Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

A CONCRETE PROPOSAL FOR DATA LOYALTY

Neil Richards, Woodrow Hartzog** & Jordan Francis****

ABSTRACT

Congress and state legislators are finally experimenting with new privacy frameworks, rights, and duties to move past the thoroughly critiqued "notice and choice" model for data privacy. While many new privacy proposals seek a more fortified version of the fair information practices, some legislators have placed a duty of data loyalty at the heart of their proposed privacy bills. This is important because a duty of data loyalty has the potential to anchor American privacy law in a way analogous to how the European Union approach is grounded in fundamental rights of privacy and data protection.

Unfortunately, there remains some uncertainty about what exactly a duty of data loyalty should require. What is needed is a clear expression of what a practicable duty of data loyalty will do, why it will do it, and to what extent. This Essay supplies such an account, and argues that to be effective, data loyalty legislation must (1) impose a broad primary duty of loyalty that is clarified through specific subsidiary duties, (2) reflect a substantive commitment against self-dealing in relationships of trust, and (3) be compatible with existing data privacy frameworks to accommodate a diverse enforcement strategy and generate political support.

To advance this approach, we offer as proof of concept a model statute for a duty of data loyalty — one that is designed to limit wrongful self-dealing with a robust "best interests" rule supplemented by specific duties with clear boundaries. The goal of this model legislation is to serve as a guide for legislators who seek to place data loyalty as the foundation of a U.S. approach to privacy. Instead of creating new legislative language from scratch, our model statute incorporates and strengthens many relevant existing data privacy rules under the unifying principle of keeping companies from betraying those who trust them with their data and online experiences. Our purpose in building

* Koch Distinguished Professor in Law and Director, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis; Affiliated Fellow, Yale Information Society Project; Faculty Associate, Berkman Klein Center for Internet & Society at Harvard University; Affiliate Scholar, Stanford Law School Center for Internet & Society.

** Professor of Law, Boston University; Fellow, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis; Faculty Associate, Berkman Klein Center for Internet & Society at Harvard University; Affiliate Scholar, Stanford Law School Center for Internet & Society.

*** Legal Research Fellow, 2022–23, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis.

on existing rules and bipartisan proposals is to demonstrate the practical appeal and feasibility of our data loyalty framework.

TABLE OF CONTENTS

I. INTRODUCTION

For privacy scholars, the last few years have seen a flurry of legislative activity at the state level.[1] Several states have joined the fold by enacting comprehensive data privacy laws.[2] Many more bills, each with their own particular provisions, have been introduced at the federal, state, and local levels.[3] Even more encouraging, Congress and state

1. *See* Anokhy Desai, *US State Privacy Legislation Tracker*, IAPP (June 30, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/HL85-LCDC].

2. *Id.* (showing that Indiana, Iowa, Montana, Tennessee, and Texas have passed "comprehensive consumer privacy" laws and that Oregon has passed such a law which has yet to be signed).

3. *See* Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, IAPP (May 2023), https://iapp.org/resources/article/us-federal-privacy-legislation-tracker [https://perma.cc/MMH8-82HA] (covering privacy legislation introduced in the 118th Congress in the areas of

legislatures are finally experimenting with new privacy frameworks, rights, and duties to move past the thoroughly critiqued "notice and choice" model for data privacy. While many new privacy proposals seek a more fortified version of the fair information practices, some legislators have placed a duty of data loyalty at the heart of their proposed privacy bills.[4] This is important because a duty of data loyalty has the potential to anchor American privacy law in a way similar to how the European Union's approach is grounded in fundamental rights of privacy and data protection.

Unfortunately, there remains uncertainty about exactly what a duty of data loyalty should entail. Like the academic theories that have inspired it, U.S. legislators have been inconsistent in proposing a duty of data loyalty. Some data loyalty proposals are too broad while others are too narrow. Some have harm requirements. Others do not. Some are labeled as a duty of loyalty, but more closely resemble a duty of care. What is needed is a clear expression of what a practicable duty of data loyalty will do, why it will do it, and to what extent. In this Essay, we offer such an account. We argue that to be effective, data loyalty legislation must (1) impose a broad primary duty of loyalty that is clarified through specific subsidiary duties, (2) reflect a substantive commitment against self-dealing in relationships of trust, and (3) be compatible with existing data privacy frameworks to accommodate a diverse enforcement strategy and generate political support.

This Essay offers as proof of concept an annotated model statute for a duty of data loyalty — one that is designed to limit wrongful self-dealing with a robust "best interests" rule supplemented by specific duties with clear boundaries. This model legislation draws from the theories developed in the academic literature as well as established rules and approaches in U.S. and E.U. data privacy and data protection legislation.[5] The goal of this model legislation is to serve as a guide for

consumer/individual privacy, health privacy, financial privacy, children/education privacy, and government restrictions and obligations).

4. *See, e.g.*, New York Privacy Act, S. 365, 2023–2024 Leg. (N.Y. 2023), https://legislation.nysenate.gov/pdf/bills/2023/S365; Data Care Act of 2023, S. 744, 118th Cong. (2023); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

5. A robust body of scholarship concerning information fiduciaries has been developed in recent years. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11 (2020); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/3RR5-GHB5]; ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 8 (2018); Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 591 (2015); Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RSRV. L. REV. 193, 195–96 (2016); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 113 (2019); Jonathan Zittrain, *Engineering*

legislators who seek to place data loyalty as the foundation of a U.S. approach to privacy. Instead of creating new legislative language from scratch, our model statute incorporates and strengthens many existing data privacy rules with the goal of preventing companies from betraying those who trust them with their data and online experiences. Our purpose in building on existing rules and bipartisan proposals is to demonstrate the practical appeal and feasibility of data loyalty frameworks.

Our Essay proceeds in three parts. First, we offer a brief introduction to the concept of data loyalty, explaining the need for trust-building duties in privacy law. Second, at the heart of the Essay, we highlight the core concepts at the heart of the model statute, explaining specific drafting decisions for important concepts like prohibitions on cross-context behavioral advertising and manipulative design. This Part introduces core elements of the model data loyalty legislation and identifies the inspirations and sources of the model language. For example, this model incorporates established rules like data minimization and prohibitions on abusive trade practices as well as some language and structure from bipartisan data privacy bills. The third part of the Essay is the model statutory text. We offer an abridged version here in the Appendix. However, the full text of the model legislation is updated and preserved online, accessible by a permanent hyperlink provided here and at the end of this Essay.[6]

The most important element of our model state statute to understand is that it has two layers. The top layer is a broad primary duty of loyalty that prohibits actions that conflict with a trusting party's best interests. The second layer of a duty of loyalty takes the form of subsidiary duties which are both more specific and more restrictive. The

---

an Election, 127 HARV. L. REV. F. 335, 339–40 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1058 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 1 (2018); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today — and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game [https://perma.cc/5HE7-LRSV]; Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 446–47 (2001); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102–04 (2006); Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75, 79 (2019); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 613–14 (2015); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, J. CORP. L. 143, 144–45 (2020); Claudia Haupt, *Platforms As Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 35 (2020). For a criticism of information fiduciary proposals, see Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 499–501 (2019).

6. Neil M. Richards, Woodrow Hartzog & Jordan Francis, Model Duty of Data Loyalty Act (Dec. 12, 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4628996 [https://perma.cc/3SUX-K6AF].

model statute also incorporates individual data rights, a concrete private right of action, and other features necessary for a comprehensive yet flexible data privacy law. This model statute shows how concepts of trust, loyalty, and relational vulnerability can revolutionize our historically tepid data protection frameworks without upending the entirety of existing U.S. privacy law. Now that lawmakers have demonstrated a willingness to make a duty of loyalty the foundation of an omnibus privacy law, the time is right to take the theory of loyalty seriously and build it into viable legislation.

II. THE NEED FOR A DUTY OF DATA LOYALTY

American privacy law lacks identity. Even lawmakers' most-touted new omnibus rules like the California Consumer Privacy Act ("CCPA")[7] are diluted versions of the E.U.'s robust General Data Protection Regulation ("GDPR").[8] Other adopted state laws have been even weaker and would appear to do very little to restrain problematic data practices. More importantly, however, the European-style data protection approach is ill-suited for the United States, which lacks Europe's constitutional commitments to privacy and data protection as a fundamental human right.[9] As we have argued elsewhere, the essential ingredient that makes the GDPR work is that it rests upon a foundation of two fundamental rights: privacy and data protection. These principles give the GDPR focus and power, but legislative regimes that do not rest upon an equivalent foundation are far less likely to be effective.[10]

U.S. lawmakers' attempts to shoehorn privacy protections into consumer protection law have resulted in a failed notice-and-choice regime that too often provides only fictional notice and illusory choice.[11] Moreover, even an ideal notice-and-choice framework would do little to mitigate the massive power imbalances created by the modern data industrial complex and the abuses that follow as a result.[12] The challenge of meaningfully protecting Americans' privacy has grown tougher in recent years as recent Supreme Court decisions have made

7. CAL. CIV. CODE § 1798.100 (West).

8. Council Regulation 2016/679, 2016 O.J. (L 119).

9. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1727–33 (2020).

10. *Id.*

11. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1476–91 (2019); *see also* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 975, nn.103–04 (2017).

12. Hartzog & Richards, *supra* note 9, at 1745–46. *See generally* Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018) [hereinafter Hartzog, *Idealising Control*]; NEIL RICHARDS, WHY PRIVACY MATTERS (2022); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

it more difficult for privacy plaintiffs to satisfy Article III standing requirements,[13] limiting the ability of private litigants to obtain redress for violations of their privacy rights.

In the absence of meaningful protections, commercial surveillance has flourished and become the dominant business model of the Internet. We have explained elsewhere that "[t]he [I]nternet of the 2020s certainly provides many helpful services, but it has also become the greatest assemblage of corporate and government surveillance in human history."[14] This surveillance economy is marked by rampant self-dealing and opportunism. Powerful, information-intensive firms now mediate our personal and commercial experiences to their financial advantage and at our peril. Our relationships with these companies are plagued by stark information asymmetries and power differentials. We have no choice but to entrust our data with these firms who hold the power to shape what we see, how we interact, which options are available to us, and how we make decisions. That power imbalance leaves us vulnerable and erodes trust between us and these companies. Companies entrusted with our data engage in surreptitious data collection, profile and sort us, nudge us into acting in ways which disproportionately benefit them, share our data with shadowy networks of third parties, and employ lax data security practices which expose us to risks of future harm.[15]

To establish healthy information relationships in which everyone benefits, it is crucial to restore confidence in the companies with whom we share our data. We need assurance that these companies won't prioritize their own interests over ours to our detriment and that they will not betray us. Lawmakers must make these companies trust-*worthy*. Trust empowers people to invest in companies and share their data and experiences, safe in the knowledge that they won't be manipulated, deceived, or treated unfairly. Without laws mandating loyalty and care, the modern marketplace becomes a breeding ground for market failures that are harmful to consumers, competition, and commerce.

American privacy law needs a new identity if we want to prevent and remedy the kinds of privacy betrayals that have come to define our everyday existence. We have explained elsewhere why lawmakers looking to improve American privacy law and foster trust in digital markets should impose a duty of data loyalty on companies with respect to the human information they hold and the technological services they

13. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330 (2016); TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

14. Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 964 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*].

