systems?"[173]

The GDPR is already facilitating surveillance, rather than stopping it. The Danish privacy regulator recently approved the deployment of facial recognition as an exception to the GDPR's provisions because in some circumstances it is in the public interest.[174] Greenleaf's question highlights the fundamental limitations of the FIPs and also reveals what Julie Cohen refers to as the overdetermined institutional failures of modern privacy protection.[175] Cohen explains that:

> Data harvesting and processing are one of the principal business models of informational capitalism, so there is little motivation either to devise more effective methods of privacy regulation or to implement existing methods more rigorously. Instead, the cultural and political

---

[169] *Id.* at 32.

[170] GREENLEAF, *supra* note 4, at 60–61 (citing JAMES RULE ET AL., THE POLITICS OF PRIVACY 93 (1980)).

[171] *Id.* (citing RULE ET AL., *supra* note 170, at 93).

[172] *Id.* (citing RULE ET AL., *supra* note 170); *see also* Claudia Diaz et al., *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923, 924–25 (2013) ("The notion of the data controller as a *trusted party* is ill at ease with the anti-surveillance gist of constitutional privacy and [privacy enhancing technologies].").

[173] GREENLEAF, *supra* note 4, at 61.

[174] IT-Political Ass'n of Den., *Danish DPA Approves Automated Facial Recognition*, EDRI (June 19, 2019), https://edri.org/danish-dpa-approves-automated-facial-recognition/ [https://perma.cc/EGG7-GXL6].

[175] Cohen, *supra* note 25, at 11.

> discourses that have emerged around data centered "innovation" work to position such activities as virtuous and productive, and therefore ideally exempted from state control.[176]

Data protection advances fair processing rules at the same time as it conditions us to a world and society in which data processing is inevitable—and inevitably good. The FIPs set the preconditions for processing, but ultimately, they fail to question the implications of the processing itself.

One notable exception to this trend is the GDPR's requirement that companies have a "legitimate interest" in processing data.[177] This balancing approach as a basis for legitimizing processing in theory incorporates larger societal interests.[178] Yet this provision seems to be largely focused on the business and operational interests of the data processor and the rights of and fairness to the data subject.[179] In the absence of more substantive protections, data protection regimes normalize an advertising-based culture that forces itself upon our time, attention, and cognitive faculties so that we must watch ads when we could be doing better things.

Additionally, because data protection regimes seek to regulate across the economy, they tend to treat the entities that control the processing of data the same. The GDPR applies, after all, to the data processing of both Facebook and your local sandwich shop. But in treating these entities the same, data protection regimes ignore how there may be significant differences of scale and power between large and small entities. In this way, data protection regimes are, in a certain sense, agnostic to the realities of market and informational power.

Cohen has argued that our information rules must provide the kinds of structural support that allow private and privacy-valuing subjects to flourish.[180] To that end, she has noted the limits of FIPs-based regimes and argued that "ef-

---

[176] *Id.* at 8.

[177] Commission Regulation 2016/679, *supra* note 15, at 36.

[178] CTR. FOR INFO. POLICY LEADERSHIP, HUNTON & WILLIAMS LLP, RECOMMENDATIONS FOR IMPLEMENTING TRANSPARENCY, CONSENT AND LEGITIMATE INTEREST UNDER THE GDPR 2 (May 17, 2017), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf [https://perma.cc/3H5R-QHPD] ("Legitimate interest may be the most accountable ground for processing in many contexts, as it requires an assessment and balancing of the risks and benefits of processing for organisations, individuals and society. . . . The legitimate interests to be considered may include the interests of the controller, other controller(s), groups of individuals and society as a whole.").

[179] *See* CTR. FOR INFO. POLICY LEADERSHIP, HUNTON & WILLIAMS LLP, EXAMPLES OF LEGITIMATE INTEREST GROUNDS FOR PROCESSING OF PERSONAL DATA 1 (Mar. 16, 2017), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf [https://perma.cc/KNB7-X2HW] (legitimate interest data processing "enables responsible uses of personal data, while effectively protecting data privacy rights of individuals").

[180] Cohen, *supra* note 25, at 3.

fective protection of breathing room for self-development requires more than just data protection."[181] We agree completely. We believe that if the United States is to chart a meaningful privacy law identity, it must actively go beyond GDPR-lite and embrace rules aimed at relationships, power, and a broader vision of how personal data affects people and society—the kinds of rules that FIPs regimes cannot deploy aimed at the kinds of harms such regimes cannot envision.[182]

Privacy is not just about notice, choice, and control.[183] It is more fundamentally about human and social well-being. But data protection regimes too often fail to account for the human and social externalities of the data industrial complex. We are only beginning to assess the human and social costs of platform dominance and massive-scale data processing. In addition to core privacy-related harms associated with data collection and data use, companies' demand for personal information is negatively affecting our attention and how we spend our time, how we become informed citizens, and how we relate to each other.[184] Phenomena like "fake news," "deep fakes," non-consensual pornography and harassment, teenage mental illness, texting and driving, oversharing on social media, addiction by design, and lives spent staring bleakly into our phones are at least partially attributable to or made worse by the personal data industrial complex.[185] We need broader frameworks for personal data not just because information is personal to us, but because the incentive to exploit it creeps into nearly every aspect of our technologically mediated lives.[186]

For example, data protection regimes do little to mitigate many of the problems of technologies that are designed to be addictive to maximize interaction and data collection. For example, the average person spends four hours staring at

---

[181] *Id.* at 23.

[182] *See id.* at 22 (agreeing that privacy is not only about consent and choice, but also power dynamics within relationships).

[183] *Id.*

[184] *See, e.g.*, NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US 63, 181–82 (2014) (lamenting a reduction in human skills and less meaningful personal relationships as a result of the growing prominence of machines in daily life).

[185] *See, e.g.*, BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 5 (2018) (examining "addiction by design"); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1874 (2019) (highlighting the problems of coerced or hidden pornography and "deep fake" videos); Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 691 (2013) (noting how social media gives people the ability to easily share everything about their lives).

[186] *See* FRISCHMANN & SELINGER, *supra* note 185, at 4–6 (putting forth a theory of "techno-social engineering" that is happening today in nearly all facets of human life); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 14–15 (2019) (describing the idea of "surveillance capitalism" and the exploitation of personal data by platforms to attempt to predict and control human behavior).

their phones every day.[187] Our compulsive use of technology is wreaking havoc on our emotional and mental well-being, particularly for young people.[188] Indeed, medical professionals are coming to a consensus that screen time adversely affects the healthy development of small children.[189]

In addition to our attention getting wheedled, manipulated, swindled, or outright taken from us, the appetite for data is producing reduced cognitive skills, reduced personal intimacy and offline interactions, and a corrosion of democracy.[190] More broadly, companies' appetite for data is also helping destroy the environment (through gadget garbage and energy drain) and overcrowd our roads (with GPS algorithms "optimizing" traffic patterns as if time to destination is the only relevant variable in our transport system).[191] If the United States embraces a narrow view of data protection, it will remain agnostic to these costs at this pivotal moment and instantiate a system that seeks for maximum exposure (and profit) with little thought to collateral harm and social good.

---

[187] Melanie Curtin, *Are You on Your Phone Too Much? The Average Person Spends This Many Hours on It Every Day*, INC.COM (Oct. 30, 2018), https://www.inc.com/melanie-curtin/are-you-on-your-phone-too-much-average-person-spends-this-many-hours-on-it-every-day.html [https://perma.cc/4H5P-FCFU].

[188] *See* Catherine Price, *Putting Down Your Phone May Help You Live Longer*, N.Y. TIMES (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/well/mind/putting-down-your-phone-may-help-you-live-longer.html [https://perma.cc/88FK-KXVW] (discussing how smart phones contribute to increased stress and higher levels of cortisol in the body that can be detrimental to human health); *see also* Stephen Marche, *The Crisis of Intimacy in the Age of Digital Connectivity*, L.A. REV. BOOKS (Oct. 15, 2018), https://lareviewofbooks.org/article/crisis-intimacy-age-digital-connectivity/#! [https://perma.cc/7JYN-RA82] (positing that new technologies are straining the development of interpersonal relationships).

[189] Emily S. Rueb, *W.H.O. Says Limited or No Screen Time for Children Under 5*, N.Y. TIMES (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/health/screen-time-kids.html [https://perma.cc/X4UR-D4E5].

[190] *See, e.g.*, CARR, *supra* note 184, at 63, 181–82 (decrying the deterioration of cognitive skills and weakened personal relationships as a result of the rise of technology use in our lives); NICHOLAS CARR, THE SHALLOWS: WHAT THE INTERNET IS DOING TO OUR BRAINS 34–35 (2011) (exploring how technology use can rewire human brains and lead to the weakening of some mental abilities).

[191] Ingrid Burrington, *The Environmental Toll of a Netflix Binge*, THE ATLANTIC (Dec. 16, 2015), https://www.theatlantic.com/technology/archive/2015/12/there-are-no-clean-clouds/420744/ [https://perma.cc/NKZ4-GJVY]; A.J. Dellinger, *The Environmental Impact of Data Storage Is More than You Think—and It's Only Getting Worse*, MIC (June 12, 2019), https://www.mic.com/p/the-environmental-impact-of-data-storage-is-more-than-you-think-its-only-getting-worse-18017662 [https://perma.cc/NYG6-BBJY]; Andrew J. Hawkins, *Uber and Lyft Finally Admit They're Making Traffic Congestion Worse in Cities*, THE VERGE (Aug. 6, 2019), https://www.theverge.com/2019/8/6/20756945/uber-lyft-tnc-vmt-traffic-congestion-study-fehr-peers [https://perma.cc/ZS9L-33MT]; Joe Jacob, *Data Centers: A Latent Environmental Threat*, DUKE GREEN CLASSROOM (Mar. 8, 2017), https://sites.duke.edu/lit290s-1_02_s2017/2017/03/08/data-centers-a-latent-environmental-threat/ [https://perma.cc/G6PW-NJ2Q]; Alexis C. Madrigal, *The Perfect Selfishness of Mapping Apps*, THE ATLANTIC (Mar. 15, 2018), https://www.theatlantic.com/technology/archive/2018/03/mapping-apps-and-the-price-of-anarchy/555551/ [https://perma.cc/Q75S-SY9W].

B. The United States Is Not Europe

A second reason to be wary of a GDPR-lite solution for the United States is that the United States and the EU have very different legal structures and cultures. This is particularly true at the constitutional level, in which there are two important differences—Europe's recognition of fundamental human rights to privacy and data protection, and America's deep-seated commitment to the free expression guarantee under the First Amendment.

1. Data Protection as a Human Right

The American constitutional system has no explicit constitutional right to privacy. American constitutional law protects privacy against the government implicitly in a few areas, including the First Amendment's right to anonymous expression, the Third Amendment's protection against the quartering of soldiers in private homes during peacetime, the Fourth Amendment's "reasonable expectation of privacy" against government searches and seizures, and the Fifth and Fourteenth Amendments' substantive due process rights to information privacy and decisional autonomy.[192] Yet the American system of fundamental rights is characterized by negative rights against the state. There are very few constitutional rights that apply to private actors, and none approaching a general constitutional right to privacy, much less data protection.

