**The Cordell Institute for Policy in Medicine & Law**
Washington University in St. Louis
Anheuser-Busch Hall, Room 541B
St. Louis, Missouri 63130

**October 13, 2023**

*Submitted via email to Record@judiciary-dem.senate.gov*

**Re: Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law hearing entitled "Oversight of A.I.: Legislating on Artificial Intelligence" – Senator Josh Hawley Questions for the Record**

**Dear Senator Hawley, Committee Members, and Staff,**

Thank you for the opportunity to testify at the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law hearing entitled "Oversight of A.I.: Legislating on Artificial Intelligence" on Tuesday, September 12, 2023. Below is a written response to the question for the record from Senator Hawley. I file these comments on behalf of myself and in collaboration with my colleagues at the Cordell Institute at Washington University, Neil Richards and Ryan Durrie.

**Senator Hawley's Question for the Record:**

*1. What legislation or policies do you recommend to ensure that companies developing large language models do not exploit users' data?*

Large language models (LLMs) by their very nature are hungry for data,[1] leaky at holding this data,[2] sneaky in how they gather and use data,[3] and exclusory in their results and consequences for consumers.[4] Data exploitation and manipulation, whether in the context of creating and deploying large language models (LLMs) or otherwise, comes from an imbalance of power and information in relationships.[5] Tech companies can control what their customers see and they collect information from across the web

[1] Robert Hart, *Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database*, FORBES (May 23, 2022, 6:55am), https://www.forbes.com/sites/roberthart/2022/05/23/clearview-ai-fined-94-million-in-uk-for-illegal-facial-recognition-database/?sh=c9ef95019636; Alex Reisner, *These 183,000 Books Are Fueling The Biggest Fight In Publishing And Tech*, THE ATLANTIC (Sept. 25, 2023), https://www.theatlantic.com/technology/archive/2023/09/books3-database-generative-ai-training-copyright-infringement/675363/.
[2] Ben Derico, *ChatGPT bug leaked users' conversation histories*, BBC (Mar. 2023), https://www.bbc.com/news/technology-65047304; James Vincent, *Apple restricts employees from using ChatGPT over fear of data leaks*, THE VERGE (May 19, 2023, 3:29 AM), https://www.theverge.com/2023/5/19/23729619/apple-bans-chatgpt-openai-fears-data-leak.
[3] Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MAR. L. REV. 785 (2015).
[4] *See* Neil Richards & Woodrow Hartzog, *Against Engagement* (conference draft , Privacy Law Scholars Conference 2022) (on file with authors).
[5] *See, e.g.* Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022).

as though all accessible human information is theirs for the taking. Compared to individual consumers, tech companies have practically unlimited resources and strong financial incentives to influence people's behavior for their own benefit and profit.

Lawmakers might be tempted to turn to standard data protection rules like forcing transparency and requiring consent from people before processing their data, but this standard approach would be doomed to fail. These "fair information processing" rules haven't yet held tech companies accountable and they aren't responsive to the full scope of risks posed by LLMs. To combat the fact that LLMs are hungry, leaky, sneaky, and exclusory, lawmakers should focus on consumer relationships with the companies that gather their data or design and implement LLMs based upon this data. This relationships-focused approach would be to how the law requires confidentiality, care, and most importantly, loyalty from physicians, lawyers, and other professionals with a power imbalance related to their patients, clients, and customers.[6]

Duties of loyalty protect against self- dealing, while related duties of care placed on relationships protect against dangerous behavior and the risks of harm. In other areas of the law, the extent of these duties is proportional to the vulnerability of the trusting parties.[7] The more exposed people are to LLMs, the more loyalty, care, and confidentiality lawmakers should demand from those deploying the tools.

Many of the problems of surveillance capitalism come down to the problem of self-dealing, where an organization exploits an advantage over a trusting party to its own benefit.[8] The lack of meaningful abilities to protect consumers under American privacy law has enabled such corporate opportunism and manipulation of consumers using human information, and this failure will only be exacerbated by the increased speed and efficiency of large language models to analyze and use this data. This problem is particularly serious in the context of LLMs and other technologies that promise to understand consumers so that they can better satisfy their needs and wants. Insufficiently constrained by privacy law and driven to maximize quarterly profits by corporate law, companies can deploy a potent cocktail of techniques derived from cognitive and behavioral science to "nudge" or otherwise influence the choices consumers make.[9] And history shows us that the companies that gather consumer data have not acted as benevolently as many had hoped.[10]

Misuse and self-enrichment through data gained in these power asymmetries ultimately costs consumers their time, money, attention, mental well-being, reputation, and significant life opportunities.[11] These costs include everything from their attention being broken via intrusive "notifications," to manipulation subtly shaping the way that consumers shop and vote, to the harms of engagement-driven social media.[12] "Personalization" of the companies' contacts and engagement strategies through the use of this personal

---

[6] *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687, 1693 (2020); Hartzog & Richards, *supra* note 5, at 1697.