15. *Id.* at 970–77.

design.[16] Requiring the companies that collect and process our personal data and design our digital services to act in our best interests offers the best chance to break the cycle of self-dealing that is ingrained into the current Internet. Lawmakers and regulators within the United States and abroad are experimenting with a duty a loyalty for data privacy,[17] but these proposals have been inconsistent.[18] Some have harm requirements, while others focus narrowly on collection or use.[19] What is needed is a clear expression of what a practicable duty of data loyalty will do, why it will do it, and to what extent. This Essay thus takes the concept of a duty of data loyalty and makes it actionable by providing a model statute which could be enacted by state lawmakers.

III. FEATURES OF THE DUTY OF LOYALTY AND DRAFTING DECISIONS EXPLAINED

Attached as an Appendix to this Essay is a model state statute that would implement a duty of data loyalty. But rationales and the purposes can be hard to infer from bare statutory text. In this Part, we explain our most important drafting decisions and identify where and why we borrowed from existing legislation, bills, and other model acts.

---

16. *See generally* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 457 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1198 (2017) [hereinafter, *Privacy's Trust Gap*]; Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579, 582 (2017) [hereinafter Hartzog & Richards, *Big Data Research*]; Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?,* 6 EUR. DATA PROT. L. REV. 492 (2020) [hereinafter Richards & Hartzog, *Relational Turn*]; Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022) [hereinafter Hartzog & Richards, *Surprising Virtues*]; Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022) [hereinafter Hartzog & Richards, *Legislating Data Loyalty*]; Cordell Inst., Comment on Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 47–59 (Nov. 21, 2022) https://www.regulations.gov/comment/FTC-2022-0053-1071 [https://perma.cc/42XK-T3VM].

17. *See, e.g.*, New York Privacy Act, S. 365, 2023–2024 Leg. (N.Y. 2023), https://legislation.nysenate.gov/pdf/bills/2023/S365 [https://perma.cc/RSQ4-PTGF]; DATA PROT. COMM'N OF IR., CHILDREN FRONT AND CENTRE: FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING (Dec. 2021), https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf [https://perma.cc/F6H7-CR5K] (identifying a "zero interference" principle prioritizing the best interests of the child).

18. Woodrow Hartzog & Neil Richards, *We're So Close to Getting Data Loyalty Right*, IAPP (Jun. 14, 2022), https://iapp.org/news/a/were-so-close-to-getting-data-loyalty-right [https://perma.cc/K9F2-E9HB].

19. *Id.*

A. Legislative Inspiration: Building upon the ADPPA

The general structure of our model statute was shaped significantly by the American Data Privacy and Protection Act ("ADPPA"),[20] a federal bill introduced in 2022. The introduction of the ADPPA and its success in getting out of committee was a surprising event that occurred during this project, even though it was not ultimately passed by Congress. One notable and highly relevant aspect of the ADPPA was its embrace of a limited duty of loyalty.[21] Title I was called the "Duty of Loyalty," and, although it did not actually include a primary duty of loyalty, like a broad "no conflict" rule, it included protections, like a robust data minimization rule, which were loyalty-based.[22] It can be loyal, for example, for a company to collect only the personal data necessary to serve its customers, rather than collecting whatever personal data might benefit the entity whether now or down the road. In recognition of the comprehensive nature of the bill, its commitment to substantive rules over mere procedure and transparency, its bipartisan support, its consistency with a loyalty framework, and its use of loyalty language, we made the decision to use the ADPPA as a foundation upon which to build our model statute — copying some provisions word for word and adjusting others to be harmonious with a general duty of loyalty.

To be clear, the ADPPA, as introduced, is not our ideal privacy statute; there are some parts of it we seek to make more robust in our model statute. But we chose to use the ADPPA instead of starting from scratch because we are not proposing our ideal statute, which we have generally developed elsewhere.[23] Rather, in response to scholars' and policymakers' questions about the feasibility of a data loyalty law, our goal in this Essay is to demonstrate data loyalty's potential political appeal by showing how it might be concretely and practically implemented alongside existing frameworks.[24] This approach has several benefits. First, the language and general structure that we borrow from the ADPPA have already undergone a multi-stakeholder process, surviving a committee markup and garnering considerable bipartisan support. Second, borrowing already vetted language provides greater certainty for lawmakers, which would not be the case if we were to start

20. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

21. Senator Schatz — whose own proposed data privacy bill, the Data Care Act, included a duty of loyalty — advocated for the inclusion of a duty of loyalty in the ADPPA. Letter from Senator Brian Schatz to Representatives Cantwell, Pallone, Wicker & McMorris Rodgers (Jun. 1, 2022) (on file with authors); *see also* Data Care Act of 2021, S. 919, 117th Cong. (2021).

22. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

23. *See* Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16.

24. *See* Hartzog & Richards, *Surprising Virtues*, *supra* note 16 (responding to questions about the feasibility and desirability of data loyalty rules).

from scratch. Our biggest departure from the ADPPA, however, is the addition of a two-layer of a duty of loyalty, as explained below.

While the ADPPA was our most significant source of inspiration and language, we also drew upon concepts and language from other enacted laws and bills, such as the Data Care Act of 2021,[25] the California Consumer Privacy Act as amended by the California Privacy Rights Act,[26] the GDPR,[27] the Digital Consumer Protection Commission Act,[28] the proposed Massachusetts Information Privacy Act,[29] the Dodd-Frank Wall Street Reform and Consumer Protection Act,[30] and other sources, including some draft bills currently under consideration by lawmakers.

We also consulted other organizations' model statutes as a way of consensus building, to make sure that some collective wisdom about statutory language in privacy was reflected in our loyalty approach. In particular, we relied heavily on the Electronic Privacy Information Center's ("EPIC's") well-developed "State Data Privacy and Protection Act," a modified version of the ADPPA designed to be enacted by state lawmakers in the absence of a federal data privacy law.[31]

B. High-Level Overview

The model statute is a cross-sectoral consumer privacy bill applicable to most non-governmental organizations of a certain size (i.e., not small businesses). At a high level, there are three main components of the statute: prohibitions on self-dealing, individual data rights, and risk management.

We have previously summarized the concept of data loyalty as "the simple idea that the organizations we trust should not process our data

---

25. Data Care Act of 2021, S. 919, 117th Cong. (2021).

26. CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2023).

27. Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1 [hereinafter GDPR].

28. Digital Consumer Protection Commission Act, S. 2597, 118th Cong. (2023), https://www.warren.senate.gov/imo/media/doc/Tech%20Bill_Full%20Text.pdf [https://perma.cc/P69Z42FD].

29. Massachusetts Information Privacy Act, S. 46, 192 Leg. (Mass. 2021).

30. Dodd-Frank Wall Street Reform and Consumer Protection Act § 1031, 12 U.S.C. § 5531.

31. The authors would like to extend their gratitude to EPIC and Caitriona Fitzgerald in particular for their efforts in creating the State Data Privacy and Protection Act. The model data loyalty act will be released as both federal and state versions. EPIC's model State Data Privacy and Protection Act set a blueprint to follow in adapting the model federal data loyalty act to the state data loyalty act. For EPIC's proposed statute, see Caitriona Fitzgerald, *A Proposed Compromise: the State Data Privacy and Protection Act*, EPIC (Feb. 22, 2023), https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act [https://perma.cc/H2V5-VXAD].

or design their tools in ways that conflict with our best interests."[32] Therefore, although we often talk about loyalty in positive terms (i.e., to act in a way that is loyal), the statute actually follows the structure of many fiduciary laws by implementing loyalty as a negative "no conflict" rule, prohibiting acts or practices that conflict with the best interests of trusting parties. Thus, as a formal matter, we propose a negative duty not to betray, rather than a broad affirmative duty of loyalty.

This duty not to betray is implemented through a layered process that we call the "loyalty two-step." First, covered entities (the organizations that collect, process, or transfer covered data) are subject to a primary duty of loyalty. This primary duty is a catch-all rule that prohibits disloyal behavior. It is broad and flexible, but it is also relatively weak. Second, the primary duty is reinforced with stronger subsidiary duties of loyalty. These rules are more specific, context-dependent, and offer additional protections in specific contexts in which betrayal is most likely to be substantial and harmful. Like the primary duty, these subsidiary duties should also be interpreted according to the general "no conflict" duty. We have organized these subsidiary duties into conceptual categories that track aspects of information relationships most susceptible to dealing by the more powerful party, such as data collection, personalization, gatekeeping, influencing, and mediation. The subsidiary duties include established rules like data minimization and purpose limitation, chain-link contractual protections for downstream disclosures of covered data, new prohibitions like limits on targeted and cross-context behavioral advertising, and bans on unfair, deceptive, and abusive design decisions. The statute delegates rulemaking authority for the creation of new subsidiary duties, including new rules over time as new threats to loyalty emerge in changed technological, social, and economic circumstances.

The primary and subsidiary duties of loyalty together comprise the substantive core of the statute. Although the aim of substantive data privacy rules is to shift the focus away from privacy law's historical focus on atomistic privacy rights and privacy self-management, the statute nevertheless incorporates some traditional individual data subject rights. These rights have several virtues, such as enabling people to ensure that companies are complying with their duty loyalties as well as appealing to common and historical understandings of why privacy matters.[33] However, we do not believe that a privacy law that rests

32. Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 359 (2022).

33. *See* Margot E. Kaminski, *The Case for Data Privacy Rights (Or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 386 (2022) ("Individual rights are not sufficient by themselves, but they are necessary for data privacy. These rights reflect common and historic understandings of data privacy and why it matters to many. They instantiate the

entirely upon affirmative rights that consumers must exercise time after time for them to work would be effective. An effective privacy law should protect consumers no matter what they choose, which is the virtue that centering a duty of loyalty offers. Nevertheless, some individual rights can be important, and we have adopted them here. Similarly, the statute also adopts other historical features of data privacy laws, including procedural protections like data privacy by design and impact assessments, data security obligations, and corporate structure requirements such as the appointment of a privacy protection officer. While companies often dilute procedural protections to weaken their effectiveness,[34] we think that such rules can complement the robust data loyalty duties and prohibitions in the model statute as a meaningful way to hold companies accountable for acting in our best interests.

The statute is built around the concept of *relationships* and *relational duties*. This choice reflects the fact that relationships in which personal information is exchanged are (to our minds) (1) the basic building block of our digital economy, (2) the site in which the most substantial data harms can be created, and (3) the logical place to install consumer- and citizen-protective duties and regulations. Although we define the term "covered entity" broadly to include non-governmental organizations engaged in the collection, processing, or transfer of covered data, the primary duty of loyalty is owed only to trusting parties, those individuals who entrust a company with their covered data or mediated experience. Thus, the primary duty of loyalty focuses on first-party relationships, and only a trusting party can sue for a violation of the loyalty duties. Importantly, though, there are still obligations that apply to covered entities that are not contingent upon direct relationships with trusting parties: for example, the obligation of reasonable data security practices. However, by limiting our model statute to relationships, we recognize that additional rules would be required to fully respond to privacy threats by third parties like data brokers and ad networks that have no direct relationship to the people whose data they are using.[35] That said, to the extent that such business models often piggyback upon relationships between consumers and companies to extract data from trusted companies, we believe that our relational approach would place significant practical limits on data grabs of this sort that

---

dignitary and autonomy theories of privacy that form the basis of privacy rights around the world. They may help insulate data privacy laws from First Amendment challenges. And they also serve an overlooked role as a component of governance — a necessary aspect of institutional design.").

34. *See* ARI WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021) (exploring how companies use managerialist strategies to dilute procedural privacy protections).

35. *See* Hartzog & Richards, *supra* note 9; Richards & Hartzog, *Relational Turn*, *supra* note 16.

are unconsented, secret, and/or buried in the fine print of privacy policies and terms of service.