The status of privacy as a fundamental right in Europe is very different. The European Convention on Human Rights has long been held to protect a right to privacy, albeit one phrased as the "right to respect for private and family life."[193] The newer Charter of Fundamental Rights of the European Union not only protects a right to "respect for private and family life" in Article 7, but also has an express right of "protection of personal data" in Article 8.[194] There are two additional features of European fundamental human rights law that are distinct from the United States. First, European fundamental rights are, by definition, subject to the concept of proportionality—fundamental rights can be explicitly balanced with each other, and must also be balanced against the legitimate needs of a

---

[192] *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 598–600 (1977) (suggesting that the Fourteenth Amendment protects a constitutional right of information privacy); Katz v. United States, 389 U.S. 347, 357–59 (1967) (extending the Fourth Amendment's unreasonable search and seizure protection to wiretapping and introducing the notion of a "reasonable expectation of privacy" as the lodestar of Fourth Amendment protection); NAACP v. Alabama, 357 U.S. 449, 466 (1958) (holding that individuals' rights "to pursue their lawful private interests privately and to associate freely with others in so doing" implicated Fourteenth Amendment protections against a state law mandating a private organization to disclose its membership list).

[193] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, art. 8.

[194] Charter of Fundamental Rights of the European Union, *supra* note 75, at 397.

democratic society.[195] Second, European fundamental rights are subject to the doctrine of "horizontal effect"—if a member state fails to protect a person's fundamental right against other members of society, the fundamental right has nevertheless been violated.[196]

These constitutional differences are particularly important when privacy rules sit on top of them. In Europe, the GDPR is best understood as a vindication of fundamental human rights in privacy and data protection against other members of society, both natural persons and corporations. If a corporation (for example, Google) fails to protect the fundamental rights of privacy and data protection (for example, by allowing its search engine to access outdated but true information about a person), it has violated European law (in this case, whatever positive law instrument like the Directive or the GDPR implements that fundamental right).[197] Legal rules like the GDPR matter significantly because they are regulations enforcing fundamental rights.

By contrast, in the United States, consumer privacy rules implement public policy, but they do not enforce fundamental rights of privacy. Something like the GDPR would seem to be required by European law to vindicate fundamental rights, but American consumer-law protections like the FTC Act's prohibition on unfair and deceptive trade practices are not compelled by the U.S. Constitution.[198] Congress could repeal or shrink the FTC Act tomorrow without any constitutional problems because there is no constitutional right of consumer privacy or data protection in the U.S. system. The consumer privacy stakes are seen as lower in the American system, and privacy is just one of many interests to be traded off against one another in policy discussions, rather than a fixed constitutional limitation.

By contrast, as noted above, there is a right of privacy in the United States against government searches or seizures (including warrantless wiretapping).[199] Thus, if Congress were to repeal the federal Wiretap Act's requirement that government wiretapping requires a warrant, the government would still have to get a

---

[195] *Id.* at 406.

[196] *See* Stephen Gardbaum, *The "Horizontal Effect" of Constitutional Rights*, 102 MICH. L. REV. 387, 395, 397 (2003) (describing the European horizontal effect doctrine as "impos[ing] constitutional duties on private actors as well as on government").

[197] *See* C-131/12, Google Spain SL & Google Inc. v. Agencia Española de Protección de Datos & Mario Costeja González, 2014 EUR-Lex CELEX LEXIS 317, ¶¶ 89–99 (imposing a "right to be forgotten" derived from the EU Directive against Google under the European Charter of Fundamental Rights and Freedoms).

[198] *See* 15 U.S.C. § 45(a)(1) (2018) (outlawing "unfair or deceptive acts or practices in or affecting commerce" through a statutory decree of Congress).

[199] *See* U.S. CONST. amend. IV; *Katz*, 389 U.S. at 349–51 (ruling that placing a listening device on a public phone booth was an unconstitutional violation of the Fourth Amendment when done without a proper warrant).

warrant to wiretap a telephone.[200] But because there is nothing like the horizontal effect doctrine in American constitutional law, Congress could repeal the Wiretap Act's prohibition on private wiretapping.[201]

What this means is that European consumer privacy law is built upon a foundation of fundamental human rights that are protected against both governments and private actors; American consumer privacy law is not. Something like the GDPR or the Directive is a logical and necessary implication of the structure of the EU Constitution, but something like the GDPR is not mandated by the U.S. Constitution or any other principle of American law. Something like the GDPR could perhaps be mandated by a properly ratified international treaty,[202] but it is instructive in this regard that the United States has not yet joined Convention 108+, the only international convention on the protection of personal data.[203]

Practically speaking, although something like the GDPR-lite would be incompatible with EU constitutionalism, an American GDPR-lite would be perfectly legal; indeed, it would probably offer more protection than the current American regime of notice and choice backed up by the FTC's unfair and deceptive trade practices power. The upshot is that the absence of a constitutional foundation in the United States would mean that any attempts to enact something like the GDPR would be relatively easy for opponents to water down into something like GDPR-lite.

2. Spurious and Real First Amendment Objections

A second significant difference between the United States and Europe is the regulatory role played by the fundamental right of free expression. In Europe,

---

[200] *See generally* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. 3, 82 Stat. 197, 211 (1968) (codified as amended in scattered sections of 18 U.S.C. (2018)).

[201] *See* Gardbaum, *supra* note 196, at 388 (explaining how U.S. constitutional rights almost exclusively bind governmental but not private actors).

[202] *Cf.* Missouri v. Holland, 252 U.S. 416, 433–35 (1920) (suggesting that properly ratified international treaties cannot be challenged under the Tenth Amendment). For further exploration of this point, see Neil M. Richards, Missouri v. Holland, *in* 3 ENCYCLOPEDIA OF THE SUPREME COURT OF THE UNITED STATES 312 (David S. Tanenhaus ed., 2008).

[203] *See Convention 108+: The Modernised Version of a Landmark Instrument*, COUNCIL EUR. (May 18, 2018), https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108 [https://perma.cc/8YVR-38FG] (calling Convention 108+ the only legally enforceable international protection of personal information); *see also Council of Europe Privacy Convention*, ELECTION PRIVACY INFO. CTR., https://epic.org/privacy/intl/coeconvention/#modernconvention [https://perma.cc/H4RL-3JSR] (noting that advocacy groups have lobbied for the United States to join Convention 108+); Jennifer Baker, *What Does the Newly Signed 'Convention 108+' Mean for UK Adequacy?*, INT'L ASS'N PRIVACY PROFS. (Oct. 30, 2018), https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/ [https://perma.cc/84FA-F8EB] (indicating that the United States has not signed Convention 108+).

free expression is safeguarded by Article 10 of the European Convention and Article 11 of the EU Charter.[204] Like other European fundamental rights, these provisions are subject to proportionality analysis—where they conflict with another fundamental right such as the right to privacy or to data protection, courts must balance the rights on an equal footing.[205]

By contrast, in the United States, the fundamental right of free expression protected by the First Amendment is not subject to proportionality analysis—if a court finds that there is a First Amendment right, then the First Amendment applies to the state action, and strict scrutiny normally applies.[206] In practice, this means that in the United States, privacy protections that restrict the dissemination of true matters (particularly those found to be of legitimate public concern) can run into serious constitutional problems. For example, restrictions on the dissemination by the press of the names of rape victims have repeatedly been held to violate the First Amendment.[207]

By contrast, restrictions of this sort would not appear to create a problem under European law. In the context of data protection, it is likely that the broad right to be forgotten protected in Europe under both the Directive and the GDPR[208] would run into serious constitutional problems if enacted in the United States.[209] As we have argued elsewhere, it is possible to make too much of this difference—most regulations of commercial data in the United States do not raise any First Amendment problems,[210] a fact that the Supreme Court has itself

---

[204] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 193, art. 10 ("Everyone has the right to freedom of expression."); *see also* Charter of Fundamental Rights of the European Union, *supra* note 75, at 398 (same).

[205] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 193, art. 10 (stating that right to freedom of expression is to be balanced against interests including "national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary"); *see also* Charter of Fundamental Rights of the European Union, *supra* note 75, at 406–07 (providing that limitations on any rights provided in the charter are "[s]ubject to the principle of proportionality" and "may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others").

[206] *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1172 (2005) (providing an example of government regulation of speech's content that would receive strict scrutiny analysis).

[207] *E.g.*, Fla. Star v. B.J.F., 491 U.S. 524, 526, 532 (1989) (ruling unconstitutional Florida's imposition of civil penalties on a newspaper that printed the name of a sexual assault victim).

[208] Commission Regulation 2016/679, *supra* note 15, at 43–44.

[209] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 73–94 (2015); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1532–33 (2015).

[210] Richards, *supra* note 209, at 1505.

recognized.[211] Nevertheless, the First Amendment would raise some real obstacles to the adoption of something like the GDPR in the United States, at least with respect to some of its more controversial provisions.

Beyond these real but limited First Amendment difficulties, we are more broadly concerned about spurious First Amendment objections derailing policy discussions and being used as further ammunition to weaken any privacy rules introduced before Congress.[212] Arguments that "data is speech" and thus data protection rules are censorship have rhetorical appeal, even though they break down completely under serious analysis. We worry further that the trend in federal judicial appointments under the current administration may be more receptive to these kinds of arguments, and usher in the further use of the First Amendment as a kind of radically deregulatory digital *Lochner v. New York*, in which the Supreme Court in 1905 infamously invalidated a New York statute attempting to regulate working conditions.[213] Either way, the nature of First Amendment discourse and jurisprudence in the United States would likely cause a GDPR-lite to be further weakened, and still sit uneasily on its legal footing after being enacted.

3. Spurious and Real Standing Objections

Another constitutional difference that a U.S. GDPR might face is the doctrine of standing inferred by federal courts from Article III of the U.S. Constitution.[214] This doctrine requires that private litigants suing to enforce their rights must show, as a jurisdictional matter, that they have (1) suffered an *injury in fact* that was (2) *caused* by the defendant and that would be (3) *redressed* by a favorable judgment.[215] Privacy claims in particular have been at the forefront of

---

[211] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011) (distinguishing First Amendment free speech protections from restrictions on economic activity and commercial regulations that incidentally burden expression).

[212] *See* Richards, *supra* note 206, at 1210–21 (arguing that applying heightened First Amendment scrutiny to ordinary data privacy law is both unsupported by First Amendment jurisprudence and may be misused to usher in a new *Lochner*-type era to invalidate important economic regulations).

[213] Lochner v. New York, 198 U.S. 45, 64 (1905); *see, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1408–16 (2000) (offering an alternative to market-based, *Lochner*-like understandings of free speech); Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 538–60 (1998) (arguing that economists' pure "market-based model" of information markets is fundamentally flawed and akin to the logical fallacies that led to the *Lochner* era); Jeremy K. Kessler & David E. Pozen, *The Search for an Egalitarian First Amendment*, 118 COLUM. L. REV. 1953, 1959–60 (2018) (lamenting the Supreme Court's recent "Lochnerian" approach to the First Amendment and its use against legitimate regulation).

[214] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) (noting that Article III's standing requirements limit the types of cases that federal courts may hear).