[7] *See, e.g.*, Hartzog & Richards, *supra* note 5; Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020) at 13–14.

[8] *See, e.g.,* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[9] *See* NEIL RICHARDS, WHY PRIVACY MATTERS 39–50 (2022).

[10] *Id., See generally, Richard H. Thaler & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008) (outlining how companies can promote pro-human outcomes if given the incentives necessary to induce those outcomes) .*

[11] *See* Neil Richards & Woodrow Hartzog, *Against Engagement* (draft manuscript) (on file with authors).

[12] *See generally*, JOHANN HARI, STOLEN FOCUS: WHY YOU CAN'T PAY ATTENTION – AND HOW TO THINK DEEPLY AGAIN (2022); Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022)?

data only magnifies these harms.[13] Such "personalization" can be finely calibrated to manipulate consumers into increasing engagement, regardless of any effect on consumers' mental wellbeing.[14] With every click and post, we are further exposed to the appetite, carelessness, and influence of those developing and deploying LLMs.

LLMs will never work for the benefit of all unless society can reliably trust those designing and deploying them. Right now, the trust people are giving these companies is a blind trust that is regularly betrayed. What is needed are rules that make companies deploying LLMs trust-*worthy*. This is where duties of loyalty, care, and confidentiality come in. The core feature of a duty of loyalty is that it creates a substantive duty prohibiting self-dealing at the expense of a trusting party.[15] Relational duties, such as a duty of loyalty, offer distinct advantages for lawmakers looking to address privacy across multiple disparate actors and methods of data consumption.

First, relational duties are sensitive to power disparities within information relationships. Second, relational duties help to mitigate the issues with overwhelming corporate disclosures and requests for consent. Relational duties allow allow lawmakers to move beyond ineffective consent frameworks while preserving meaningful choices for people. These duties allow trusting parties to enter information relationships without accepting the risks of whatever harmful data practices and consequences lurk in the fine print, the business model, or the technology.[16] They can also allow a broader range of potential choices because under a duty of loyalty, people are protected regardless of what they choose.[17] Relationships open the possibility of more robust enforcement rules because they are voluntarily entered into and because they are more consistent with free expression principles. This is why relational rules have long been recognized in American law.[18]

A substantive duty of data loyalty could revolutionize American privacy law. As we have argued in previous articles, comments, and testimony,[19] we believe that creating a broad duty of data loyalty offers three important advantages that other approaches do not. First, a duty of loyalty is substantially more able than a traditional data protection approach to address the novel problems created by the explosion of "big data" processing and analytics.[20] These include algorithmic discrimination, manipulation, oppression, and shaming that are caused by the ubiquity of modern technology platforms. Second, loyalty helps solve privacy law's harm problem in a way that is consistent with the direction of current Supreme Court

[13] This is precisely what happened in the Cambridge Analytica scandal, in which Facebook data was used to create finely calibrated psychological profiles of voters identified by their real names, suggesting which kinds of arguments would be most effective at getting them to act in the ways that the paying political advertisers wanted them to. *See* RICHARDS, *supra* note 9, at 25–26.

[14] These are the allegations Facebook whistleblower Frances Haugen presented under oath before lawmakers in the United States and around the world in 2021. *See, e.g.,* Billy Perrigo, *Inside Frances Haugen's Decision to Take on Facebook*, TIME (Nov. 22, 2021) https://time.com/6121931/frances-haugen-facebook-whistleblower-profile/ [https://per ma.cc/L8QN-6GD5].

[15] *See generally*, U.S. Sen. Comm. on Health Educ. Lab. & Pensions, Comment Letter on Improving Americans' Health Data Privacy (Sept. 28, 2023), (on file with The Cordell Institute for Policy in Medicine & Law); Hartzog & Richards, *supra* note 5.