Because this Essay proposes a model statute, some of the longer and more complex aspects found in other privacy laws have been moved in our model to rulemaking provisions or proposed legislative findings.[36] After workshopping several longer and more complex drafts, we decided that a shorter statute would be more flexible and adaptable to future developments, and we made the decision to abbreviate some portions of the statute that were less central to articulating the core loyalty duties. For example, specific data security obligations and transparency requirements have been moved to rulemaking, while proposed conflict resolution principles for covered entities to navigate conflicts of interest between different groups of trusting parties have been moved to proposed legislative findings. [37]

C. The Duty of Loyalty

We believe that an effective data loyalty model requires a two-tiered approach.[38] This approach, which we call the "loyalty two-step," is the core of our proposal. The first step is for lawmakers to articulate a broad, primary duty of loyalty which serves as a catch-all for disloyal behavior.[39] That primary duty should be supplemented by the second step: subsidiary duties of loyalty that are more specific, sensitive to context, and controlling when applicable.[40]

1. Primary Duty

The keystone of our model statute is a catch-all primary duty of data loyalty. Framed as a "no conflicts" rule, this duty would permit self-dealing data practices and technological design choices unless and until they conflict with a reasonable trusting party's best interests implicated by their exposure:

---

36. Legislative findings present an opportunity to include principles that should inform the reading of the statute but which, for a variety of reasons, may overcomplicate the statute by direct inclusion. *See* Cameron Kerry & John B. Morris, *Legislative Findings Will Be Important to Federal Privacy Legislation*, LAWFARE (Dec. 14, 2020), https://www.lawfaremedia.org/article/legislative-findings-will-be-important-federal-privacy-legislation [https://perma.cc/FY73-98U2] (discussing how legislative findings present an opportunity to proclaim the significance of privacy and to inform judges, regulators, and lawyers applying a privacy law).

37. *See infra* Section III.C.1.e; *see e.g.*, Appendix sec. 21(a)(6).

38. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 371.

39. *Id.* at 370.

40. *Id.*

> A covered entity owes a duty of loyalty to all trusting parties. This duty is defined by the extent of a reasonable trusting party's exposure.
>
> Under this duty, a covered entity shall not collect, process, or transfer covered data in a way that conflicts with the best interests of trusting parties; or design or implement an information technology in a way that conflicts with the best interests of trusting parties.
>
> A covered entity's acts or practices conflict with the best interests of trusting parties when either the collection, processing, or transfer of covered data or the design or implementation of an information technology results in a disproportionate allocation of benefits in favor of the covered entity relative to the degree of individual and collective risk posed to the trusting parties.[41]

The key aspects of the duty, which the statute explicitly addresses, are: *who* it applies to (covered entities), *how* it is defined (to the extent of a trusting party's exposure) and *what* it requires (covered entities to refrain from acting in ways that conflict with the best interests of reasonable trusting parties). This duty frames best interests as a consideration of the relative allocations of benefits and risks within an information relationship.

a. Covered Entities and Trusting Parties

The model statute prohibits covered entities from acting in ways that conflict with the best interests of trusting parties. Adapted from the ADPPA, "covered entity" is defined broadly as any entity or any person, other than an individual acting in a noncommercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data.[42] There are four categories of entities that the model statute would not apply to: government entities, people or entities acting as a service provider to government entities, certain organizations that provide assistance on missing and exploited children issues, and small businesses.[43]

41. *Infra* Appendix sec. 3(a).
42. *Infra* Appendix sec. 2(7).
43. *Infra* Appendix sec. 2(7).

Rather than talking about "users," "consumers," or "data subjects," this statute protects trusting parties, defined as individuals who entrust their personal data and mediated experiences with a covered entity.[44]

b. Best Interests

The duty of loyalty prohibits covered entities from engaging in data practices that conflict with the best interests of reasonable trusting parties. This duty would not generally prohibit covered entities from acting in their own self-interest; rather, it prohibits those self-interested actions that come at the detriment of trusting parties:

> A covered entity's acts or practices conflict with the best interests of trusting parties when either the collection, processing or transfer of covered data or the design or implementation of an information technology results in a significantly disproportionate allocation of benefits in favor of the covered entity relative to the degree of individual and collective risk to the trusting parties.[45]

This framing of best interests captures two aspects of self-dealing that should be mitigated. Trusted parties often have the ability to hide both the existence and degree of benefit they are deriving from requests for personal information and design decisions.[46] People might assume that certain services or options are being made primarily for their benefit, when in fact the opposite is true. The extent of people's exploitation is not often clear until the benefits of an exposure are compared. A situation where trusted parties are being enriched significantly more than exposed people is a signal of exploitation. Often people will be given a fig leaf — a coupon, a trinket, "personalization," or a *de minimis* feature in exchange — for a significant exposure of data, time, or attention that is essential to a company's business model. By itself and in a normal commercial relationship, this might be acceptable. However, when people are extremely vulnerable, trusting, and shouldering most of the risk in an exchange, this imbalance makes the trusted party's actions disloyal.

A stricter form of this principle is embodied in the data minimization requirement.[47] If the collection, processing, or transfer of personal data is truly necessary to provide a product or service requested by an individual, then there should be few concerns about a disproportionate

44. *Infra* Appendix sec. 2(45).
45. *Infra* Appendix sec. 3(a).
46. Hartzog & Richards, *Duty of Loyalty*, *supra* note 14, at 979.
47. *See infra* Section III.C.2.a.

allocation of benefits. The first prong (the allocation of benefits) thus targets only excessive data extraction and similar practices. The second prong (the degree of risk to trusting parties) requires covered entities to weigh the risks that a trusting party faces as a result of data practices. For example, certain data practices might, if implemented without care, expose trusting parties to risks of stalking or identity theft. The second prong places the onus on covered entities to ensure that the products or services they are selling are safe and reliable.

Requiring covered entities to avoid creating a disproportionate risk of harm or loss raises the question of which negative outcomes should be considered. To ensure that a broad scope of potential privacy harms is being weighed, the statute defines harm in accordance with the broad taxonomy of privacy harms created by Danielle Citron and Daniel Solove, including physical harm that results in bodily injury or death; economic harm, including time spent protecting oneself from risk of harm due to the breach or misuse of covered data; reputational harms affecting standing in the community, business opportunities, or employment; psychological harm in the form of emotional distress or disturbance that have long been recognized in privacy law; various autonomy harms such as coercion, manipulation, failure to inform, thwarted expectations, lack of control, and chilling effects; discrimination harms that entrench inequality or disadvantage people based on certain characteristics or affiliations; and relationship harms.[48] We include the word "loss" in this definition to cover detrimental outcomes that often fall outside the standard range of privacy harms, such as attention theft, loneliness, and opportunity costs.[49] We also included language sensitive to both individualized risks as well as more collective, societal risks that are harder to measure at the individual level, such as disparate impacts, corrosion of public discourse, and barriers to civic participation.

c. Exposure

One of the common criticisms directed against duty of data loyalty proposals is that the duty is too vague. To address this, the statute clarifies that the scope of the duty is limited to the extent of a trusting party's exposure.[50] Exposure is defined as:

> [T]he degree to which a trusting party has made themselves vulnerable to harm or loss to a covered entity

48. *Infra* Appendix sec. 2(24); *see also* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830–59 (2022).

49. Attention theft refers to design choices that optimize for engagement by exploiting cognitive biases and behavioral science.

50. *Infra* Appendix sec. 3(a).

> with their data and mediated experiences. A trusting party's exposure when interacting with an information technology includes what a covered entity can see or knows about that trusting party, which choices and options are available to trusting party, and what the trusting party can see or know about the covered entity. A covered entity shall assess a trusting party's exposure by considering the nature and length of the relationship between the parties, the nature and sensitivity of the data collected, processed, or transferred, and the nature and sensitivity of the choices and signals mediated or controlled by the covered entity. For the purposes of this section, vulnerability to harm or loss includes, but is not limited to, vulnerability to [enumerated privacy harms derived from the Citron-Solove taxonomy identified above as well as loss].[51]

Tying the duty of loyalty to exposure is an attempt to limit the scope of the duty to the context of the information relationship. For example, Google does not have an automatic obligation to remind all Android users to brush their teeth before bed because that has no connection to the information relationship the company forms with its users. On the other hand, this obligation might arise for a dental health app, depending upon representations made and the function of the app's relationship with users. But both the dental health app and Google would have an obligation not to sell trusting parties' data to insurers and others who might use that personal data to the trusting party's detriment. Data practices and information technologies should improve the lives of humans, and doing so requires that humans can trust companies deploying such practices and technologies. Imposing a duty of data loyalty that is limited in scope by the trusting party's exposure fosters such trust by encouraging humans to adopt such technologies and disclose their data, safe in the knowledge that they will not be betrayed. In this way, the level of protection for the individual is directly proportionate to the level of her exposure: you get to hold my data, but you can't use it to betray me.

d. Reasonable Trusting Parties

Another common criticism of data loyalty proposals is that companies are not equipped to know what is in the subjective best interests of every individual trusting party. To address this concern, the model statute adopts both a "reasonable person" standard and a collective best

51. *Infra* Appendix sec. 2(21).

interests approach.[52] Introducing a reasonableness standard will help covered entities better determine the scope of their duties and inject a normative element into their analysis,[53] and the collective interests approach will help lawmakers to move past privacy law's overly individualistic focus and to combat systemic harms.[54]

e. Conflicts

Implementing a duty of loyalty with a best interests standard creates a potential problem if there are conflicting interests between different trusting parties. Limiting the duty to collective interests reduces the likelihood of conflicts between trusting parties,[55] but it does not eliminate that risk. Certain data practices might implicate different groups of reasonable trusting parties differently, particularly where intersecting identities create a different benefit and risk calculus for one group as opposed to another.[56] To remedy this problem, we have attempted to incorporate intersectional considerations into the duty of loyalty. When a conflict exists between the best interests of different subsets of reasonable trusting parties, a covered entity should prioritize the best interests of the groups with the greatest degree of vulnerability. To determine which groups of trusting parties have the greatest degree of vulnerability, a covered entity should evaluate how the act or practice in question will create different benefits or risks for trusting parties as a result of race, color, religion, national origin, sex, disability, or other protected characteristics. In the absence of disproportionate vulnerabilities, those bound by a duty of loyalty should avoid preferential treatment. If implemented correctly, conflict resolution provisions like these should encourage covered entities to be proactive in their efforts to identify and reduce human bias and discrimination. This hierarchy of interests is not included in the text of the statute itself but instead in the proposed legislative findings.[57]

2. Subsidiary Duties

The second step of implementing a duty of loyalty is identifying the contexts for strong subsidiary duties which reinforce and support

52. *Infra* Appendix sec. 3 (referring to "reasonable trusting parties"). For an overview of the collective best interests approach, see Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 374–75.

53. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 374.

54. *Id.*

55. *Id.*

56. *See* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 132 YALE L.J.F. 907, 928–33 (2022).