[215] *Id.* at 409.

standing doctrine developments in recent years, as courts have often refused to take privacy law's dignitary, psychological, or procedural harms seriously.[216] Two Supreme Court decisions are particularly important in this trend. In *Clapper v. Amnesty International USA*, the Supreme Court held that plaintiffs challenging amendments to federal surveillance law could not bring a claim because their fears were "highly speculative" in nature and because "allegations of possible future injury are not sufficient."[217] More significantly, in *Spokeo v. Robins*, involving a claim that a data broker had failed to follow the procedures laid down by the Fair Credit Reporting Act, the Court held not only that private litigants had to show that they had suffered "concrete" harm as a legal matter, but also that "a bare procedural violation" would be insufficient to show concreteness, and thus standing and jurisdiction over the claim.[218] Such developments show a hostility in the federal judiciary towards legal claims that are *abstract*, focused on violations of *procedures* laid down by law, and that tend towards the prevention of *future* injury. Of course, these are precisely the hallmarks of data protection regimes, which prescribe *procedures* to forestall *future* harms that are violations of the *abstract* right of privacy. To be clear, we do not mean to suggest that privacy claims cannot be enforced in American courts (they clearly can be), but rather that data protection-style claims can face particular standing problems that make it more difficult for plaintiffs to obtain relief than is the case in Europe. This conclusion, in fact, was recently reached by the Data Protection Commissioner of Ireland in the high-profile 2017 case *Schrems v. Data Protection Commissioner*, and sustained by the Irish High Court and Irish Supreme Court.[219] Thus, a U.S. GDPR that sought to use private rights of action to enforce privacy rights (like the European GDPR does) would face additional constitutional hurdles stemming from U.S. standing doctrine that could further limit its effectiveness and scope.

More generally, the different constitutional footing of privacy rights in the United States would make implementation of a faithful U.S. GDPR difficult, and would further push regulators towards what we are calling "GDPR-lite."

---

[216] MCGEVERAN, *supra* note 5, at 199 ("Developments in privacy law, particularly standing doctrine, have also increased the obstacles to private suits, including class actions.").

[217] 568 U.S. at 409–10.

[218] 136 S. Ct. 1540, 1548–50 (2016). *See generally* Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681.

[219] Data Prot. Comm'r v. Facebook Ire. Ltd. & Schrems [2017] IEHC 545, 70, 197 (H. Ct.) (Ir.), *aff'd*, [2019] IESC 46 (SC) (Ir.). The case is currently before the European Court of Justice for resolution of substantive points of European law.

C. Data Protection Is Myopic

FIPs-based regimes were relatively well-equipped for the initial wave of personal computing in the 1960s and 1970s.[220] Electronic data was relatively costly, scarce, and manageable. Computers had yet to become ingrained in our daily lives and the internet had yet to be democratized. Because data processing seemed revolutionary, lawmakers embraced fairness as a goal that could balance people's privacy and well-being with innovation and efficiency.[221]

That was fifty years ago—a time of network television, rotary dial phones, and slow computers that filled entire rooms. Today's lawmakers need to update both the goals and the tools of our data regulation model.[222] Automated technologies and substantially greater amounts of data have pushed FIPs principles like "data minimization, transparency, choice, and access to the limit."[223] Progress in robotics, genomics, "biometrics, and algorithmic decision-making" are putting pressure on rules meant to ensure fair aggregation of personal information in databases.[224]

Although the FIPs can probably continue to be a necessary component of any federal data privacy framework, they are not sufficient for several reasons.[225] First, the FIPs contain "several blind spots."[226] They are largely concerned with data aggregation by companies.[227] They do not meaningfully address human vulnerabilities to each other on platforms like social media, human susceptibility to manipulation, or issues of platform power and competition policy.[228] Robots and artificial intelligence (AI) that act like humans, tools that measure brain activity, and advances in genomics raise problems related to how people respond to anthropomorphic technologies, how people might one day be unable to hide thoughts, harm that comes from forecasting of things that have not even happened yet, and protecting "personal" DNA data that is shared with family members as a function of elementary biology.

---

[220] Hartzog, *supra* note 58, at 953.

[221] *See* SEC'Y ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., *supra* note 44, at xx–xxi (suggesting standards of fair information practice in light of the new effects of "computerization" on society).

[222] *See* GELLMAN, *supra* note 45, at 43 (noting criticism of the FIPs for failing to maintain "pace with information technology").

[223] Hartzog, *supra* note 58, at 953.

[224] *Id.*

[225] GELLMAN, *supra* note 45, at 1.

[226] Hartzog, *supra* note 58, at 954.

[227] *Id.*

[228] *Id.*

The state of privacy protection is also bad and getting worse. For years, the rate and scale of privacy failures has grown exponentially.[229] The fragile wall that policymakers constructed half a century ago to mitigate the risks of discrete databases is cracking. The time-honored response to any privacy issue from government and industry has been to give users more control.[230] From social media to biometric information, proposed solutions include some combination of "privacy self-management" concepts like control, informed consent, transparency, notice, and choice.[231] Even the GDPR speaks to the idea that "natural persons should have control of their own personal data."[232]

These concepts are attractive because they seem empowering. But in basing policy principles for data protection on notice and choice, privacy frameworks are asking too much from a concept that works best when preserved, optimized, and deployed in remarkably limited doses. People only have so much time and so many cognitive resources to allocate. Even under ideal circumstances, our consent is far too precious and finite to meaningfully scale.

The problem with notice and choice models is that they create incentives for companies to hide the risks in their data practices though manipulative design, vague abstractions, and complex words as the companies also shift risk onto data subjects. As we have explained in detail elsewhere, the notice and choice "approach has been a spectacular failure."[233]

Bert-Jaap Koops has argued that European data protection law is based on the delusion that it can give people control over their data, which it cannot.[234] We agree. Even the idealized, perfected transparency and control model contemplated by these frameworks is impossible to achieve in mediated environments. There are several reasons why. First, the control that companies promise people is an illusion. Engineers design their technologies to produce particular results.[235] Human choices are constrained by the design of the tools they use.[236]

---

[229] *See, e.g.*, Lapowsky, *supra* note 93 (highlighting the monumental Cambridge Analytica privacy scandal).

[230] *See, e.g.*, Mathews & Bowman, *supra* note 11 (indicating that the intent driving the CCPA is to give people more control over their personal data).

[231] *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013) (explaining how policies based around these concepts have driven privacy regulation since the 1970s).

[232] Commission Regulation 2016/679, *supra* note 15, at 2.

[233] Richards & Hartzog, *supra* note 67, at 1498–99.

[234] *See generally* Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIVACY L. 250 (2014). *See also generally* Shannon Togawa Mercer, *The Limitations of European Data Protection as a Model for Global Privacy Regulation*, 114 AM. J. INT'L L. UNBOUND 20 (2020), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/885BD6110E4AF6C9F7412AE3F2C481F0/S2398772319000837a.pdf/limitations_of_european_data_protection_as_a_model_for_global_privacy_regulation.pdf [https://perma.cc/Z3HM-3JFD].

[235] *See* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns* 3 (Univ. of Chi., Working Paper No. 719, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Companies decide the kind of boxes people get to check, buttons they press, switches they activate and deactivate, and other settings they get to fiddle with.[237] By presenting limited choices as "more options" for users, companies can instill in users a false sense of control by obscuring who is really in control of the interaction.[238]

Data collectors also have incentives to use the power of design to manufacture our consent. Deploying the insights of behavioral economics, companies create manipulative interfaces that "exploit our built-in tendencies to prefer shiny, colorful buttons and ignore dull, grey ones."[239] They may also shame us into feeling bad about withholding data or declining options.[240] Many times, companies make the ability to exercise control possible but costly through forced work, subtle misdirection, and incentive tethering.[241] Sometimes platforms design online services to wheedle people into oversharing through gamification, such as keeping a "streak" going or nudging people to share old posts or congratulate others on Facebook.[242] Companies know how impulsive sharing can be and therefore implement an entire system to make it easy.[243]

Second, notice and choice regimes are overwhelming. They simply do not scale because they conceive of control and transparency as something people can never get enough of.[244] Human users are presented with a dizzying array of switches, delete buttons, and privacy settings.[245] We are told that all is revealed in a company's privacy policy, if only we would read it.[246] When privacy harms happen, companies promise more and better controls. And if they happen again, the diagnosis is often that companies simply must have not added enough or improved dials and checkboxes.[247]

Control over personal information is attractive in the abstract, but in practice it is often an overwhelming obligation. Mobile apps can ask users for over

---

[https://perma.cc/SXX9-26VS] (arguing that corporations build their tech interfaces to unwittingly force users into certain choices).

[236] *Id.*

[237] Woodrow Hartzog, Opinion, *The Case Against Idealising Control*, 4 EUR. DATA PROTECTION L. REV. 423, 426 (2018).

[238] *Id.*

[239] *Id.* at 427.

[240] Luguri & Strahilevitz, *supra* note 235, at 10 (describing this practice of "confirmshaming").

[241] For more information on the concept of dark patterns, see generally DARK PATTERNS, http://www.darkpatterns.org [https://perma.cc/QA4H-R8JD].

[242] Luguri & Strahilevitz, *supra* note 235 at 10 (highlighting this practice of "gamification").

[243] *See* Richards, *supra* note 185, at 691 (discussing "frictionless sharing").

[244] Hartzog, *supra* note 58, at 974–75.

[245] *Id.* at 975.

[246] *See id.* at 974–75 (noting it is practically impossible for everyone to read all the privacy policies they see).

[247] *See id.* at 974 (criticizing the notion that any privacy problem can be fixed with more user control).

two hundred permissions and even the average app asks for about five.[248] As the authors of this Article have put it elsewhere, "[t]he problem with thinking of privacy as control is that if we are given our wish for more privacy, it means we are given so much control that we choke on it."[249]

Even if the law were to require that privacy protective choices were the default option, companies could still repeatedly ask us to flip the publicity switch.[250] People that have turned off notifications on their mobile apps can attest to the persistent, grinding requests to turn them back on almost every time they open the app. And even if a company were to somehow deliver perfect information and provide meaningful choices, it would not solve the limited bandwidth we have as human beings limited to one brain. Every piece of information meant to inform us is a demand on our time and resources. Right now, every company gets to make those demands whenever they want. The result is a thousand voices all crying out simultaneously asking us to make decisions. People have no real way to filter those requests. Instead, users become burdened, overwhelmed, and resigned to the path of least resistance. As Brett Frischmann and Evan Selinger have explored, our consent has been manufactured, so we just click "agree."[251]

There are ways to balance data exploitation and protecting people, but it requires human protection and not just data protection. It requires a framework that reimagines the relationships between people and the companies they interact with. It also requires that we place trust at the center of our approach to digital consumer protection. As we have argued in other articles, being trustworthy in the digital age means companies must be *discreet* with our data, *honest* about the risk of data practices, *protective* of our personal information and, above all, *loyal* to us—the data subjects and customers.[252] As we describe below, our privacy

---

[248] MICHELLE ATKINSON, PEW RESEARCH CTR., APPS PERMISSIONS IN THE GOOGLE PLAY STORE 4 (2015), https://www.pewresearch.org/internet/2015/11/10/apps-permissions-in-the-google-play-store/ [https://perma.cc/924C-8HNQ].

[249] Hartzog, *supra* note 237, at 429.

[250] *See* Commission Regulation 2016/679, *supra* note 15, at 48 (mandating that companies, by default, ensure a level of data privacy in the European Union); *see also id.* at 15 (suggesting the same).

[251] *See* FRISCHMANN & SELINGER, *supra* note 185, at 5 (arguing that simply hitting "I agree" to unread terms and conditions is a result of "addiction by design").