[16] *Id.*

[17] For an extended critique of consent-based models for data processing, *see* Hartzog & Richards, *supra* note 5; *see also* Richards & Hartzog, *supra* note 11, and HARI, *supra* note 12.

[18] HARI *Supra* note 12.

[19] *See e.g., Neil Richards & Woodrow Hartzog, A Duty of Loyalty for Privacy Law, 99 WASH. U. L. REV. 961; U.S. Sen. Comm. on Health Educ. Lab. & Pensions, Comment Letter on Improving Americans' Health Data Privacy (Sept. 28, 2023), (on file with The Cordell Institute for Policy in Medicine & Law); Fed. Trade Comm'n, Comments of the Cordell Institute on the Prevalence of Commercial Surveillance and Data Security Practices that Harm Consumers (Nov. 22, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284020; U.S. Senate Comm. on the Judiciary, Subcomm. on Priv. Tech. and the L., Testimony of Woodrow Hartzog on "Legislating of Artificial Intelligence" (Sept. 12, 2023), https://www.judiciary.senate.gov/imo/media/doc/2023-09-12_pm_-_testimony_-_hartzog.pdf; Nat'l Telecomm. and Info. Admin., Comments of the Cordell Institute on AI Accountability (June 12, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4477426.*

[20] *See generally* Woodrow Hartzog & Neil Richards, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579 (2017)

doctrine. The exploitation of a relationship against a trusting party's interests, such as in a case of conflict of interest, can be a legally-cognizable concrete harm even if no other tangible harm manifests.[21] This is significant because American plaintiffs in privacy and data breach lawsuits have struggled to articulate harm that courts will recognize, particularly as the federal courts have tightened the rules for what constitutes a recognizable harm.[22] By contrast, because our common law duties of loyalty are literally older than the United States itself, they offer a tried and tested mechanism to resolve the power imbalances in relationships like those between doctors and patients and platforms and consumers.

A third benefit of a loyalty-based approach to privacy law is that loyalty duties have a long and established development in our law, most famously in the law of fiduciaries. A duty of data loyalty could draw heavily from this tradition and its proven ability to protect against the power imbalances in relationships in a fair, principled, and meaningful way. (We note that the professional ethics of both lawyers and doctors already require that they be loyal to their clients and patients; perhaps those of data scientists should as well.)[23] Loyalty, care, and confidentiality are not just foundational concepts in American law, they are also deeply intuitive. Lawmakers should not underestimate loyalty's rhetorical potential. A rallying cry requiring companies to "act in our best interests" could motivate American privacy reform in the way that "the right to be let alone" did at the turn of the twentieth century. Technocratic terms like "data minimization" and "legitimate interests of the data controller" do little for public imagination or comprehension. By contrast, loyalty is clear, it is easy to understand, and it is potentially robust enough to counterbalance spurious industry claims about the importance of "innovation" or the idea that commercial data processing implicates significant First Amendment issues. GDPR-style ideas like requiring companies to undergo data protection impact assessments can feel wonky and feeble, but every person in America likely knows how it feels to be betrayed.

There is also a roadmap for lawmakers looking to impose duties of loyalty on the powerful. Fiduciary law scholars have identified a tried and tested two-step process that lawmakers use to implement loyalty obligations in such a fair and just way.[24] Lawmakers first articulate a primary, general duty of loyalty—one that can be relatively permissive but acts as a residual backstop against betrayal. Second, courts and lawmakers go about the task of creating and refining what have been referred to as "subsidiary" duties that are more specific and sensitive to context. These subsidiary duties target the most opportunistic contexts for self-dealing and typically result in a mix of overlapping open-ended rules, maxims, more specific standards, and context-specific rules.

Thus, we propose that a duty of data loyalty should be implemented on two levels through what we have called the "loyalty two-step."[25] The first level is a broad and general "catch all" prohibition on substantial conflicts with the trusting party's best interests. This would prevent the most egregious forms of disloyalty across the board, and it would also serve to orient the company's incentives generally against betrayal