57. These are not included in the Appendix to this Essay, but they are available on the permanent online version of the statute.

the primary duty. Targeted at different aspects of the information relationship, the subsidiary duties either create affirmative obligations to take certain loyal actions or prohibit certain disloyal acts or practices. Many of the subsidiary duties we identify come from pre-existing privacy rules and best practices, like data minimization or individual data rights, which are consistent with a loyalty framework. This process should result in a set of rules that is greater than the sum of its parts. The specificity of the subsidiary duties will create more certainty and less room for dilution by covered entities. The primary duty will act as an animating principle, interpretive guide, and catch-all for disloyal behaviors that were unforeseen at the time of drafting. Because the primary duty acts as a baseline standard, the model statute can evolve as technologies, contexts, and business models evolve. However, for the duty of loyalty to remain vital, updates to the subsidiary duties will be necessary over time. The different areas in which subsidiary duties are imposed include collection, personalization, gatekeeping, influencing, and mediation.

a. Collection

Trusting parties become exposed the moment that a trusted party invites disclosure and collects personal information. It is imperative that the duty of loyalty attach at that moment in order to protect trusting parties from disloyal data collection, as well as to ensure that protections to the individual continue through the life cycle of the data.[58] The unnecessary collection of personal data results in a disproportionate allocation of benefits and risks to the detriment of trusting parties. The trusted party benefits as it gathers lucrative data that can be monetized in the present or future, but few to no benefits flow to the trusting party whose interests are not furthered by such collection. The trusting party is also saddled with a variety of risks when data is unnecessarily collected, including data breach, manipulation, exposure, and a host of other potential data harms. Unnecessary and disproportionate data collection is therefore disloyal. (In this respect, our model not only converges upon data protection law's familiar mandate of data minimization but also offers a coherent justification for why data maximization is problematic.) Our model statute includes a robust version of data minimization based on functionality. A covered entity acts loyally when collecting, processing, or transferring covered data that is strictly necessary to provide or maintain a specific product or service requested by the trusting party to whom the data pertains or to affect a

58. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 379.

legitimate interest of the covered entity.[59] Our data minimization rule is adapted from language in the ADPPA, but it replaces the ADPPA's proposed whitelist with a flexible legitimate interests exception to be clarified in regulations and through litigation. We did this because statutory specifications of exceptions run a greater risk of becoming obsolete quickly as technology and business models advance rapidly.

Here, the primary duty of loyalty serves as a value-laden baseline and backstop that informs what data collection is reasonably necessary and proportionate.[60] Our legislation is also consistent with specific prohibitions on the collection of certain kinds of data. These kinds of prohibitions, such as a contextual prohibition on the collection of geolocation or biometric data, are justified in circumstances where trusted parties are so powerful and the incentive for conflicted self-dealing is so great that loyalty requires the trusted entity to "tie themselves to the mast" and refrain from collecting the information at all. In other words, in certain contexts, the mere existence of data would be so tempting as to make betrayal inevitable and thus disloyal. Our duty makes the self-binding in the interests of loyalty mandatory to protect individuals.

In addition to prohibiting exploitative data extraction, a secondary benefit of a robust data minimization rule is that it will help bridge the gap between privacy and security.[61] Data minimization is a fundamental element of good data security because unnecessary and disproportionate data collection magnifies the consequences of data breach and gives fraudsters personal information which can be used to carry out subsequent attacks.[62] Thus, a robust data minimization rule can also bolster a trusted party's duty of loyal gatekeeping. Data that is not collected, after all, cannot be stolen.

b. Personalization

Personalization, whereby people are treated differently based upon personal information or characteristics, is a defining feature of many digital products and services.[63] In some contexts, personalization can be desirable, like when video streaming services and news feeds deliver

59. *Infra* Appendix sec. 4(a)(1). Legitimate interests, adapted from the GDPR, are defined as lawful objectives which are not disloyal. Legitimate interests offers a more flexible and future-proof approach to data minimization and purpose limitation than a whitelist of exceptions. The "strictly necessary" requirement should mitigate abuse of legitimate interests as an exception to data minimization, and the Attorney General has rulemaking authority to define specific legitimate interests.

60. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 379.

61. DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 128–57 (2022).

62. Cordell Inst., *supra* note 16, at 70–72.

63. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 380.

relevant content recommendations. But personalization can devolve into corrosive forms of targeting where it is not done loyally. Members of historically marginalized or vulnerable groups may be the target of intentional discrimination or suffer disparate impacts from a data ecosystem which reflects historical discrimination.[64] The controversial practice of targeted advertising can be either loyal or disloyal personalization, depending on how such targeting is employed, whose interests are being served, and how the used data is protected and/or shared.[65] The model statute bans disloyal targeted advertising as well as all cross-context behavioral advertising.[66]

c. Gatekeeping

Covered entities control third-party access to trusting parties and their personal data.[67] Sometimes access to trusting parties and their data can be loyal, such as where advertisers place contextual ads on a website or when interoperability protocols help trusting parties transfer data from one site or service to another.[68] Lax gatekeeping practices, however, are disloyal. Unrestricted sales of information to data brokers increase the risk that trusting parties will be the victims of fraud, stalking, manipulation, or other harms.[69] So too can access rules that permit exfiltration of personal data by third parties, as illustrated by the Cambridge Analytica scandal.[70] Government backdoors subject trusting parties to government surveillance and undermine data security practices.[71] These kinds of acts and practices disproportionately benefit the covered entity and subject trusting parties to disproportionate risk. The

64. *See, e.g.*, Jinyan Zang, *Solving the Problem of Racially Discriminatory Advertising on Facebook*, BROOKINGS INST. (Oct. 19, 2021), https://www.brookings.edu/articles/solving-the-problem-of-racially-discriminatory-advertising-on-facebook [https://perma.cc/A5AP-PQLR].

65. *Cf.* IRISH COUNCIL ON CIVIL LIBERTIES, THE BIGGEST DATA BREACH 2 (2022) (finding that "U.S. Internet users' online behavior and locations are tracked and shared 107 trillion times a year").

66. *Infra* Appendix sec. 5. The definition of targeted advertising comes from the ADPPA, whereas the definition of cross-context behavioral advertising is adapted from the CCPA. *Id.* secs. 2(13), 2(23).

67. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 380.

68. *Id.*

69. *See, e.g.*, Alistair Simmons, *The Justice Department's Agreement With a Data Broker That Facilitated Elder Fraud*, LAWFARE (Nov. 7, 2022), https://www.lawfaremedia.org/article/justice-departments-agreement-data-broker-facilitated-elder-fraud [https://perma.cc/K988-WTGW].

70. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/H2RC-DRWK].

71. *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, CTR. FOR DEMOCRACY & TECH. (Mar. 3, 2016), https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government-surveillance [https://perma.cc/BMZ5-8NVU].

model statute therefore imposes a subsidiary duty of loyal gatekeeping. Features of this duty include binding downstream recipients of covered data with a written contract requiring compliance with this Act, requiring reasonable data security practices, and requiring reasonable safeguards and protections against unauthorized scraping of covered data.[72]

One critical aspect of loyal gatekeeping is onward transfer requirements. It is not enough to merely limit disclosures or transfers of personal data to where it is strictly necessary or in the best interests of reasonable trusting parties because the transfer to third parties breaks the relational link. There is no direct connection between the trusting party and the new entity in possession of the trusting party's personal data, leaving the trusting party unable to prevent or remedy misuses of their personal data. In light of that risk, our statute includes an onward transfer requirement that provides a chain-link protection by which trusting parties can enforce their data privacy rights against downward recipients of personal data.[73]

d. Influencing

The primary duty of loyalty addresses the collection, processing, and transfer of personal data, as well as the design and implementation of information technologies. In contrast to the other subsidiary duties, influencing focuses on design to a greater degree. Trusted parties influence us when they design information technologies. There is no escaping this — all designs make some things harder and other things easier — which is why design is not neutral but political. We have explained elsewhere that "[t]echnologies are artifacts built to act upon the world. Every conscious design decision made in the creation of a website or app is meant to facilitate a particular kind of behavior."[74] Designers act disloyally when they employ malicious user interface elements (sometimes called "dark patterns") in ways that are meant to influence a trusting party's behavior against their best interests.[75]

To prevent disloyal influencing through design, the model statute imposes a subsidiary duty of loyal influencing. There are two main aspects of this subsidiary duty. First, a covered entity is prohibited from designing or implementing an information technology in a way that is unfair, deceptive, or abusive. The elements of unfair and deceptive

72. *Infra* Appendix sec. 5. The subsidiary duty of loyal gatekeeping complements and animates later sections of the model statute concerning the relationship between covered entities, service providers, and third parties. *Id.* sec. 18.

73. *Infra* Appendix sec. 6; *see* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 683 (2012).

74. Hartzog & Richards, *Surprising Virtues*, *supra* note 16, at 1029.

75. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 381–82.

design track those provisions of the FTC Act,[76] while the concept of abusive design was inspired by the authority of the Consumer Financial Protection Bureau.[77] Combatting abusive design is a central goal of imposing a loyalty framework. The second aspect of loyal influencing is a prohibition on the use of manipulative designs or practices to prevent trusting parties from exercising individual data rights under the model statute.[78]

e. Mediation

Although information relationships always entail communication and interaction between the trusting party and the trusted party, platforms often allow trusting parties to interact with one another. Whether the product or service in question is a traditional social media platform, a mobile payment service app, or a book cataloging service, it is increasingly common for services to be constructed as social by design.[79] With this intentional shift to social features comes a need for trusted parties to mediate interactions between trusting parties. However, the incentives of trusting parties and trusted parties are not necessarily aligned.[80] Platforms desire continual and endless growth, which is currently achieved by optimizing algorithms to reward impulsive and petty reactions.[81] Reduced barriers for speaking to and finding other users can lead to individual harms such as bullying and harassment.[82] It is imperative that covered entities instead prioritize the well-being of trusting parties, especially those most vulnerable.

The recent increased push to protect children and teenagers from the harms of disloyal social media practices has led to a flurry of proposed and enacted legislation concerning mediation. Although we do not advocate for children-specific privacy rules,[83] our model statute includes a subsidiary duty of loyal mediation that adopts certain features from youth privacy proposals like the Digital Consumer Protection

76. *See* 15 U.S.C. § 45; FTC POLICY STATEMENT ON DECEPTION: LETTER TO COMMITTEE ON ENERGY AND COMMERCE, (Oct. 14, 1983); *infra* Appendix sec. 7.

77. *Policy Statement on Abusive Acts or Practices*, CONSUMER FIN. PROT. BUREAU, (Apr. 3, 2023), https://www.consumerfinance.gov/compliance/supervisory-guidance/policy-statement-on-abusiveness [https://perma.cc/JDT9-J9H7]; *see also* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of the U.S. Code).

78. *Infra* Appendix sec. 7(d).

79. *See* Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 383.

80. *See generally* JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM (2019).

81. Hartzog & Richards, *Surprising Virtues*, *supra* note 16, at 1032.

82. Hartzog & Richards, *supra* note 9, at 1758 (citing DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 56–72 (2014); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 65–66 (2009); Woodrow Hartzog & Evan Selinger, *Increasing the Transaction Costs for Harassment*, 95 B.U. L. REV. ANNEX 47, 47–51 (2015)).

83. *Infra* Section III.D.