[252] For more information on taking trust seriously in privacy law, see generally DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102–04 (2004); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Ian Kerr, *Personal Relationships in the Year 2000: Me and My ISP*, *in* PERSONAL RELATIONSHIPS OF DEPENDENCE AND INDEPENDENCE 78 (Law Comm'n of Can. ed., 2002); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017); Richards & Hartzog, *supra* note 8.

frameworks should be built to encourage and ensure this kind of trustworthy conduct.[253]

Traditional data protection frameworks are so focused on the data of each individual that they overlook important social and civil rights implications of collecting and processing personal data. Marginalized communities, particularly communities of color, shoulder a disproportionate burden from privacy abuses.[254] U.S. lawmakers should embrace a privacy identity that goes beyond narrow and individualized conceptions of privacy to incorporate more societal and group-based concerns as well as civil rights-based protections.

Finally, lawmakers must always remember that privacy is inevitably about the distribution and exercise of power. Scholars including Lisa Austin, Julie Cohen, and Dan Solove have noted that privacy rules will only be effective if they meaningfully address the disparities of power between people and those collecting and using our information.[255] This means crafting rules and frameworks that target the structure of organizations and re-allocate power among the stakeholders in the digital ecosystem. Regardless of which choice lawmakers make, without structural support, resources, and a strong political mandate for enforcement, any privacy framework will merely be a pretext for exploitation. Whether legislation creates a new data privacy agency or emboldens existing federal agencies, regulators must have broad grants of authority, including rulemaking provisions where necessary, robust civil penalty authority, and the ability to seek injunctions quickly to stop illegal practices. Regulation should also include private causes of action and rights for data subjects, so long as these do not become the sole privacy enforcement mechanisms.

The modern data ecosystem is something of a runaway train. Trust rules can help, but they too will not be enough. Some data practices might be so dangerous that they should be taken off the table entirely. Others might be harmful to society in ways that do not implicate a violation of any trust. To be fully responsive to modern data problems, a meaningful U.S. privacy framework needs to embrace substantive boundaries for data collection and use. In the next Part, we propose a new regulatory framework to solidify America's privacy identity as inclusive and responsive to how companies obtain and yield the power related to the collection and use of personal information—one that goes beyond the limits of the data protection model.[256]

---

[253] *See infra* notes 287–236 and accompanying text.

[254] Group Letter to Congress on Civil Rights in Privacy Legislation 2 (Feb. 13, 2019), http://civilrightsdocs.info/pdf/policy/letters/2019/Roundtable-Letter-on-CRBig-Data-Privacy.pdf [https://perma.cc/GMS5-83P7].

[255] *See supra* note 25 and accompanying text.

[256] *See infra* notes 257–358 and accompanying text.

IV. A New Framework for American Privacy

So now what? As we seek a governance framework for our data-driven society, there is a lot we can learn from constitutional law. A constitution is a framework, a blueprint, and a design for governance. The U.S. Constitution, for example, is first and foremost a design blueprint for government, creating the legislative, executive, and judicial powers, and allocating them among the three branches of a federal government of limited and enumerated powers and the state governments of broader but inferior powers.[257] This was the ratified Constitution of 1788, to which the substantive protections of the Bill of Rights were added shortly thereafter, substantive rights thought to be a necessary safeguard to procedural protections.[258]

In this constitutional moment for privacy policy, we need to think carefully about the structures we will use to govern the flow of human information that is reshaping our society. We need a new framework for privacy that is sensible, practical, and durable. To be clear, we are not calling for the constitutionalizing of privacy, but rather drawing an analogy to constitutional law, and making an argument for a new frame of governance for privacy. Like the U.S. Constitution, this blueprint would operate at several different levels. At the level of procedure, this blueprint should prescribe fair and ethical procedures for the processing of human information, just like the data protection model does.[259] Analogous to the unamended Constitution of 1788, it would prescribe processes that would regulate and regularize data processing. But the blueprint would also operate at the level of substance. Just as the drafters of the 1788 Constitution realized that procedural rules alone are susceptible to abuse by those who wield their powers, our blueprint would also place restrictions on certain kinds of data practices.[260] This is akin to the strategy of the Bill of Rights, which takes certain dangerous government practices (censorship, a state church, abolition of jury trials, cruel and unusual punishments) off the table.[261]

The GDPR and the data protection project represent a procedural move like the 1788 Constitution—allocation of authority and responsibility, and prescrip-

---

[257] *See* U.S. Const. arts. I, II, III (dividing the federal government into three distinct branches, each with different powers).

[258] *See id.* amends. I–X (constituting the Bill of Rights).

[259] *See* Chander et al., *supra* note 103, at 14 (noting the FIPs are foundational to the GDPR).

[260] *See* Leonard W. Levy, Origins of the Bill of Rights 27–34 (1999) (noting that Anti-Federalists, including Thomas Jefferson, believed a majority-driven government could abuse its power if a bill of rights were not added to the Constitution).

[261] *See* U.S. Const. amend. I (prohibiting the establishment of a state church or the abridgment of free speech); *id.* amend. VI (securing the right to jury trials); *id.* amend. VIII (prohibiting cruel and unusual punishments).

tion of ordinary procedures.[262] But procedural requirements are little protection without substantive limitations to back them up. In its constitutional moment, American privacy policy has confronted the same problem faced by America's founding generation in its own constitutional moment—the need for substantive rules to shore up well-meaning but ultimately insufficient procedural ones.

This is perhaps not as radical a step as it might seem at first glance. Privacy lawyers already talk in constitutional terms with respect to data governance frameworks.[263] What are binding corporate rules but a data constitution? We should bring a similar blueprint-like approach to privacy law. The endeavor to restrain corporate power can learn a lot from the governance project of the eighteenth century for government power. But the line between procedure and substance is famously blurry. Indeed, even in the U.S. Constitution, the procedural strategy includes structural protections and the substantive strategy includes procedural protections.[264] As we reckon with privacy law's constitutional moment, we think it is more helpful to identify areas that should be targeted by any multilayered strategy to draft a new U.S. privacy framework. We do so with an eye towards crafting rules and structural mandates that create incentives and business models that not only protect people as individuals, society as a whole, and our natural resources, but also nurture safe and sustainable information relationships and technological developments that benefit everybody.

Every law or regulatory regime has a landscape on which it is focused, that is, a particular area or dynamic that is to be affected. For example, data is the locus of the GDPR. All of the rules that constitute the GDPR revolve around it—how it is collected, processed, and shared.[265] But as we have explained in this Article, one of the key limitations of the GDPR is that there is much more to the personal data industrial complex than the collection and processing of data. If we are concerned with how the power created and distributed by personal data is obtained and exploited, then we think a layered procedural, substantive, and structural approach to privacy law can be reflected in *four* overlapping areas, only one of which is data *as* data. We argue that all four focal points of privacy must be addressed if a governing framework for our human information is to be

---

[262] *See* Hoofnagle et al., *supra* note 2, at 85–88 (describing some of the GDPR's procedural requirements for data collectors).

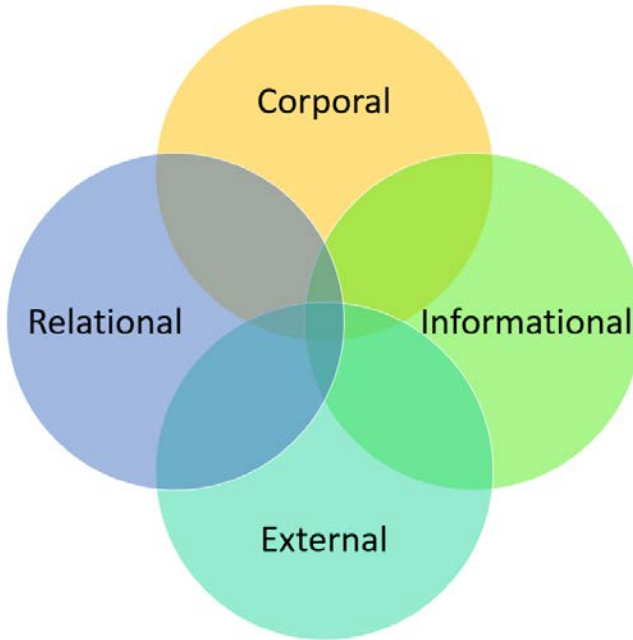
[263] *See, e.g.*, Chander et al., *supra* note 103, at 12–13 (arguing that the new GDPR in Europe is a natural outgrowth of the European constitutional documents that recognize data protection as a "fundamental human right").

[264] *See, e.g.*, Todd David Peterson, *Procedural Checks: How the Constitution (and Congress) Control the Power of the Three Branches*, 13 DUKE J. CONST. L. & PUB. POL'Y 209, 230 (2017) (arguing that the Constitution's "case or controversy" procedural requirement imposed on Article III courts actually limits those courts' ability to exercise their substantive power).

[265] *See* Mathews & Bowman, *supra* note 11 (saying the GDPR covers disclosures made to data subjects, procedures for data breach notification, data security, international data transfers, and more).

complete: (1) corporate matters; (2) trustworthy relationships; (3) data collection and processing; and (4) personal data's externalities.

We envision these four landscapes for privacy regulation as related and overlapping:



Each landscape invokes a different set of rules, structural changes, and dynamics. For example, laws targeting corporal matters would seek to address not only the amount of power corporate entities have in the marketplace (and how they wield it), but also any law aimed at how organizations use the corporate form and how that form might be relevant to people's privacy. *Corporal* privacy rules would include structural questions regarding the corporate form and piercing the corporate veil, corporate licensing and registration requirements, and taxation issues.[266] Meanwhile, *Relational* privacy rules would look to the relative power disparities within information relationships and the vulnerabilities of those who expose themselves to data collectors.[267] *Informational* protection rules focus on data like the fair processing requirements of the GDPR that follow the data regardless of corporal form or the nature of relationships between parties.[268] The final tier of laws would target *External* consequences—the external costs (what an economist would call "externalities") imposed on society by the personal data

[266] *See infra* notes 279–286 and accompanying text.
[267] *See infra* notes 287–327 and accompanying text.
[268] *See infra* notes 328–337 and accompanying text.

industrial complex, including environmental pollution, corrosion of democratic self-governance, and reduced well-being through the hijacking of attention.[269]

Thinking about privacy law in terms of landscape areas rather than solely through the lens of data protection has some distinct advantages. It allows lawmakers to see the big picture, then to focus rules with an eye towards directly addressing the root of a problem rather than clumsily using data rules to deal with issues that data rules can address in only an indirect way at best. For example, data protection rules often require companies to obtain the consent of users before engaging in risky practices.[270] But the harm to be avoided is not necessarily a lack of autonomy in decision making, but rather some other harm such as manipulation, overexposure, chilling effects, loss of opportunity, or some other harm that results from a data collector's recklessness, indiscretion, and disloyalty, or from the power effects in a relationship. This is an issue regarding the *relationship* between the data subject and the data collection, and it is better addressed directly with trust-enforcing rules like duties of confidence, care, and loyalty.[271]

Conceptualizing the problem of privacy regulation in this way allows for a more careful, nuanced, and directed approach. It allows regulators to target power more directly, treating specific pathologies that arise in one area (i.e., relationships) but not others (i.e., data), and to treat companies differently according to their power, size, and relationships to the data collector.[272] It would allow lawmakers to address a broader range of privacy harms without having to create one omnibus law to rule them all like the GDPR.[273] A landscape approach to an overarching privacy framework could also guide lawmakers in adjacent areas like antitrust, environmental law, health law, and consumer protection law without any formal intervention or regulatory commingling. Having an approach to privacy rules that is also compatible with other areas implicated by the personal data industrial complex would allow lawmakers and regulators to foment support for meaningful rules across the board that more directly responds to problems of power, relationships, data, and externalities in a consistent way.

---

[269] *See infra* notes 339–358 and accompanying text.

[270] *See, e.g.*, Mathews & Bowman, *supra* note 11 (discussing GDPR provisions that require companies to get customers' consent before they sell customers' data).

[271] *See* Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKANIZATION (Mar. 5, 2014, 4:50 PM), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/6BUG-JUJY] (arguing that online services that collect personal data from individuals should be treated as "information fiduciaries").

[272] *Cf. id.* (suggesting that treating all online companies the same when imposing fiduciary duties onto them would be a mistake because all companies are different).

[273] *See* Mathews & Bowman, *supra* note 11 (calling the GDPR "an omnibus law").

Some scholars and lawmakers are skeptical that a layered approach to privacy regulation will work.[274] Some see the best answer as a monolithic, omnibus approach that works as a clearinghouse or one-stop-shop for all privacy-related matters.[275] Others fear that relational approaches like fiduciary trust rules are either antithetical to structural approaches like competition law or will devour the political clout or resources necessary to pursue other ends.[276] Nevertheless, the history of regulation in the United States demonstrates that not only is a layered approach possible, but that it might be the only way to effectively accomplish rule creation and enforcement. The FTC enforces many different privacy laws in addition to Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices.[277] The FTC itself shares privacy regulatory authority with Health and Human Services, the Federal Communications Commission, and state attorneys general.[278] This is to say nothing of the complex web of rules stemming from private tort and contract law as well as constitutional law. Lawmakers, courts, and regulators regularly balance conflicting interests and loyalties, issuing targeted rules that address some, but not all, privacy problems. America's privacy identity need not reside in one omnibus framework or one regulatory agency as in Europe, but rather in a demonstrated (but wholesale) commitment to addressing power and vulnerability in substance, structure, and procedure in all relevant areas.

A. Corporal

If privacy is about power, then the center of power lies with corporate structure and affordances.[279] Corporate entities amass market power, use structure to dilute and deflect responsibility, and act based on financial incentives that affect the other three privacy dynamics of relationships, data, and externalities.[280] Any meaningful privacy framework should directly address corporate matters like misused market power, dangerous corporate structure, and corrosive business incentives.

---

[274] *See* Schwartz, *supra* note 39, at 923–27 (presenting the common arguments in favor of an omnibus privacy law as opposed to fragmented ones).

[275] *Id.*

[276] *See, e.g.*, Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 528 (2019) (arguing that a privacy law regime focused on establishing fiduciary responsibilities without addressing larger problems, such as "market structure or political-economic influence," is fundamentally flawed).

[277] 15 U.S.C. § 45(a)(1) (2018).

[278] Hartzog & Solove, *supra* note 32, at 2236, 2256.

[279] *See* Austin, *supra* note 25, at 131 (suggesting that privacy relationships are mostly about power).

[280] *See, e.g.*, Khan & Pozen, *supra* note 276, at 527–28 (discussing the large market share tech giants have accumulated, the market structure within which they operate, and how it all puts private data at risk).

1. Competition

Competition law has been underutilized as a privacy regulatory tool, but there is a groundswell of support to change that.[281] Thanks to personal data and the interactive nature of digital technologies, platforms have unique incentives, affordances, and market power unlike anything regulators have ever seen before. Competition and antitrust law are the traditional tools to directly address such dangerous accumulations of power. As Lina Khan and David Pozen argue in calling for a focus on platform dominance instead of relational privacy protections:

> The relevant inquiry for legal reformers, we submit, should be not just how a firm such as Google or Facebook exercises its power over end users, but whether it ought to enjoy that kind of power in the first place. Limiting the dominance of some of these firms may well have salutary effects for consumer privacy, both by facilitating competition on privacy protection and by reducing the likelihood that any single data-security failure will cascade into a much broader harm.[282]

Pozen and Khan are correct that a focus solely on data protection or trust might distract from antitrust approaches to platform regulation, but we see no need to make a stark choice between antitrust and what we are calling here *relational trust*. Our frameworks of privacy regulation need not ignore information relationships to focus on platform dominance, as we argue in this Article. But to ignore legal tools designed to address platform power would leave privacy law incomplete.

---

[281] *See, e.g.*, MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 335 (2016) (urging government competition officials to acknowledge data's potential to have anticompetitive effects); TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 3 (2018) (noting that antitrust laws should be updated to deal with new challenges presented by large tech companies); Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 792–97 (2017) (calling for new antitrust laws that account for the ways in which companies can use data for anticompetitive purposes); Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 980–82 (2019) (promoting "structural separations," a type of antitrust remedy, for large online operators); Khan & Pozen, *supra* note 276, at 528 (arguing that antitrust enforcement against large tech companies will reduce the threat they pose to data privacy); Robert Walters et al., *Personal Data Law and Competition Law—Where Is It Heading?*, 39 EUR. COMPETITION L. REV. 505, 505 (2018) (noting the increased demands on antitrust officials to examine the anticompetitive effects of possessing personal data); Gabriela Zanfir-Fortuna & Sinziana Ianc, *Data Protection and Competition Law: The Dawn of 'Uberprotection'* (Working Paper, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290824 [https://perma.cc/SXX9-26VS] (discussing the emergence of competition law in the context of data privacy).

[282] Khan & Pozen, *supra* note 276, at 528.

2. Corporate Structure

Privacy law should be concerned with a number of corporate matters, including limiting how the corporate form is used to shield bad actors from personal liability. One major issue surrounding the FTC's complaint against Facebook in the Cambridge Analytica scandal was whether Facebook founder and CEO Mark Zuckerberg would be held personally responsible for overseeing unfair and deceptive trade practices.[283] Such personal liability is common in other areas of the law, such as securities violations.[284] Some have even proposed the prospect of criminal punishment for executives guilty of egregious privacy violations.[285] Given what is at stake when large online platforms abuse their power, liability of this sort in certain instances seems warranted.

Other structural corporate approaches might include empowering chief privacy officers and other ombudsman-like employees with meaningful decision-making abilities and insulation from executive pushback when their decisions might impose costs on a company's business model. Lawmakers could also provide statutory protection for whistleblowers that call out corporate malfeasance and chicanery regarding personal information. More fundamentally, lawmakers could mitigate or alter the primacy of shareholders for platforms with dominant power regarding personal information. In the least, lawmakers could explore backing away from maximizing shareholder value on a quarterly basis as a way to encourage more long-term sustainable relationships with users.[286]

Let us be clear about what we are suggesting here. We are not calling for the upending of corporate law or rampant and unconstrained piercing of the corporate veil. Instead, we are trying to highlight that corporate law rules can act as regulatory levers over platforms and other tech companies in ways that traditional privacy law tools might not. The digital revolution has upended many settled expectations in our society, including those of regulation. It would be naïve to expect that the new powers that information capitalism has brought would not require an adjustment to the toolkit used to regulate companies to prevent harm

---

[283] Aarti Shahani & Avie Schneider, *FTC to Hold Facebook CEO Mark Zuckerberg Liable for Any Future Privacy Violations*, NPR (July 24, 2019), https://www.npr.org/2019/07/24/741282397/facebook-to-pay-5-billion-to-settle-ftc-privacy-case [https://perma.cc/J69P-RATQ].

[284] *See, e.g.*, Merritt B. Fox, *Civil Liability and Mandatory Disclosure*, 109 COLUM. L. REV. 237, 241–42 (2009) (noting personal civil liability for officers and directors for material misstatements in a company's SEC registration statement).

[285] *See* Albert Fox Cahn, *Prison Time Is the Answer to Tech's Privacy Crisis*, MEDIUM (July 22, 2019), https://onezero.medium.com/prison-time-is-the-answer-to-techs-privacy-crisis-53da1559124f [https://perma.cc/MK9J-SQUZ] (arguing that criminal penalties will provide more effective deterrence against privacy violations than even large corporate fines).

[286] *See* Tamara Belinfanti & Lynn Stout, *Contested Visions: The Value of Systems Theory for Corporate Law*, 166 U. PA. L. REV. 579, 605 (2018) (noting that maximizing shareholder value has been the paradigmatic purpose for corporate law for nearly thirty years).

and nudge them in socially beneficial directions. Appropriate use of corporate law's regulatory tools, then, would seem a logical response to the privacy problems stemming from corporate informational power.

B. Relational

The most important privacy-relevant relationships in the modern age are those between data subjects and data collectors—between humans and the companies that collect and process their information. Much of the personal data about U.S. internet users stems from relationships with either their internet and mobile service providers, with websites and apps they use, or with major tech platforms like Google, Amazon, Apple, Facebook, and Microsoft.[287] This means that many, if not most, privacy concerns are rooted in a relationship characterized by extreme information and power asymmetries.[288]

In these relationships, users are vulnerable, and platforms have all the power because they design the environment that dictates the interaction.[289] These companies also are much more knowledgeable about the risks that come with people sharing their data. They also know much more about us (and what makes us tick) than we know about them. They know our likes and dislikes, how long our mouse hovers over particular links, what our friends are doing (and saying behind our backs), and they have the machinery to exploit it all.[290] And all we know is that we have fifteen minutes to check Instagram, send that email, or order that printer toner before our lunch break is over, so who has time to engage in threat modeling or read terms of use?

The extreme vulnerability of people to companies in information relationships means we should have much better rules for and recognition of a trustworthy relationship.[291] In previous research, we and other scholars, including Ari Waldman, have called for lawmakers to turn away from the ineffective notice and choice model toward rules designed to protect the trust that users place in companies when they share their personal information.[292] Our proposals have

---

[287] *See* Khan & Pozen, *supra* note 276, at 498 (noting that online businesses, especially large ones like Google and Facebook, gather "enormous" amounts of data on their users).

[288] *See id.* at 520 (arguing that relationships between users and large online platforms such as Facebook are marked by an "unusually stark asymmetry of information").

[289] *See id.* (claiming that most people do not understand the basic operations of digital businesses and that companies impose their control on users).

[290] *See id.* (noting that Facebook accumulates data to discern users' interests, traits, political preferences, and consumer desires).

[291] *See id.* (positing that large online service providers, like Facebook, create "an elaborate system of social control").

[292] Richards & Hartzog, *supra* note 252, 1213–24; Richards & Hartzog, *supra* note 8, at 434–35; Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579, 590

similarities to the movement to treat data collectors as "information fiduciaries" and to impose stringent duties of confidentiality, care, and loyalty on those who collect and process personal information.[293] This movement is reflected in Senator Brian Schatz's proposed Data Care Act of 2018.[294] Nevertheless, the trust rules we are calling for have a broader application beyond the formalized framework of information fiduciaries. Trust rules are certainly relational in nature, but are not necessarily dependent upon formal relationships to function, much less on the complete framework of fiduciary duties. In other words, lawmakers certainly can and should establish duties owed by specific entrustees to those who make themselves vulnerable through exposure, but they might also create rules and frameworks generally aimed at creating and preserving trustworthy relationships or rules simply justified by the vulnerability of users to the platforms with which they interact.

As we have argued elsewhere, trustworthy entities have four features that the law should promote—discretion, honesty, protection, and loyalty.

1. Discretion

One of the most fundamental and oldest privacy protections is the duty of confidentiality.[295] The obligation to keep a confidence was once formidable and a key component of certain relationships in the Anglo-American common law. Nevertheless, in the United States, with the advent of Prosser's four privacy torts, the tort cause of action for breach of confidence stalled.[296] As contract law gradually favored boilerplate language, confidentiality agreements became less of a focus for those individuals sharing information with others,[297] though the growth of the non-disclosure agreements (NDAs) has continued in recent years outside the consumer context.