Commission Act,[84] which would have placed a duty of care and a duty of mitigation on social media companies and required certain protective default settings.[85] Our model statute adopts select rules from those proposals and expands those protections to apply to all trusting parties rather than only minors. Incorporating language from the Fair Credit Reporting Act,[86] the goal of mediation is to require covered entities to implement reasonable safeguards for systems that facilitate interactions between trusting parties and others.[87]

D. Decoupling Choice and Consent

Implementing a loyalty framework would mean the end of the failed "notice and choice" approach to privacy. A vast transdisciplinary scholarly literature has documented the many failures of notice and choice.[88] Two interrelated problems with the U.S. privacy law status quo are an overreliance on consent and the conflation of choice and consent.[89] "Choice" refers to our ability to freely make decisions. In the context of modern commercial relationships and data privacy, choice entails entering into information relationships and making specific decisions within those relationships. For example, when people choose to use a particular product or service, they might make additional choices within that relationship, such as by adjusting certain settings to utilize features that enhance or modify that relationship, product, or service. Any data privacy law should protect an individual's right to make such choices. "Consent" is distinct from choice because consent includes legal consequences. We can thus *choose* to wear a particular hat, but we can *consent* to a contract, and not the other way around. Going beyond mere choice, consent means changing the default legal relationship between parties to reallocate duties, risks, and benefits. Consent thus opens to the door for opportunism because it allows a company to bundle with its products or services additional data practices that do not further the trusting party's objectives.[90] Talk of "consent" must then include an analysis not merely of legal consequences but their validity, such as when we talk about the "gold standard" of "knowing and

84. Press Release, Senator Elizabeth Warren, Warren, Graham Unveil Bipartisan Bill to Rein in Big Tech (Jul. 27, 2023), https://www.warren.senate.gov/newsroom/press-releases/warren-graham-unveil-bipartisan-bill-to-rein-in-big-tech [https://perma.cc/P8VD-J6XF].

85. *See infra* Appendix secs. 3–4.

86. 15 U.S.C. § 1681e(a).

87. *Infra* Appendix sec. 8.

88. *See supra* note 12 and accompanying text.

89. Richards & Hartzog, *supra* note 11, at 1465–66; Cordell Inst., *supra* note 16, at 47–59; Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. (forthcoming 2024).

90. *See* Richards & Hartzog, *supra* note 11, at 1486–88 (describing the pathology of coerced consent).

voluntary" consent.[91] But even in situations with heightened consent requirements, trusting parties still suffer from the overwhelming nature of control as well as the residual risk shed by companies.[92] Reliance on the word "consent" perpetuates a false narrative that data practices are legitimized by an individual's agreement to them, as if individuals and companies are equals entering into an arms-length interaction.[93]

One benefit of grounding data privacy rules in relational duties is that it allows for a much-needed decoupling of choice and consent.[94] The model statute is designed to preserve choice without relying on the legal and moral "magic" of consent. In this way, individuals will be protected against betrayal no matter what they choose. This change is the product of several drafting decisions. First, consent does not factor into the best interests calculus. Instead of letting companies continue to legitimize their data practices (by requiring trusting parties to consent to such practices to access their products or services), under our model statute a data practice must survive the primary duty of loyalty purely on its merits. This requirement is analogous to provisions in food safety law that consumers cannot consent to unsafe foods and beverages. Reinforcing our primary duty is the subsidiary duty of loyal collection, which requires data minimization based on a theory of functionality. The data minimization rule is a good example of how data privacy legislation, free from the concept of consent, can allow consumer choice to flourish. Thus, by taking harmful choices off the table, loyalty frees individuals to choose without constantly worrying that a particular choice will authorize betrayal. Limiting the collection, processing, and transfer of covered data to what is reasonably necessary and proportionate to provide or maintain a requested service respects the individual's right to make free choices in the market without subjecting the trusting party to unnecessary bundled data practices. Including a legitimate interests exception preserves a business's ability to engage in mutually beneficial uses of covered data.

---

91. *Id.* at 1461–76.

92. *See supra* note 12 and accompanying text.

93. Hartzog & Richards, *Surprising Virtues*, *supra* note 16, at 992–99 (describing how modern information relationships are uniquely risky for consumers because of their ongoing, frequent, constructed, interactive, and responsive nature, leading to power imbalances between individuals and the companies who collect and process personal data); RICHARDS, *supra* note 12, at 42–44; BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 14 (2015) (arguing that there is no way to get things done in the digital age without exposing our data to third parties; "[n]o other way to reserve the hotel room or seat on the plane, to file the IRS form, to recall the library book, or to send money to our loved one in prison").

94. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 16, at 361 ("These duties allow trusting parties to enter into information to enter into information relationships without accepting the risks of whatever harmful data practices and consequences lurk in the fine print, the business model, or the technology. They can also allow trusting parties to select from a range of choices without fear of betrayal because they would be protected no matter what they chose.").

E. Protecting Children, Teenagers, and Adults

Conversations concerning data privacy, design, and mediation are increasingly dominated by calls to protect children and teenagers.[95] While this concern has remained prominent in tech policy, current discussions receive notably broad bipartisan support across different institutions.[96] This goal is laudable. We should aim to protect children and teenagers from disloyal data practices, such as extractive data collection and design optimized for excessive engagement.[97] But protecting minors will not be enough. Lawmakers do not face a binary choice between protecting children and teenagers or protecting adults.[98] Enacting strong data privacy protections that extend broadly to *all people* would protect the most vulnerable. Thus, the model statute creates broad protections for all trusting parties rather than distinct rules for children and teenagers.[99]

F. Waiver and Remedies

A robust private right of action is vital for ensuring optimal levels of enforcement.[100] However, private enforcement is only possible when individuals are protected from boilerplate waiver provisions included in terms of service. The ease with which companies can extract waivers for duties is one of the core failures of U.S. data privacy law.[101] To avoid the kind of structural inequalities perpetuated by boilerplate provisions and notice and choice, our model statute extends protections to

95. *See, e.g.*, Ryan Barwick, *Congress Is Considering Bills That Could Regulate How Advertisers Interact with Children,* MKTG. BREW (Mar. 1, 2023), https://www.marketingbrew.com/stories/2023/03/01/congress-is-considering-bills-that-could-regulate-how-advertisers-interact-with-children [https://perma.cc/QF8J-ES42] (discussing a growing push by President Biden and Congress to regulate children's privacy).

96. The Federal Trade Commission has emphasized the need to protect children's privacy. *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,299 (proposed Aug. 22, 2022) (Dissenting Statement of Commissioner Christine S. Wilson); *See* Cristiano Lima & Aaron Schaffer, *The FTC's Newest Member Wants to Scrutinize How Tech May Harm Kids*, WASH. POST (Aug. 25, 2022), https://www.washingtonpost.com/politics/2022/08/25/ftc-newest-member-wants-dial-up-scrutiny-kids-online-safety [https://perma.cc/YSR5-8K39].

97. *See, e.g.*, Complaint at 2, United States v. Microsoft Corp., No. 23-cv-00836 (W.D. Wash. Jun. 5, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/microsoftcomplaintcivilpenalties.pdf (alleging that Microsoft, in connection with its Xbox Live online service and related products, collected personal information from children under the age of 13 in violation of the COPPA Rule, collected such information before notifying parents and obtaining parental consent, and retained such personal information longer than necessary).

98. Cordell Inst., *supra* note 16, at 76–79.

99. Despite not explicitly tying statutory protections to age, age can still be a relevant consideration when a covered entity weighs the relative benefits and risks posed to trusting parties.

100. *See* Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639, 1655–68 (2022).

101. Hartzog & Richards, *Duty of Loyalty*, *supra* note 14, at 998–99.

all trusting parties, regardless of age, by holding unenforceable pre-dispute arbitration agreements, pre-dispute joint action waivers, and generally prohibiting waivers.[102]

Another key provision for private enforcement is the inclusion of restitution as a remedy in addition to compensatory damages. Although some violations of the statute could lead to easily quantifiable compensable harm, limiting recovery to compensatory damages would reintroduce a harm requirement that we sought to eliminate. By contrast, under a loyalty framework, the covered entity's economic gains from disloyal acts will often serve as the better measure of harm.[103]

IV. CONCLUSION

Lawmakers have the opportunity to revolutionize modern American privacy law by implementing a duty of loyalty. Operating as an animating force, interpretive guide, and catch-all provision, a loyalty framework would bring more coherence, flexibility, and accountability than privacy rules such as data minimization serving as standalone laws.[104] This Essay offers a model data loyalty act as proof of concept. Rather than attempting to say definitively what data loyalty must be, we offer our model only as a guide to lawmakers and as a foundation upon which they can build consensus. We have shown what a practical duty of data loyalty will do, why it will do it, and to what extent. The burden is now on lawmakers to make data loyalty a reality.

---

102. This provision was inspired by the Data Care Act of 2021. S. 919, 117th Cong. § 5 (2021).

103. *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 680 (2019).

104. Hartzog & Richards, *Surprising Virtues*, *supra* note 16, at 1024.

APPENDIX: STATE DUTY OF DATA LOYALTY ACT [ABRIDGED]

Included as an appendix to this Essay is an abridged version of the state model data loyalty act. Less important sections have been either omitted or summarized and are noted with brackets. Our proposed legislative findings and sample regulations are also omitted here but will be made available with the unabridged version of the statute. For a full up-to-date version of the model statute, see: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4628996 [https://perma.cc/3SUX-K6AF].

Section 1. Short Title.[105]

This Act may be cited as the "[State] Data Loyalty Act."

Section 2. Definitions.[106]

In this Act:

(1) ["Authentication"].[107]

(2) ["Biometric data"].[108]

---

105. Our model statute primarily borrows language from two sources: The State Data Privacy and Protection Act ("SDPPA"), a model bill created by the Electronic Privacy Information Center, *see* Caitriona Fitzgerald, *A Proposed Compromise: the State Data Privacy and Protection Act*, EPIC (Feb. 22, 2023), https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act [hereinafter SDPPA]; and the American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) [hereinafter ADPPA], which the SDPPA is itself modeled upon. When this project began, we initially worked from the ADPPA and began reworking that bill to include a full-blown general duty of data loyalty. While adapting that draft into a version suitable for state lawmakers, EPIC released their state version of the ADPPA, which provided a roadmap for us to convert the draft federal model data loyalty act into a state version. We are grateful to the EPIC team for their efforts.

106. We adopted many of the definitions from the ADPPA, but we excluded certain terms from that bill, renamed others, included terms from other statutes, bills, and model statutes, and added original terms. Terms cut from the ADPPA include: affirmative express consent, commission, covered minor, covered high-impact social media company, executive agency, state, state privacy authority, and substantial privacy risk. Terms from the ADPPA that we included but renamed include: third-party collecting entity (data broker) and unique persistent identifier (unique identifier). Terms that were present in the ADPPA but we moved from elsewhere in the bill to their own definition entry include: employee data, revenue, small business, pre-dispute arbitration agreement, and pre-dispute joint-action waiver. Terms that we adopted from other statutes, bills, and model statutes include: cross-context behavioral advertising and legitimate interest. Terms that are original to these authors include: decision space, exposure, information relationship, information technology, reasonable trusting party, scraping, and trusting party. Each definition below has an explanatory footnote noting where the term came from and any changes made from the source material.

107. ADPPA § 2(2); SDPPA § 2(a)(2).

108. ADPPA § 2(3); SDPPA § 2(a)(3).

(3) "Collect" and "collection"[109] mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means. This includes receiving information from the consumer either actively, through interactions such as user registration, or passively, by observing the consumer's behavior.

(4) ["Control"].[110]

(5) "Covered algorithm"[111] means a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision-making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual.

(6) "Covered data"[112] means information, including derived data and unique identifiers, that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual; provided, however, that "covered data" does not include —

(A) de-identified data;

(B) employee data; or

(C) public information.

(7) "Covered entity"[113] means any entity or any person, other than an individual acting in a noncommercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data. "Covered entity" includes any entity or person that controls, is controlled by, or is under common control with the covered entity. An entity shall not be considered to be a

109. ADPPA § 2(4); SDPPA § 2(a)(4). The second sentence of this definition, regarding active and passive collection, is an original contribution.

110. ADPPA § 2(6); SDPPA § 2(a)(5).

111. ADPPA § 2(7); SDPPA § 2(a)(6). For an explanation of covered algorithms and how this model statute is approaching artificial intelligence, automated decision-making technology, and profiling, see *infra* note 159 and accompanying text.