(2017); *see also* WALDMAN, *supra* note 252, at 77–146 (providing a framework for trust-driven privacy law).

[293] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1221–30 (2016) (calling for these fiduciary duties to be attached to online service providers); Balkin, *supra* note 271 (same); *see also* SOLOVE, *supra* note 252, at 213–14 (drawing on confidential relationships protected by law—such as those in the realm of doctor-patient relationships and the law of evidence—to be applied to privacy).

[294] Data Care Act of 2018, S. 3744, 115th Cong. (2018).

[295] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 133–35 (2007) (exploring long-standing commitments to confidentiality in Anglo-American law).

[296] *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1888–90 (2010) (demonstrating how Prosser's rigid conceptualization of tort privacy separated it from confidentiality and limited its ability to evolve).

[297] *See* Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 764 & n.2, 781 (2014) (noting the rise of boilerplate online contracts lacking explicitly negotiated confidentiality provisions).

Lawmakers looking for ways to embolden American privacy law could start by revitalizing the tort of confidentiality by expanding it to cover new kinds of information relationships typified by asymmetrical power and vulnerabilities.[298] They could broaden secondary liability doctrines like "inducement to breach confidentiality" and "interference with confidential relationships" that could be applied to reckless platforms that encourage breaches of confidence through design. For example, there are obvious applications of such doctrines to websites that solicit non-consensual pornography from former partners or lovers.[299] Judges and lawmakers both could revive the doctrine of implied confidentiality to apply to user interfaces as well as face-to-face interactions.[300] And finally, courts, lawmakers, and regulators could evolve private law and statutory frameworks to foster a kind of "chain-link confidentiality" that would follow information as it moved downstream from one confidant to the next, empowering the trusting party every step of the way.[301]

Trust, however, involves more than just confidentiality and nondisclosure. As we have explained in other research, "[t]here are ways other than rigid nondisclosure that entrustees can protect trustors. They can limit to whom they disclose information, they can limit what they share with others, and they can control how they share information to make sure they preserve the trust placed in them."[302] Lawmakers could also create frameworks that facilitate limited disclosure to particular parties or in deidentified and obfuscated ways.[303] This would allow trustees to act discreetly while still sharing certain information with others. But the basic point is that discretion is a foundation of trust, and the law should promote trust in information relationships by creating incentives, and where appropriate duties, to be discreet.

2. Honesty

Paradoxically, openness is a foundational principle of privacy and data protection law, at least when it comes to openness about data practices. The idea is

---

[298] *See* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1670 (2011) (arguing that courts should broaden their contract analysis of interactive websites in order to find elements of contracts, including promises to protect privacy, within website designs themselves).

[299] For similar proposals, see DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 167–81 (2014) (proposing legislative reforms to address the problem of non-consensual pornography); Citron, *supra* note 185, at 1944–53 (same).

[300] Hartzog, *supra* note 297, at 765.

[301] Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 659–60 (2012).

[302] Richards & Hartzog, *supra* note 8, at 460.

[303] *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 708–09 (2016) (calling for a new legal framework for data protection that is "process-based," rather than solely concerned with harm, so that data can be shared with others while still safeguarding privacy).

if companies are transparent, people will be on notice of the risks of exposure and interaction in the digital world. But of course, this ethos is too often used in dense privacy policies as a fiction to exploit people under a thin veneer of compliance in a way that does little to keep them safe or on actual notice.[304] If companies are to keep the trust they have been given, it is not enough to be merely passively "open" or "transparent." Trust "requires an affirmative obligation of honesty to correct misinterpretations and to actively dispel notions of mistaken trust."[305]

A focus on honesty flips the focus of transparency from formal disclosure requirements to a focus on the reasonable expectations of entrustees. Being honest means lawmakers should create rules that balance honesty with notions of safety, as with products liability law. For example, companies that make dangerous products are not at fault if the dangerous aspects of a tool can be reasonably avoided with a warning.[306] But if no warning would be reasonably effective, the product must simply be made safer.[307] Honesty also means exploring the full range of design and information dissemination techniques beyond just words. Ryan Calo, for example, has called for new strategies of "visceral" notice:

> Unlike traditional notice that relies upon text or symbols to convey information, emerging strategies of "visceral" notice leverage a consumer's very experience of a product or service to warn or inform. A regulation might require that a cell phone camera make a shutter sound so people know their photo is being taken. Or a law could incentivize websites to be more formal (as opposed to casual) wherever they collect personal information, as formality tends to place people on greater guard about what they disclose.[308]

Other scholars in the field of human computer interaction have researched ways to create design spaces for effective privacy notices by focusing on timing, channel, modality, and control.[309]

---

[304] *See* Richards & Hartzog, *supra* note 67, at 1498–99 (arguing that transparency is an insufficient goal, and that a focus on mere transparency has led to "a sea of 'I agree' buttons, drop-down menus, and switches that [people] are unable to navigate").

[305] Richards & Hartzog, *supra* note 8, at 462.

[306] *See* David G. Owen, *The Puzzle of Comment* j, 55 HASTINGS L.J. 1377, 1381 (2004) (pointing to general tort law that says products are not found to be defective or unreasonably dangerous if they bear warnings which make the product safe to use when followed).

[307] *See id.* at 1393 (acknowledging that no matter how clear or numerous product warnings are, companies are still liable for manufacture and design defects).

[308] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2012) (footnotes omitted).

[309] Florian Schaub et al., *A Design Space for Effective Privacy Notices*, SYMP. USABLE PRIVACY & SECURITY, 2015, at 1, 6–10, https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf [https://perma.cc/ZGW7-F2MP].

Paul Ohm has recently called for "forthright code," explaining that "[e]ven when software isn't deceptive, far too often it still is not as honest as it could be, giving rise to consumer harm, power imbalances, and a worrisome restructuring of society. With increasing and troubling frequency, software hides the full truth in order to control or manipulate us."[310] Ohm argues that regulators should mandate "forthrightness from our code," that "would impose an affirmative obligation to warn rather than a passive obligation to inform."[311] According to Ohm:

> A forthright company will anticipate what a consumer does not understand because of cognitive biases, information overload, or other mechanisms that interfere with information comprehension, and will be obligated to communicate important information in a way that overcomes these barriers. . . .
>
> We could begin to assess not only what a company said but also what a company concealed. It might become illegal to exploit a user's known biases and vulnerabilities.[312]

Such arguments are consistent with the call for honesty as a foundational element of trust that we call for here, as in other work.

3. Protection

It seems that a major company suffers a major data breach almost every week. These are, among other things, data security failures. Almost all FIPs-based regimes have data security obligations, with language usually along the lines of "[p]ersonal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."[313] As we have explained elsewhere, "[p]olicymakers have tended to interpret security requirements in terms of the process data holders must take to protect against attackers. This mainly consists of regularly auditing data assets and risk, minimizing data, implementing technical, physical, and administrative safeguards, and creating and following a data breach response plan."[314] But if we want to be serious about safeguarding trust, more entities need to be responsible for security, while the law must recognize broader theories of harm, such as increased risk and anxiety and the costs of reasonable pre-

---

[310] Paul Ohm, *Forthright Code*, 56 HOUS. L. REV. 471, 472 (2018).

[311] *Id.* at 472–73.

[312] *Id.* at 473.

[313] *See* ORG. FOR ECON. COOPERATION & DEV., *supra* note 54, at 15 (containing the "security safeguards principle," part of the OECD's 2013 Privacy Framework that was based on the FIPs).

[314] Richards & Hartzog, *supra* note 8, at 465–66 (footnotes omitted).

ventative measures.[315] Trust violations resulting from a failure to protect users carry with them the right for those harmed users to bring suit against the entrustees who have failed them.

4. Loyalty

Above all, humans trusting entities with their personal data should be able to demand loyalty from those entrustees. The duty of loyalty is a hallmark of fiduciary relationships that requires a strict commitment to refrain from self-dealing and a firm prioritization of the trustors' interests over the interests of the entrustee.[316] Although trust rules for data collectors can be modeled on such firm duties of loyalty, they need not be so uniformly robust.[317] In this respect we depart from some readings of the information fiduciaries movement.[318] Lawmakers might consider imposing a duty of *reasonable* loyalty on data collectors that would restrict only unreasonable self-dealing. Alternatively, lawmakers could create rules and frameworks targeted at specific kinds of activities that are, in practice, disloyal. That is, those practices that serve the interests of the entrustee at the expense of the trusting and vulnerable party.

A good example of disloyal behavior by trusted companies are so-called "dark patterns" in software user interfaces.[319] Dark patterns are "user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions."[320] Common examples include unnecessary multiple checkboxes and extra clicks required to unsubscribe from marketing emails; prominently featured "I AGREE" buttons placed next to small, hidden, and blended-in "no thanks" buttons; and options to decline framed in such a way as to shame the user into agreeing to certain proposals ("no thanks, I hate free stuff!"), a practice known as "confirmshaming."[321] Such acts are disloyal because they are intentional attempts to use both design and the insights of behavioral economics to privilege a

---

[315] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) (arguing that courts in data breach cases have focused too heavily on a narrow conception of harm that does not include risk and anxiety to the plaintiffs, even in cases where defendants' fault is clear).

[316] Richards & Hartzog, *supra* note 8, at 468.

[317] *See id.* at 458 (recognizing that imposing full fiduciary duties onto information relationships could be "burdensome").

[318] *See id.* (suggesting that it is a mistake to believe that legal rules must either choose to protect data subjects with fiduciaries or choose not to protect them at all).

[319] *See* DARK PATTERNS, *supra* note 241 (describing dark patterns as "tricks used in websites and apps that make [people] do things that [they] didn't mean to").

[320] Luguri & Strahilevitz, *supra* note 235, at 3.

[321] *Id.* at 6–9; *see* TYPES OF DARK PATTERN, https://www.darkpatterns.org/types-of-dark-pattern [https://perma.cc/57AW-QCMH] (discussing "confirmshaming").

company's interests in data collection and attention harvesting over the user's autonomy and privacy interests.

Lawmakers could discourage disloyal behavior several different ways. For example, Congress could modify Section 5 of the FTC Act to include a prohibition against abusive trade practices. The notion of abusive design already exists elsewhere in consumer protection law, most prominently from the relatively new Bureau of Consumer Financial Protection.[322] The Dodd-Frank Wall Street Reform and Consumer Protection Act authorized the Bureau of Consumer Financial Protection to prohibit any "abusive" act or practice that:

> (1) *materially interferes* with the ability of a consumer to understand a term or condition of a consumer financial product or service; or
> (2) takes unreasonable advantage of—
> (A) a *lack of understanding* on the part of the consumer of the material risks, costs, or conditions of the product or service;
> (B) the *inability of the consumer to protect* the interests of the consumer in selecting or using a consumer financial product or service; or
> (C) the reasonable *reliance* by the consumer on a covered person to act in the interests of the consumer.[323]

This language squarely targets practices that elevate a company's financial interests over the interests of a vulnerable trustor and adversely affects the trusting party.

Lawmakers could also create legislation that targets dark patterns; indeed, several already have. The proposed DETOUR Act, introduced by Senators Warner and Fischer, would make it unlawful for any large online operator:

> (A) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data; (B) to subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user involved; or (C) to design, modify, or manipulate a user interface on a website or online service, or portion thereof, that is directed to an individual under the age of 13, with the purpose or substantial effect of cultivating com-

---

[322] *See* 12 U.S.C. § 5531(d) (2018) (defining abusive practices "in connection with the provision of a consumer financial product or service"); *see also id.* § 5491(a) (establishing the Bureau of Consumer Financial Protection to "regulate the offering and provision of consumer financial products or services under the Federal consumer financial laws").

[323] *Id.* § 5531(d) (emphasis added).

> pulsive usage, including video auto-play functions initiated without the consent of a user.[324]

Senator Hawley has also introduced a similar piece of legislation prohibiting manipulative design aimed at children and video game players.[325] Senator Schatz's Data Care Act, in addition to a duty of care and a duty of confidentiality, would impose an explicit duty of loyalty on data collectors.[326] The duty of loyalty in the act would require that:

> An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user.[327]

C. Informational

As we explained in Part II, despite being incomplete, the data protection approach embodied in the GDPR has many virtues.[328] Many of its limitations would be eliminated by a comprehensive strategy of the sort we are calling for here. As part of such a strategy, U.S. privacy law should build upon the wisdom of the GDPR, which facilitates fair data processing with a greater willingness to prohibit certain problematic kinds of collection and processing outright.[329] Data subject rights, procedural requirements like data protection and algorithmic impact assessments, and structural requirements, such as requiring a data protection officer, should be incorporated into U.S. data protection law in ways similar to

---

[324] Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. § 3(a)(1) (2019).

[325] Press Release, Josh Hawley, U.S. Senator for Mo., Senator Hawley to Introduce Legislation Banning Manipulative Video Game Features Aimed at Children (May 8, 2019), https://www.hawley.senate.gov/senator-hawley-introduce-legislation-banning-manipulative-video-game-features-aimed-children [https://perma.cc/CKY4-LMPK].

[326] Press Release, Brian Schatz, U.S. Senator for Haw., Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online (Dec. 12, 2018), https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online [https://perma.cc/VTQ4-6V5Z]. We must disclose at this point that this bill was in part influenced by our other academic work, and we consulted with Capitol Hill staff before this bill was enrolled.

[327] Data Care Act of 2018, S. 3744; *see also* Woodrow Hartzog & Neil Richards, *It's Time to Try Something Different on Internet Privacy*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-0315-11e9-9122-82e98f91ee6f_story.html [https://perma.cc/NAG8-WA8S] (discussing Senator Schatz's bill and its proposed duty of loyalty).

[328] *See supra* notes 137–159 and accompanying text.

[329] *See* Hoofnagle et al., *supra* note 2, at 76 (laying out the four criteria that must be met under the GDPR before data collectors may legally process data).

the GDPR (making appropriate allowances for American free speech and standing doctrines).[330] A strong data protection framework may not be sufficient to regulate the digital economy, but it is necessary.

Lawmakers might improve upon the conventional wisdom regarding data protection in several different ways. First, they can get serious about limiting collection in the first place.[331] Some scholars have argued that since the internet's creation, the restrictions on data collection are equally (and sometimes more) important than rules surrounding data use.[332] Data that does not exist cannot be exposed, shared, breached, or misused. FIPs-based data protection regimes are resistant to outright and inflexible collection limits because the FIPs are designed to facilitate, not restrict processing. The FIPs, after all, usually cash out in procedural rather than substantive rights. But data distributes power to collectors. Limiting collection could help restore balance. Pointedly, though, if lawmakers are to meaningfully limit collection, they will have to accept and be clear about the financial costs of so doing, and prepare to make the case that such costs are necessary for the kind of innovation that is both sustainable and actually advances human values and human flourishing.[333]

Lawmakers could also consider more rigid mandatory deletion requirements instead of flexible, context-sensitive ones. In harmony with the spirit of deletion, lawmakers committed to privacy should also ignore calls for mandatory data retention periods, a practice that Europe finds constitutionally repugnant on

---

[330] *See id.* at 85–89 (noting the data subject rights, data protection requirements, and obligation for corporations to have data protection officers, all contained within the GDPR).

[331] *See id.* at 76 (stating that data collection and processing are almost always allowed under U.S. laws).

[332] *See, e.g.*, Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1919 (2013) (decrying "unfettered information collection and processing"); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1538–39 (2000) (criticizing privacy laws that have relatively strong rules regarding data use but still allow too much data collection); Bruce Schneier, *Helen Nissenbaum on Regulating Data Collection and Use*, SCHNEIER ON SECURITY (Apr. 20, 2016, 6:27 AM), https://www.schneier.com/blog/archives/2016/04/helen_nissenbau.html [https://perma.cc/8SGU-ZJ4E] (discussing a proposal to continue to focus on collection regulation).

[333] The work of Julie Cohen is instructive on this point. Cohen wrote:

> [T]here is reason to worry when privacy is squeezed to the margins and when the pathways of serendipity are disrupted and rearranged to serve more linear, commercial imperatives. Environments that disfavor critical independence of mind and that discourage the kinds of tinkering and behavioral variation out of which innovation emerges will, over time, predictably and systematically disfavor innovation of all types. Environments designed to promote consumptive and profit-maximizing choices will systematically disfavor innovations designed to promote other values. The modulated society is dedicated to prediction but not necessarily to understanding or to advancing human material, intellectual, and political well-being. Data processing offers important benefits, but so does privacy. A healthy society needs both.

Cohen, *supra* note 332, at 1927.

multiple grounds.[334] Finally, lawmakers could create rules and duties that respect the value of data obscurity. Obscurity exists when it is hard to find or understand data about people (compare, for example, a library card catalog to a Google search), and obscure data is relatively safe.[335] We rely upon our obscurity every day when making choices about how much, when, and where we expose ourselves. For example, you might purchase sensitive or embarrassing products with cash in a publicly accessible drug store where anyone can see you, but the likelihood of anyone noticing or tracking you is quite low. Obscurity such as this has been a natural feature of human life that we have relied upon since time immemorial, but one that the law too rarely takes into consideration.

Lawmakers seeking a holistic approach to privacy should create rules that help create and protect our obscurity and our ability to manage it. The practice of deidentification of data has long been a feature of privacy law, and although deidentification is rarely perfect, it is often adequately obscure to do the work required of it.[336] This could take the form of design rules that prevent obscurity lurches (like unilaterally changing people's privacy settings on social networks to maximum exposure) or it might consist of outright bans on uniquely dangerous technologies like facial recognition tools. The cities of San Francisco and Oakland in California and Somerville in Massachusetts, for example, have recently passed legislation banning government use of facial recognition.[337] And as more of our immutable genetic data is sequenced by physicians and direct-to-consumer genomic testing companies, we should seriously consider obscurity protections for such data before we inadvertently create a national genetic database ripe for abuse.

---

[334] *See* Joined Cases C-293/12 & C-594/12, Dig. Rights Ir. Ltd. v. Minister, 2014 EUR-Lex CELEX LEXIS 238, ¶ 69 (Apr. 8, 2014) (finding that data retention requirements placed in publicly available electronic communications services violate Articles 7 and 8 of the Charter of Fundamental Rights of the European Union).

[335] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1358 (2015); *see, e.g.*, Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 44 (2013) (claiming that "[o]nline information that is not searchable, accessible, or understandable poses less of a threat to a user's privacy"); *see also* Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 397 (2013) (calling for methods of obscurity to be built into online social interactions so that users can protect their own privacy).

[336] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1735 (2010) (showing how recent developments making reidentification easier have made deidentification efforts less effective).

[337] Charlie Osborne, *Oakland Follows San Francisco's Lead in Banning Facial Recognition Tech*, ZDNET (July 19, 2019), https://www.zdnet.com/article/oakland-city-follows-san-franciscos-lead-in-banning-facial-recognition-tech/ [https://perma.cc/DBJ6-3MB5]; Sarah Wu, *Somerville City Council Passes Facial Recognition Ban*, BOS. GLOBE (June 27, 2019), https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html [https://perma.cc/Y2GC-E4JX].

D. External

Industry's appetite for data does not just affect our autonomy, dignity, and privacy. The personal data industrial complex also imposes significant externalities onto society and our environment that have little to do with data, information relationships, or corporate matters. If our privacy and human information framework is to be complete, lawmakers must also deal with personal data externalities in this constitutional moment. They vividly illustrate how the European data protection approach rooted in the FIPs cannot possibly address the full range of problems caused by data collection and processing.

To be clear, we are not arguing that lawmakers need to tackle all privacy, democracy, and environmental sustainability issues within one omnibus law. Such matters are far too vast, complex, and important to be handled within one framework. This is precisely why we are suggesting here that a legislative approach to regulating the digital economy will be incomplete unless it contemplates and attempts to reasonably mitigate the costs imposed by industry's appetite for personal data. This might involve creating rules that require companies to consider these externalities in their decision-making processes or for regulators and judges to consider these externalities when adjudicating issues of responsibility, fault, foreseeability, and harm. But it could also involve a series of concurrent initiatives that modify existing rules (inside and outside traditional privacy law) and perhaps entirely new laws that may or may not be tethered to privacy regulatory regimes.

1. Environmental Protection

From an existential perspective, protecting the environment is as important as any other goal of privacy law. Civil society cannot exist without a safe and sustainable environment. For all of its talk of the virtues of innovation, Silicon Valley is producing technologies that are ravaging our planet at an unprecedented rate.[338] Researchers have hypothesized that training a single AI model can emit as much carbon as five cars over their entire lifetimes.[339] Tech companies' strategy of "planned obsolescence"—creating phones and computers that expire after a few years in order to get us to buy more phones and computers—is de-

---

[338] *See supra* note 191 and accompanying text.

[339] *See, e.g.*, Karen Hao, *Training a Single AI Model Can Emit as Much Carbon as Five Cars in Their Lifetimes*, MIT TECH. REV. (June 6, 2019), https://www.technologyreview.com/s/613630/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/ [https://perma.cc/8DMW-A97F]; *see also* James Temple, *Bitcoin Mining May Be Pumping Out as Much CO2 Per Year as Kansas City*, MIT TECH. REV. (June 12, 2019), https://www.technologyreview.com/s/613658/bitcoin-mining-may-be-pumping-out-as-much-cosub2-sub-per-year-as-kansas-city/ [https://perma.cc/R3TF-KW4C] (documenting further deleterious effects of technology on the environment).

pleting our metal reserves and creating massive amounts of electronic waste.[340] Many people just throw their tech in the trash, or export it to create mountains of waste in the developing world. This waste is a direct and foreseeable consequence of the importance of technologies fueled by industry's desire for information.

Again, to be clear, we are not arguing that environmental law is part of privacy law and should be swallowed up by it. Rather, we are arguing that rules that protect our privacy also protect our environment, adding justification to these rules. Thinking too narrowly about privacy means we fail to appreciate the true nature and scale of the problems created by our digital transformation. These problems cannot be solved discretely, but must be solved holistically.

2. Mental Health

Our phones and computers are designed to be addictive.[341] That is because tech companies have powerful financial incentives to make sure you never put down your phone or log off your computer. The data spigot must keep flowing. Shoshana Zuboff calls this phenomenon "surveillance capitalism," and it is ruining us.[342] Our addiction to technology is harming our mental well-being, our social relationships, and even the very nature of what it means to be a human in our modern world.[343]

In an insightful piece, Nellie Bowles has noted how the proliferation of screens has turned human contact into a luxury good. Bowles explains:

> Life for anyone but the very rich—the physical experience of learning, living and dying—is increasingly mediated by screens. Not only are screens themselves cheap to make, but they also make things

---

[340] Julianne Tveten, *Who Will Clean Up Silicon Valley's E-Wasteland?*, FAST COMPANY (July 24, 2017), https://www.fastcompany.com/40443695/who-will-clean-up-silicon-valleys-e-wasteland [https://perma.cc/JF25-ZJ75].