112. ADPPA § 2(8); SDPPA § 2(a)(7) We made several changes to the ADPPA's definition of covered data. First, we reworded the definition for clarity. Second, we updated the exception for "publicly available information" to reflect our change of that term to "public information." Third, we removed the exception for "inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual."

113. ADPPA § 2(9); SDPPA § 2(a)(8). This definition was slightly reworded for clarity consistent with the SDPPA. One notable change from the ADPPA is that we chose to exempt "small businesses."

covered entity for purposes of this Act in so far as the entity is acting as a service provider. The term "covered entity does not include —

> (A) a Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district, agency, or political subdivision of the Federal Government or a State, Tribal, territorial, or local government;
>
> (B) a person or an entity that is collecting, processing, or transferring covered data on behalf of a Federal, State, Tribal, territorial, or local government entity, in so far as such person or entity is acting as a service provider to the government entity;
>
> (C) an entity that serves as a congressionally designated nonprofit, national resource center, and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues; or
>
> (D) a small business.

(8) "Covered language"[114] means the ten languages with the most users in the United States, according to the most recent United States Census.

(9) "Cross-context behavioral advertising"[115] means the targeting of advertising to a consumer based on the consumer's covered data obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts. Cross-context behavioral advertising includes retargeting, the use of "look-alike" consumer behavioral profiles, and use of first party data in a third party context.

(10) "Data broker"[116] means a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data; and does not include a covered

---

114. ADPPA § 2(10); SDPPA § 2(a)(10).

115. This term comes from the California Consumer Privacy Act as amended by the California Privacy Rights Act. CAL. CIV. CODE § 1798.140(k). In terms of personalized and/or targeted advertisements, the ADPPA referred only to targeted advertisements, whereas we wanted to draw a distinction between targeted advertising generally and the subset of practices encompassed by cross-context behavioral advertising.

116. The ADPPA used the term "third-party collecting entity," ADPPA § 2(36), but the SDPPA replaced that term with data broker, SDPPA § 2(a)(12). We prefer the term data broker for its clarity and salience.

entity in so far as such entity processes employee data collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third party providing benefits to the employee. An entity may not be considered to be a data broker for purposes of this Act if the entity is acting as a service provider.

> (A) For purposes of this paragraph, the term "principal source of revenue" means, for the prior 12-month period, either —
>
> > (i) more than fifty percent of all revenue of the covered entity; or
> >
> > (ii) obtaining revenue from processing or transferring the covered data of more than 5,000,000 individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data.

(11) "De-identified data"[117] means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider —

> (A) takes reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;
>
> (B) publicly commits in a clear and conspicuous manner —
>
> > (i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and
> >
> > (ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and
>
> (C) contractually obligates any person or entity that receives the information from the covered entity or service provider —

117. ADPPA § 2(12); SDPPA § 2(a)(13).

(i) to comply with all of the provisions of this paragraph with respect to the information; and

(ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.

(12) "Decision space"[118] means the array of aesthetic and functional elements within an information technology, including physical, hardware, and software features that shape a trusting party's expectations about how a technology functions and can be used. "Decision space" includes interactive settings and choices presented to a trusting party when interfacing with a digital service or technology, including but not limited to: the size, shape, and prominence of control elements, settings, and choices; hypertext and hypermedia; coloration and font choice; buttons; sliders; switches; radio buttons; check boxes; scroll bars; hyperlinks; and motion-captured gestures.

(13) "Derived data"[119] means covered data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about an individual or an individual's device.

(14) "Device"[120] means any electronic equipment capable of collecting, processing, or transferring covered data that is used by one or more individuals.

(15) ["Employee"][121]

(16) ["Employee data"][122]

(17) "Exposure"[123] means the degree to which a trusting party has made themselves vulnerable to harm or loss to entrusting a covered

118. This is an original term in the model statute.

119. ADPPA § 2(13); SDPPA § 2(a)(14).

120. ADPPA § 2(14); SDPPA § 2(a)(15).

121. ADPPA § 2(15); SDPPA § 2(a)(16).

122. ADPPA § 2(8)(c); SDPPA § 2(a)(17). The decision to exclude employee data from covered data reflects the choice to use the ADPPA as the foundation for the model legislation rather than a conscious decision that that employee data should not be protected by the duty of loyalty.

123. This is an original term in the model statute. The concept of exposure is important to cabin the duty of loyalty. The duty of loyalty is a negative "no conflicts" rule: A covered entity cannot collect, process, or transfer covered data in a way that conflicts with the best interests of a trusting party. A data practice conflicts with the best interests of a trusting party when the risks posed to the trusting party are disproportionate relative to the benefits which flow to the trusting party and covered entity. The risks that a data practice pose to a trusting party flow from the trusting party's exposure. Thus, when a covered entity assesses the risks

entity with their data and mediated experiences. A trusting party's exposure when interacting with an information technology is shaped by what a covered entity can see or knows about that trusting party, which choices and options are available to trusting party, and what the trusting party can see or know about the covered entity. A covered entity shall assess a trusting party's exposure by considering the nature and length of the relationship between the parties, the nature of the data collected, processed, or transferred (including whether any such data is sensitive covered data), and the nature of the choices and signals mediated or controlled by the covered entity. For the purposes of this Section, vulnerability to harm or loss includes, but is not limited to, vulnerability to the following:

> (A) Physical harm which results in bodily injury or death.
>
> (B) Economic harm resulting in monetary loss, loss in the value of some asset, or time spent to protect oneself from risk of harm due to the breach or misuse of covered data.
>
> (C) Reputational harms affecting an individual's reputation, standing in the community, business opportunities, or employment.
>
> (D) Psychological harm in the form of emotional distress, which entails feelings of annoyance, frustration, fear, embarrassment, anger, and various degrees of anxiety, or disturbance, which entails intrusions that disturb tranquility, interrupt activities, or unreasonably consume a trusting party's time.
>
> (E) Autonomy harms, such as —
>
> (i) coercion, where a trusting party's freedom to act or choose has been impaired;
>
> (ii) manipulation, where there exists undue influence over a trusting party's behavior or decision-making;

---

posed to a trusting party by a data practice, the covered entity should consider the possible harms or loss listed in this definition (e.g., physical, economic, reputational, etc.) in light of the nature of the trusting party's relationship to the covered entity. The list of harms (except for loss) are derived from the taxonomy of privacy harms identified by Danielle Citron and Daniel Solove. *See supra* note 48 and accompanying text.

(iii) failure to inform, where a covered entity has failed to provide trusting parties with sufficient information to make decisions;

(iv) thwarted expectations, where a covered entity engages in acts or practices which undermine trusting parties' choices regarding data practices;

(v) lack of control, where trusting parties are rendered unable to make meaningful choices about their covered data or prevent future misuse of it; and

(vi) chilling effects, where a trusting party is inhibited from engaging in lawful activities.

(F) Discrimination harms, where an act or practice involving covered data entrenches inequality or disadvantages people based on gender, sex, sexual orientation, race, color, national origin, age, disability, group membership, or other characteristics or affiliations.

(G) Relationship harms, where the misuse or mishandling of covered data damages personal relationships, professional relationships, or relationships with organizations.

(H) Loss, which includes but is not limited to attention capture and opportunity costs of engagement with an information technology.

(18) "First party advertising or marketing"[124] means advertising or marketing, conducted by a covered entity that collected covered data from the trusting party linked or reasonably linkable to that data, through either direct communications with a user such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by or on behalf of such covered entity, or on a web site or app operated by or on behalf of such covered entity.

(19) "Genetic information"[125] means any covered data, regardless of its format, that concerns an individual's genetic characteristics, including —

(A) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid (DNA) of an individual; or

---

124. ADPPA § 2(17); SDPPA § 2(a)(18).
125. ADPPA § 2(18); SDPPA § 2(a)(19).

(B) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph (A).

(20) "Individual"[126] means a natural person who is a [INSERT STATE] resident or present in [INSERT STATE].

(21) "Information relationship"[127] means the discrete or ongoing interactions between individuals and covered entities which are mediated by information technologies.

(22) "Information technology"[128] means any technology, product, device, service, or method used by a covered entity to collect, process, or transfer covered data.

(23) "Large data holder"[129] means a covered entity or service provider that, in the most recent calendar year —

(C) had annual gross revenues of $250,000,000 or more; and

(D) collected, processed, or transferred the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals, excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; and the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals.

(E) "Large data holder" does not include any instance in which the covered entity or service provider would qualify as a large data holder solely on the basis of collecting or processing personal email addresses, personal telephone numbers, or log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity or service provider.

(24) "Legitimate interest"[130] means a lawful objective that does not conflict with the best interests of reasonable trusting parties. Collection or processing is strictly necessary to effect a legitimate interest pursued by the covered entity if such interest is not overridden by

126. ADPPA § 2(19); SDPPA § 2(a)(20).
127. This is an original term in the model statute.
128. This is an original term in the model statute.
129. ADPPA § 2(22): SDPPA § 2(a)(22).
130. This term is derived from the GDPR. *See* GDPR art. 6(1)(f).

the interests or rights and freedoms of the trusting party under this Act which require protection of covered data.

(25) ["Market research"].[131]

(26) ["Material"].[132]

(27) ["Precise geolocation information"].[133]

(28) ["Pre-dispute arbitration agreement"].[134]

(29) ["Pre-dispute joint-action waiver"].[135]

(30) "Process"[136] means to conduct or direct any operation or set of operations performed, whether by manual or automated means, on covered data or on sets of covered data, including but not limited to analyzing, organizing, structuring, maintaining, retaining, storing, using, adapting or altering, retrieving, consulting, aligning or combining, deleting, erasing, or destroying or otherwise handling covered data.

(31) "Processing purpose"[137] means a reason for which a covered entity or service provider collects, processes, or transfers covered data that is specific and granular enough for a reasonable individual to understand the material facts of how and why the covered entity or service provider collects, processes, or transfers the covered data.

(32) "Public information"[138] means any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from —

(A) Federal, State, or local government records, if the covered entity collects, processes, and transfers such

131. ADPPA § 2(22); SDPPA § 2(a)(23).
132. ADPPA § 2(23); SDPPA § 2(a)(24).
133. ADPPA § 2(24); SDPPA § 2(a)(25).
134. ADPPA § 403(b)(3)(A).
135. ADPPA § 403(b)(3)(B).
136. This definition combines elements of the ADPPA and SDPPA definitions of "process" with a more expansive definition of "processing" from the E.U.'s GDPR. ADPPA § 2(25); SDPPA § 2(a)(26); GDPR art. 4(2).
137. ADPPA § 2(26); SDPPA § 2(a)(27).
138. The ADPPA used the term "publicly available information" to carve out certain information from the definition of covered data. ADPPA § 2(27); SDPPA § 2(a)(28). We made the substantive change of replacing this with "public information." Focusing the inquiry on availability will lead to an overinclusion of information available on social media and the broader Internet, despite the reality that most online content is unlikely to ever be accessed by a broad audience. Instead, the inquiry focuses on whether publicity has given to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. This takes an element of the public disclosure of private facts tort (that traditionally has been used to limit the ability of people to seek redress for privacy violations) and repurposes it in a privacy-protective way. Thus, our definition of public information focuses more on obscurity than availability.

> information in accordance with any restrictions or terms of use placed on the information by the relevant government entity; a disclosure that has been made to the general public as required by Federal, State, or local law;
>
> (B) the visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession; or
>
> (C) publicity given to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.
>
> (D) "Public information" does not include any obscene visual depiction (as defined in section 1460 of title 18 of the United States Code); any inference made exclusively from multiple independent sources of public information; biometric data; public information that has been combined with covered data; genetic information, unless otherwise made available by the individual to whom the information pertains; or intimate images known to have been created or shared without consent.

(33) "Reasonable trusting party"[139] means a hypothetical ordinary person who enters into information relationships and makes choices within such relationships which entail only a reasonable allocation of risks and benefits between the covered entity and the reasonable trusting party.

(34) ["Revenue"].[140]

(35) "Scraping"[141] means the automated collection of covered data, whether structured or unstructured, by a third party from an information technology for the purpose of processing or onward transfer.

(36) ["Sensitive covered data,"[142] which includes biometric data, precise geolocation, and other categories of information generally regarded as "sensitive"].

(37) "Service provider"[143] means a person or entity that collects, processes, or transfers covered data on behalf of, and at the

---

139. This is an original term in the model statute. Although a covered entity owes a duty of loyalty to trusting parties (those individuals who are invited to trust a covered entity with their data and mediated experiences), that duty is assessed by a reasonable person standard.

140. ADPPA § 209(c); SDPPA § 2(a)(29).

141. This is an original term in the model statute.

142. SDPPA § 2(a)(30); ADPPA § 2(28). Under this model statute, sensitive covered data is largely inconsequential. However, the definition of exposure requires consideration of whether the data in question is sensitive covered data.

143. SDPPA § 2(a)(31); ADPPA § 2(29).

direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity; and receives covered data from or on behalf of a covered entity or a Federal, State, Tribal, territorial, or local government entity. A service provider that receives service provider data from another service provider as permitted under this Act shall be treated as a service provider under this Act with respect to such data.

(38) ["Service provider data"[144] means covered data that is collected or processed by or has been transferred to a service provider for the purpose of allowing the service provider to perform a service or function on behalf of the transferring entity].

(39) "Small business"[145] means a covered entity or a service provider that meets the following criteria for the period of the 3 preceding calendar years (or for the period during which the covered entity or service provider has been in existence if such period is less than 3 years):

> (A) The covered entity or service provider's average annual gross revenues during the period did not exceed $41,000,000;
>
> (B) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy; and
>
> (C) The covered entity is not a data broker.

(40) "Targeted advertising"[146] means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier; provided, however, that "targeted advertising" does

144. SDPPA § 2(a)(32); ADPPA § 2(30).

145. SDPPA § 2(a)(33); ADPPA § 209. Although we adopt the same definition of small business as the SDPPA, one notable difference is that our model statute exempts small businesses from coverage rather than subjecting them to lesser requirements than other covered entities.

146. SDPPA § 2(a)(35); ADPPA § 2(34). The definition of targeted advertising should be read in conjunction with the definition of cross-context behavioral advertising above.

not include: advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback; contextual advertising, which is when an advertisement is displayed based on the content in which the advertisement appears and does not vary based on who is viewing the advertisement; or processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content performance, reach, or frequency, including independent measurement.

(41) "Third party"[147] means —

(A) any person or entity, including a covered entity, that —

(i) collects, processes, or transfers covered data that the person or entity did not collect directly from the individual linked or linkable to such covered data; or

(ii) collects, processes, or transfers covered data and is not a consumer-facing business with which the individual linked or reasonably linkable to such covered data expects and intends to interact; and

(iii) is not a service provider with respect to such data;

(B) does not include a person or entity that collects covered data from another entity if the two entities are related by common ownership or corporate control, but only if a reasonable trusting party's expectation would be that such entities share information.

(42) "Third party data"[148] means covered data that has been transferred to a third party.

(43) "Transfer"[149] means to sell, share, rent, release, license, disclose, disseminate, make available, or otherwise communicate covered data orally, in writing, electronically, or by any other means.

147. ADPPA § 2(35); SDPPA § 2(a)(36). Subparagraphs (i) and (ii) were each used in the ADPPA and SDPPA respectively. We chose to include both.

148. ADPPA § 2(37); SDPPA § 2(a)(37).

149. Expanded upon ADPPA § 2(38) and SDPPA § 2(a)(38) to clarify that selling covered data is a transfer.

(44) "Trusting party"[150] means any individual who entrusts their personal data and mediated experiences with a covered entity.

(45) ["Unique identifier"].[151]

Section 3. Duty of Loyalty.

(a) A covered entity owes a duty of loyalty to all trusting parties. This duty is defined by the extent of a reasonable trusting party's exposure.

(b) Under this duty, a covered entity shall not collect, process, or transfer covered data in a way that conflicts with the best interests of trusting parties; or design or implement an information technology in a way that conflicts with the best interests of reasonable trusting parties. A covered entity's acts or practices conflict with the best interests of trusting parties when either the collection, processing, or transfer of covered data or the design or implementation of an information technology results in a disproportionate allocation of benefits in favor of the covered entity relative to the degree of individual and collective risk posed to the trusting parties.

Section 4. Loyal Collection.

(a) Data Minimization and Purpose Limitation.[152]

(1) A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is strictly necessary and proportionate to —

150. This is an original term in the model statute. This model statute adopts the term trusting party, as opposed to consumer, individual, or data subject, to emphasize that the duty of loyalty is relational. Although a covered entity owes a duty of loyalty to trusting parties, the standard by which that duty is judged is one of reasonableness, thus protecting a covered entity from having to comply with the idiosyncratic preferences of each unique trusting party.

151. ADPPA § 2(39); SDPPA § 2(a)(39).

152. This section was modeled after ADPPA § 101, but a number of significant changes were made. First, the primary duty of loyalty in Section 3 of this Act adds in a baseline limit on data collection, prohibiting a covered entity from collecting, processing, or transferring covered data in a way that conflicts with the best interests of a trusting party. This subsidiary duty builds on that, providing that data collection is presumptively loyal where it is either strictly necessary to provide or maintain a specific product or service requested by the individual to whom the data pertains or to effect a legitimate interest of the covered entity. The introduction of legitimate interests is a notable departure from the ADPPA, which preferred a whitelist approach. In contrast, we preferred a more flexible exception. The second major departure from the ADPPA is the raised threshold: collection, processing, or transfer of covered data must be *strictly necessary* to its given purpose rather than "reasonably necessary and proportionate."

(A) provide or maintain a specific product or service requested by the trusting party to whom the data pertains; or

(B) effect a legitimate interest of the covered entity.

Section 5. Loyal Personalization.

(a) A covered entity or service provider that directly delivers a targeted advertisement shall do so only where the delivery of the targeted advertisement does not conflict with the best interests of reasonable trusting parties.

(b) A covered entity or service provider shall not collect, process, or transfer covered data for the purpose of delivering a cross-context behavioral advertisement.

(c) A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

(d) First party advertising or marketing does not violate the duty of loyalty.

Section 6. Loyal Gatekeeping.

(a) A covered entity is prohibited from transferring covered data to a third party or service provider except where allowed under the data minimization rule of Section 4 of this Act. When a covered entity does transfer covered data to a third party or service provider, that covered entity shall, in accordance with Section 16 of this Act, require the third party or service provider, as a condition of receipt of such covered data, to contractually agree to be bound by the duties and obligations of this Act. Trusting parties whose covered data are transferred shall have the right to enforce such contracts directly as intended third-party beneficiaries.

(b) A covered entity or service provider shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition in accordance with any regulations or amendments to this Act.

(c) A covered entity shall implement reasonable safeguards and protections into any information technologies to prevent unauthorized third parties from scraping covered data concerning trusted parties.

Section 7. Loyal Influencing.[153]

(a) It is an unfair act for a covered entity to design or implement an information technology in a way that causes or is likely to cause substantial harm to trusting parties which is not reasonably avoidable by trusting parties and not outweighed by countervailing benefits to trusting parties or to competition.

(b) It is a deceptive act or practice for a covered entity to design or implement an information technology in a way that misleads or is likely to mislead a reasonable trusting party in a material way.

(c) It is an abusive act or practice for a covered entity to design or implement an information technology in a way that will exploit predictable biases to interfere with a trusting party's decision-making process in an adversarial way. A covered entity shall not process covered data or design information technologies in a way that —

(1) materially interferes with the ability of trusting parties to understand a term or condition of a covered entity's product or service; or

(2) takes unreasonable advantage of —

(C) a lack of understanding on the part of a trusting party of the material risks, costs, or conditions of a covered entity's product or service;

(D) the inability of a trusting party to protect the interests of the trusting party in selecting or using a covered entity's product or service; or

(E) the reasonable reliance by a trusting party on a covered entity to act in the interests of the trusting party.

(3) has the purpose or substantial effect of obscuring, subverting, or impairing the autonomy, decision making, or choice of a reasonable trusting party in an interaction with the service of the entity by such trusting party, in a way that conflicts with the best interests of the trusting party (including interests of the trusting party in privacy or data security), which include —

153. Unfair influencing focuses on design or implementation of an unfair trade practice that is unfair, deceptive, or abusive, reflecting the three prongs of American consumer protection law in the FTC Act and Dodd-Frank. Subsection (d) is derived from ADPPA § 204, but references to affirmative express consent have been removed.

(A) selecting a default software or platform setting that favors the interests of the covered entity over the interests of the trusting party with respect to covered data; or

(B) modifying the decision space of the user on the platform or service of the covered entity to emphasize or advantage choices that benefit the interests of the covered entity over the interests of the consumer.

(d) A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this Act through —

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the design, modification, or manipulation of any decision space with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable trusting party's autonomy, decision making, or choice to exercise any such right.

Section 8. Loyal Mediation.

(a) In designing, deploying, and maintaining information technologies that facilitate a trusting party's interaction with individuals, including natural persons and legal entities, covered entities shall maintain reasonable procedures designed to prevent and mitigate the foreseeable risks to physical and mental health; patterns of use that indicate or encourage addiction-like behaviors; physical harm, online bullying, and harassment; and unfair, deceptive, or abusive marketing practices.

(b) A covered entity shall provide readily-accessible and easy-to-use safeguards to enable trusting parties to control their experience and covered data on the platform, including settings to limit the ability of other individuals to contact or find a trusting party; prevent other individuals from viewing a trusting party's personal data collected by or shared on the platform, in particular restricting public access to covered data; limit features that increase, sustain, or extend use of the covered entity's service, such as automatic playing of media, rewards for time spent on the platform, and notifications; opt-out of algorithmic recommendation systems that use covered data; delete the trusting party's account and request removal of covered data; restrict the sharing of the precise geolocation information of a trusting party and to provide notice regarding the tracking of a trusting party's precise geolocation information; and limit the time spent by a trusting party on the

platform. The safeguards required under this Section will, by default, be set at the most protective setting.

Section 9. Privacy by Design.[154]

(a) A covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data or the design of information technologies. A covered entity and service provider shall —

(1) identify, assess, and mitigate risks of harm or loss to trusting parties related to the products and services of the covered entity;

(2) identify the benefits that flow to trusting parties and the covered entity; and

(3) implement reasonable training and safeguards within the covered entity and service provider to promote compliance with this Act.

(b) [Omitted: details regarding scope of subsection (a)].