[341] *See, e.g.*, NIR EYAL & RYAN HOOVER, HOOKED: HOW TO BUILD HABIT-FORMING PRODUCTS 2–3 (2014); Tristan Harris, *How Technology Is Hijacking Your Mind from a Magician and Google Design Ethicist*, MEDIUM (May 18, 2016), https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 [https://perma.cc/LEG8-UAMC].

[342] *See* ZUBOFF, *supra* note 186, at 9 (defining "surveillance capitalism" in highly pejorative terms).

[343] *See, e.g.*, CARR, *supra* note 184, at 63, 181–82 (describing "an erosion of skills, a dulling of perceptions, and a slowing of reactions" as a result of human dependence on machines, as well as social media's degradation of social relationships); CARR, *supra* note 190, at 16 (suggesting the internet is changing humans to be more machine-like); FRISCHMANN & SELINGER, *supra* note 185, at 10 (warning that technology has caused less developed memory, social relationships, and abilities to make decisions); SHERRY TURKLE, ALONE TOGETHER: WHY WE EXPECT MORE FROM TECHNOLOGY AND LESS FROM EACH OTHER 35–36 (2011) (documenting how machines replace people and social interactions between them).

> cheaper. Any place that can fit a screen in (classrooms, hospitals, airports, restaurants) can cut costs. And any activity that can happen on a screen becomes cheaper. The texture of life, the tactile experience, is becoming smooth glass.[344]

The problem is that to break our addiction, we have to have the means and capacity to do so. It is very difficult to rely upon simple willpower.[345] Bowles illustrates this point by explaining:

> The rich do not live like this. The rich have grown afraid of screens. They want their children to play with blocks, and tech-free private schools are booming. Humans are more expensive, and rich people are willing and able to pay for them. Conspicuous human interaction—living without a phone for a day, quitting social networks and not answering email—has become a status symbol.[346]

All this means that any comprehensive approach to privacy must also reckon with how industry's insatiable appetite for data contributed to the corrosion of our mental wellness and social fabric and created a new dimension to the long-recognized "digital divide" between rich and poor.[347] One start might be to target the manipulative tech designs that are meant to draw people in, similar to the legislation proposed by Senator Hawley.[348] Perhaps tech companies could be required to be loyal to users in a way that was mindful of mitigating harmful addictive behaviors and a more holistic view of users' well-being. Legislation could also include support and educational initiatives and mandates regarding healthy and limited engagement with screens and devices as well as targeting business models and the incentives companies have in the first place to extract every bit of personal information they can from every user. But any serious and

---

[344] Nellie Bowles, *Human Contact Is Now a Luxury Good*, N.Y. TIMES (Mar. 23, 2019), https://www.nytimes.com/2019/03/23/sunday-review/human-contact-luxury-screens.html [https://perma.cc/86L4-3RL8].

[345] *See* Jia Tolentino, *What It Takes to Put Your Phone Away*, NEW YORKER (Apr. 22, 2019), https://www.newyorker.com/magazine/2019/04/29/what-it-takes-to-put-your-phone-away [https://perma.cc/A8ZT-63HF] (suggesting that a lifestyle change, rather than mere willpower, is necessary to keep technologies from dominating our lives).

[346] Bowles, *supra* note 344.

[347] *See, e.g.*, Jakob Nielsen, *Digital Divide: The 3 Stages*, NIELSEN NORMAN GROUP (Nov. 19, 2006), https://www.nngroup.com/articles/digital-divide-the-three-stages/ [https://perma.cc/HU5L-DZS9] (discussing the "digital divide" between those who can afford technology and those who cannot, those who know how to use it and those who do not, and those who are empowered to take advantage of it and those who are not). Individuals who are unable to or unsure of how to fully utilize technology "remain at the mercy of other people's decisions." *Id.*

[348] *See* Press Release, *supra* note 325 (announcing a bill to curb addictive design of children's video games).

comprehensive approach to dealing with problems of privacy or the personal information industrial complex must consider mental health.

3. Digital Civil Rights

The internet makes speaking easy and anonymous. And in their quest for more data and greater interactions, social media platforms have sought to make it entirely "frictionless": so easy and costless we share intuitively and with almost no reflection.[349] And when speech becomes costless and consequence-free through anonymity, then harassment, bile, and abuse follow, largely against women, people of color, and other marginalized and vulnerable populations. This means that any holistic and layered approach must also reckon with the fact that when platforms optimize their data spigots by making interaction cost- and consequence-free, they facilitate harassment and abuse in ways that jeopardize what Danielle Citron has called our "cyber civil rights."[350]

Data-driven companies also threaten peoples' due process rights as algorithms make decisions about people's health, finances, jobs, ability to travel, and other essential life activities. Citron has argued for a "technological due process" that is ensured in these systems.[351] The modern discourse around this topic has centered around algorithmic fairness, transparency, and accountability. Any approach to data privacy that does not incorporate algorithmic accountability will be incomplete. Some early attempts at this kind of regulation have already been made. As Margot Kaminski and Andrew Selbst wrote, "[t]he bill, called the Algorithmic Accountability Act and introduced last month by Senator Ron Wyden, Senator Cory Booker and Representative Yvette D. Clarke, is a good start, but it may not be robust enough to hold tech companies accountable."[352] According to Kaminski and Selbst:

---

[349] *See, e.g.*, Richards, *supra* note 185, at 691 (discussing "frictionless sharing" and social media's capacity to allow users to automatically share virtually all of their activities online); *see also* William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 15–16 (same).

[350] *See* CITRON, *supra* note 299, at 56–72 (explaining the ways in which the internet promotes cyber-harassment and abuse, including the ease with which information is spread); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 65–66 (2009) (arguing that a majority of online harassment and attacks are aimed at women, racial and religious minorities, and gays and lesbians, in violation of their civil rights); *see also* Woodrow Hartzog & Evan Selinger, *Increasing the Transaction Costs for Harassment*, 95 B.U. L. REV. ANNEX 47, 47–51 (2015), http://www.bu.edu/bulawreview/files/2015/11/HARTZOG.pdf [https://perma.cc/AYB2-VEJT] (arguing that online harassment and abuse is simply too easy and that companies should take steps to increase transaction costs for communicating online).

[351] Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258 (2007).

[352] Margot E. Kaminski & Andrew D. Selbst, *The Legislation That Targets the Racist Impacts of Tech*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/tech-racism-algorithms.html [https://perma.cc/8SWL-Z9Y5].

> The proposed bill would be a significant step forward toward ensuring that algorithms are fair and nondiscriminatory. It requires certain businesses that use "high-risk automated decision systems" (such as those that predict a person's work performance, financial situation, or health) to conduct algorithmic impact assessments. This means they must, as Mr. Booker put it, "regularly evaluate their tools for accuracy, fairness, bias and discrimination."[353]

Nevertheless, the scholars argue the bill is lacking in enforcement provisions, missing meaningful public input, and does not mandate enough transparency to the public.[354]

4. Democracy

When the internet entered the public consciousness in the mid-1990s, it was touted as promising revolutionary empowerment of citizens and a new, more responsive democracy. Two decades later, we can see that some of those revolutionary promises were naïve at best. Digital technologies have certainly improved some dimensions of our democracy, but they have threatened others.[355] Although digital communications technologies have enabled anyone with access to the internet to speak directly to the world, they have also enabled new forms of electoral interference, voter suppression, and demagoguery.[356] Personal data can be used to drive friendly voters to the polls, to nudge unfriendly ones to stay home, or to influence voters in others ways, whether by the Obama campaign's data scientists in 2012, or by Cambridge Analytica to influence the outcome of the Brexit Referendum and the 2016 Presidential Election.[357] Naturally, this is a complex problem, and important First, Fourteenth, and Fifteenth Amendment considerations come into play when discussing electoral regulation. As we comprehensively confront the costs as well as the benefits of largely unregulated innovation around the exploitation of personal data, we must, however, always

---

[353] *Id.*

[354] *Id.*

[355] *See, e.g.*, CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA 259–62 (2018) (arguing that the internet can boost political accountability as well as help citizens to learn information and absorb a wide variety of political opinions, but that it also can brew polarization and easily spread fake information).

[356] *See* Danielle Keats Citron & Neil M. Richards, *Four Principles for Digital Expression (You Won't Believe #3!)*, 95 WASH. U. L. REV. 1353, 1376–77 (2018) (discussing how the internet and social media allowed for foreign money and fake news to have an impact on the 2016 U.S. presidential election).

[357] *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 428 (2014) (discussing the Obama campaign's use of big data to help in its fundraising and get-out-the-vote activities in 2012); Lapowsky, *supra* note 93 (documenting the role of Cambridge Analytica in the 2016 U.S. presidential election).

consider the risks and costs those technologies have imposed on our democratic practices and structures and seek to mitigate them in a way that is consistent with our constitutional traditions of democratic and republican self-government.[358]

This is why we conceive of the four privacy law dynamics (corporal, relational, informational, and external) as overlapping. Rules can affect multiple dynamics at the same time and one dynamic can be used to help justify rules focused on another. If privacy is important because it is necessary for human flourishing, our privacy-relevant rules should include a conceptualization for human flourishing that goes beyond autonomy and dignity derived from control over data and includes mental and social well-being as we interact and expose ourselves and our information to the world.

CONCLUSION

Privacy's constitutional moment is upon us, which means the legal, technical, and social structures governing the processing of human information are up for grabs. There is no avoiding the decision facing our society and our regulators; for the reasons we have explained in this Article, even a decision to do nothing at that national level will be consequential. In facing this constitutional moment, we must choose wisely as a society, but we fear that both the default option of GDPR-lite through national inaction but state action and the easy option of GDPR-lite through national action would be a mistake. America needs more than a watered-down version of the GDPR. In fact, it needs more than what all the existing models of data protection can give on their own. The advent of the constitutional moment means that right now the window is open for Congress to claim its identity. But it will not be open for much longer. We argue that a comprehensive model is the best path forward. This would include fundamental elements of data protection, such as default prohibitions on data processing and data subject rights, but it would not purely be defined by the limited data protection model. Instead, the comprehensive model could incorporate relational rules built around loyalty and care, and could be more layered and compartmentalized so that certain kinds of practices would be prohibited outright. The comprehensive model would address data externalities and not consider data processing to be an eternally virtuous goal.

To be sure, the comprehensive model we call for here is less refined, less compatible with international regimes, and less certain than the off-the-shelf default option of watered-down European-style data protection. But the comprehensive model responds to the problems at hand with tools that American law-

[358] *Cf.* SUNSTEIN, *supra* note 355, at 258–59 (arguing that the United States must figure out how to regulate speech—and by extension, the availability of information to the public while still maintaining its commitment to free expression and democratic self-government).

makers, regulators, and courts have regularly used. At the dawn of the industrial revolution, we had no idea what negligence, products liability, environmental protection, unfair and deceptive trade practices, or workplace safety was either. We will need to develop new and analogous but similarly imaginative and responsive concepts for the information age. We have bodies of doctrine, principles, and factors to guide us. As we confront privacy's constitutional moment, America's privacy policy should reflect that protecting privacy requires more than just protecting data. We need to protect people as well.