(c) Not later than 1 year after the date of enactment of this Act and biennially thereafter, each covered entity shall conduct a data loyalty assessment. Such assessment shall weigh the relative benefits of the covered entity's covered data collecting, processing, and transfer practices against the risks of such practices to trusting parties. The covered entity shall make a summary of such data loyalty assessment publicly available in a place that is easily accessible to individuals. The data loyalty assessment shall —

(1) be reasonable and appropriate in scope given —

(A) the nature of the covered data collected, processed, and transferred by the covered entity;

154. ADPPA § 103; SDPPA § 5. This section has been heavily modified from the ADPPA to reflect the central role of loyalty. If the duty of loyalty is limited to the extent of a trusting party's exposure, then so too are the privacy by design obligations. Data practices that entail a higher degree of risk of harm or loss to trusting parties necessitate stronger privacy by design safeguards, and vice versa. One major change to this section is the decision to require data loyalty assessments under this section rather than under section 15. The data loyalty assessment requirements are likely to be updated to reflect the best standards from newly enacted or finalized state rules on data protection impacts assessments, such as those in Colorado or California.

(B) the volume of the covered data collected, processed, and transferred by the covered entity;

(C) the relative benefits conferred upon the covered entity and trusting parties by the collecting, processing, and transfer of covered data by the covered entity; and

(D) the risks posed to trusting parties by the collecting, processing, and transfer of covered data by the large data holder;

(2) be documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under paragraph (1);

(3) include additional information required by regulations issued by the Attorney General;

(4) upon request, make such data loyalty assessments available to the Attorney General; and

(5) if the covered entity is a large data holder, be approved by the privacy protection officer designated in Section 15, as applicable.

Section 10. Transparency.[155]

(a) Each covered entity shall make publicly available, in a clear, conspicuous, not misleading, and easy-to-read and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity.

(b) [If a covered entity makes a material change to its privacy policy or practices, it must, before implementing the material change, provide trusting parties with a reasonable opportunity to object or exercise any applicable rights under this Act].

(c) Nothing in this Section may be construed to affect the requirements for covered entities under Sections 3 through 9, 11, or 12.

155. ADPPA § 202; SDPPA § 7. This section has been heavily modified from the ADPPA to reflect the diminished role of consent in this model act. Furthermore, specific transparency requirements have been removed from the body of the statute and moved to proposed rulemaking.

Section 11. Individual Data Rights.[156]

[Omitted: A covered entity shall provide trusting parties with rights of access, correction, deletion, and portability].

Section 12. Protection from Retaliation through Service or Pricing.[157]

(a) [Protection from price retaliation for exercising a right under this Act].

(b) [Exceptions for billing, bona fide loyalty programs, etc.].

(c) Notwithstanding the provisions in this subsection, no covered entity may offer different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

Section 13. Data Brokers.[158]

(a) [Data brokers shall place a clear, conspicuous, not misleading, and readily accessible notice on their website or mobile application notifying individuals that the entity is a data broker and including a link to the website established under this Section].

(b) [Establishing of a searchable data broker registry with options for individual's to exercise data rights].

(c) [Liability for failing to register].

Section 14. Civil Rights and Algorithms.[159]

(a) A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on

156. ADPPA § 203; SDPPA § 8.

157. ADPPA § 104; SDPPA § 6.

158. ADPPA § 206; SDPPA § 11. We followed EPIC's decision in the SDPPA to use the term "data broker" rather than "third party collecting entity."

159. ADPPA § 207; SDPPA § 12. That the model statute incorporates the ADPPA's provisions on "covered algorithms" is a consequence of the initial decision to use the ADPPA as the foundation for the model data loyalty act. Future versions of the model statute are likely to have updated provisions regarding artificial intelligence, automated decision-making technology, and profiling. *See Oversight of A.I.: Legislating on Artificial Intelligence, Hearing Before the S. Comm. on the Judiciary, Subcomm. on Priv., Tech., and the L.*, 118th Cong. 1 (2023) (testimony of Woodrow Hartzog) (arguing that "[t]o bring AI within the rule of law, lawmakers must go beyond half measures to ensure that AI systems and the actors that deploy them are worthy of our trust"); Cordell Inst., Comment Letter on NTIA's AI Accountability Policy Request for Comment (June 12, 2023), https://www.regulations.gov/comment/NTIA-2023-0005-1291 [https://perma.cc/NS5H-X6UY].

the basis of race, color, religion, national origin, sex, or disability. This does not apply to:

(1) the collection, processing, or transfer of covered data for the purpose of —

(A) a covered entity's or a service provider's self-testing to prevent or mitigate unlawful discrimination; or

(B) diversifying an applicant, participant, or customer pool; or

(2) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).

(b) [A covered entity that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group of individuals, and uses such covered algorithm, solely or in part, to collect, process, or transfer covered data shall conduct annually a data loyalty assessment of such algorithm. The data loyalty assessment shall provide information regarding design and methodology, the purpose and proposed uses, descriptions of the data used by the covered algorithm, an assessment of the necessity and proportionality of the covered algorithm in relation to its stated purpose, and additional requirements for large data holders].

(c) [A covered entity or service provider that knowingly develops a covered algorithm that is designed to, solely or in part, to collect, process, or transfer covered data in furtherance of a consequential decision shall prior to deploying the covered algorithm evaluate the design, structure, and inputs of the covered algorithm to reduce the risk of potential harms identified under this Section].

(d) In complying with this Section, a covered entity and a service provider may focus the data loyalty assessment or evaluation on any covered algorithm, or portions of a covered algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms identified under this Section.

(e) [A covered entity and a service provider shall be required to submit the data loyalty assessment or evaluation conducted under subsections (b) or (c) to the Attorney General and make a summary of such publicly available].

Section 15. Executive Responsibility.[160]

(a) Beginning 1 year after the date of enactment of this Act, an executive officer of a large data holder shall annually certify, in good faith, to the Attorney General that the entity maintains —

> (1) internal controls reasonably designed to comply with this Act; and
>
> (2) internal reporting structures to ensure that such certifying executive officer is involved in and responsible for the decisions that affect the compliance by the large data holder with this Act.

(b) [Good faith requirement for the certification submitted under subsection (a)].

(c) [A covered entity or service provider shall designate 1 or more qualified employees as privacy officers and 1 or more qualified employees as data security officers]

(d) [A large data holder must designate at least one of the officers described in subsection (c) to report directly to the highest official at the large data holder as a privacy protection officer, who has additional obligations with regard to privacy and security policies, audits, employee training, and more].

Section 16. Service Providers and Third Parties.[161]

> [Omitted: Duties and obligations of service providers and third parties, written contract requirements for service providers and third parties, and due diligence requirements for covered entities transferring covered data to a third party or service provider].

160. ADPPA § 301; SDPPA § 15. One notable departure from the ADPPA is that we modified and moved the requirement to conduct privacy impact assessments (which we relabeled as data loyalty assessments) under Section 301(d) & (e), to the privacy by design requirements under Section 9 of this model act. This section is otherwise largely unchanged from the ADPPA. We have long argued that privacy reform requires using corporate law's regulatory tools to respond to privacy problems stemming from corporate informational power, which may include individual responsibility of executives and the creation of independent privacy roles within corporate entities. Hartzog & Richards, *supra* note 9, at 1744–45.

161. ADPPA § 302; SDPPA § 16.

Section 17. Enforcement.[162]

(a) The Attorney General, District Attorney, or a City Corporation Counsel may bring a civil action in the name of the State, or as *parens patriae* on behalf of the residents of the State, against any covered entity or service provider that violated this Act to —

(1) enjoin such act or practice;

(2) enforce compliance with this Act or such regulation;

(3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of such State; or

(4) obtain reasonable attorneys' fees and other litigation costs reasonably incurred.

Section 18. Enforcement by Persons.[163]

(a) Beginning on the date that is two years after the date on which this Act takes effect, any person or class of persons subject to a violation of this Act or a regulation promulgated under this Act may bring a civil action against a covered entity in any court of competent jurisdiction.

(b) In a civil action brought under paragraph (a) in which a plaintiff prevails, the court may award the plaintiff —

(1) an amount equal to the sum of any compensatory damages or restitution;

(2) disgorgement, injunctive relief, and other equitable remedies;

(3) declaratory relief; and

(4) reasonable attorney's fees and litigation costs.

(c) [No waiver, pre-dispute arbitration agreement, or pre-dispute joint action waiver is enforceable].

(d) [30 day right to care before claim for injunctive relief by person or class of persons]

---

162. ADPPA § 402; SDPPA § 17.

163. ADPPA § 403; SDPPA § 18. Notable changes to this section include the explicit inclusion of restitution as a remedy, disgorgement and other equitable remedies, and prohibitions on waiver.

(e) This Section shall only apply to a claim alleging a violation of [select Sections, including Sections 3–8] or a regulation promulgated pursuant to any such Section.

Section 19. Relationship to Federal and State Laws.[164]

(a) [Covered entities or service providers that are required to comply with select laws, such as title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-2), and are in compliance with the data privacy requirements of such, shall be deemed to be in compliance with the related requirements of this Act solely and exclusively with respect to data subject to the requirements of such regulations, part, title, or Act].

(b) [Covered entities or service providers that are required to comply with select laws, such as title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d–2), and are in compliance with the information security requirements of such, shall be deemed to be in compliance with the data security requirements of this Act, solely and exclusively with respect to data subject to the requirements of such regulations, part, title, or Act].

(c) Nothing in this Act shall be construed to limit or diminish First Amendment freedoms guaranteed under the Constitution.

Section 20. Severability.[165]

[Omitted].

Section 21. Rulemaking.[166]

(a) The Attorney General may promulgate rules for the purposes of carrying out this Act, including, but not limited to the following areas:

---

164. This section borrowed language from SDPPA § 19, which is based on ADPPA § 404. Changes made by these authors include the addition of subsection (c), which is a First Amendment savings clause. That language was included in the ADPPA, but as part of the data minimization rule § 101(e). For consistency and clarity, we chose to move that language to this Section.

165. SDPPA § 20; ADPPA § 405.

166. Adapted from SDPPA § 21. These authors made changes to reflect the loyalty framework introduced as well as situations where it made more sense to condense the statute and

(1) establishing new subsidiary duties of loyalty;

(2) [adjusting the monetary thresholds and the data collected thresholds in the definitions of "large data holder" and "small business"];

(3) [further defining "precise geolocation information"];

(4) [updating or adding categories to the definition of "sensitive covered data"];

(5) establishing a list of practices that constitute legitimate interests under Section 4 as long as such purposes are consistent with the reasonable expectations of individuals and the duty of loyalty;

(6) establishing reasonable administrative, technical, and physical data security practices and procedures under Section 6;

(7) further defining what constitutes reasonable policies, practices, and procedures under Section 9;

(8) establishing the form and content of the transparency obligations under Section 10;

(9) [establishing processes for covered entities to comply with requests to exercise rights under Section 11];

(10) [establishing rules and procedures to facilitate an individual's or the individual's authorized agent's exercise of rights under Section 11];

(11) [establishing additional permissive exceptions to Section 11];

(12) [establishing how often, and under what circumstances, an individual may request a correction pursuant to Section 11];

(13) the development and use of a recognizable and uniform opt-out logo or button by all covered entities to promote awareness of the opportunity to opt-out of targeted advertising and transfers to third parties;

---

offload specific details to rulemaking, including the transparency obligations under Section 10 and the data security obligations under Section 6.

(14) requiring covered entities obligated to conduct assessments under Sections 9 or 14 to establish a process to ensure that audits are thorough and independent;

(15) requiring additional information necessary for compliance with the assessments required under Sections 9 and 14;

(16) excluding from the algorithmic loyalty assessments required under Section 14(b) any covered algorithm that presents low or minimal consequential risk of harm to an individual or group of individuals;

(17) setting compliance requirements for service providers and third parties.

Section 22. Effective Date.

[Omitted].