[21] *See* TAMAR FRANKEL, FIDUCIARY LAW 107–08 (2011) ("The duty of loyalty supports the main purpose of fiduciary law: to prohibit fiduciaries from misappropriating or misusing entrusted property or power. Thus, the duty of loyalty is manifested by important preventative rules. Such rules prohibit actions even though they are not necessarily injurious to entrustors."); see also *Spokeo v. Robbins* 136 S.Ct. 1540 (2016).
[22] See, e.g., *TransUnion LLC v. Ramirez,* 141 S.Ct. 2190 (2021); *Spokeo, Inc. v. Robins,* 136 S.Ct. 1540 (2016).
[23] Richards & Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 968 (2021).
[24] *See e.g.* Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care* in THE OXFORD HANDBOOK OF FIDUCIARY LAW 419 (Evan J. Criddle et al., 2019). ("The duties of loyalty and care, which we might call the primary fiduciary duties, are typically structured as broad, open-ended standards that speak generally. By contrast, the other fiduciary duties, which we might call the subsidiary or implementing fiduciary duties, are typically structured as rules or at least as more specific standards that speak with greater specificity.").
[25] *See* Hartzog & Richards, *supra* note 5.

rather than micromanaging specific instances. It would also supply a backstop against novel or innovative forms of betrayal that allows the law to evolve for new circumstances. The second level subsidiary duty of loyalty rules should be more specific and, where necessary, restrictive. This would involve the articulation of specific and substantive rules targeting particular contexts and actions that provide clearer rules than the general duty and would leave less wiggle room to ensure accountability. This clarity will keep the frameworks from becoming watered down. In the health care context, for example, bright-line rules should be more restrictive where companies are using personal health data for marketing or persuasion, or where they are collecting location data, but more permissive where personal health data is being used for biomedical research in the public interest. Through this layered approach, a duty of data loyalty could provide both general applicability as well as sensitivity to specific contexts.[26]

There is already bipartisan support for a duty of loyalty, including the proposed American Data Privacy and Protection Act (ADPPA).[27] However, the best starting point for statutory language is the proposed bipartisan Digital Consumer Protection Commission Act of 2023 (DCPCA) for online platform regulation.[28] The relevant language appears in Section 2411:

> ‘‘**SEC. 2411. DUTY OF LOYALTY.**
>
> A covered entity may not process personal data or design information technologies in a way that substantially conflicts with the best interests of a person with respect to—
>
> (1) the experience of the person when using a platform owned or controlled by the covered entity;
> or
> (2) the personal data of the person.”[29]

An advantage of using this language as a starting point is that it builds on any bipartisan support that the DCDPA already has. If this Committee is further interested in how a duty of loyalty might be developed in legislation, we have attached our article *Legislating Data Loyalty*, appearing in the *Notre Dame Law Review Reflection*. And of course, we stand ready to help in any further ways that the Committee might find helpful as it tackles this complex and important set of policy issues.

In conclusion, we believe that a duty of loyalty provides the strongest, and most comprehensive protections against the misuse of consumer data by the creators and deployers of LLMs. This duty, implemented through the loyalty two-step described above could address the potentially hungry, leaky, sneaky, and exclusory effects of the unfettered proliferation of LLMs.

---

[26] *Id.*
[27] *See* Woodrow Hartzog & Neil Richards, *We’re So Close to Getting Data Loyalty Right*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (June 14, 2022), https://iapp.org/news/a/were-so-close-to-getting-data-loyalty-right/.
[28] Digital Consumer Protection Commission Act of 2023, S. 2597, 118th Cong. (2023).
[29] *Id.* at § 2411.

Respectfully submitted,

Woodrow Hartzog, Professor of Law at Boston University and Cordell Institute Fellow [30]
Neil Richards, Koch Distinguished Professor of Law at Washington University and Cordell Institute Faculty Director[31]
Ryan Durrie, Cordell Institute Associate Director[32]

[30] Professor of Law, Boston University; Faculty Associate, Berkman Klein Center for Internet & Society at Harvard University; Affiliate Scholar, Stanford Law School Center for Internet & Society.
[31] Koch Distinguished Professor in Law and Director, Cordell Institute, 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.
[32] Associate Director for Policy, Cordell Institute, Washington University in St. Louis. We would also like to thank our Cordell Institute Research Fellow Agnish Chakraburtty for his assistance with this response.

# LEGISLATING DATA LOYALTY

*Woodrow Hartzog* & Neil Richards***

*Lawmakers looking to embolden privacy law have begun to consider imposing duties of loyalty on organizations trusted with people's data and online experiences. The idea behind loyalty is simple: organizations should not process data or design technologies that conflict with the best interests of trusting parties. But the logistics and implementation of data loyalty need to be developed if the concept is going to be capable of moving privacy law beyond its "notice and consent" roots to confront people's vulnerabilities in their relationship with powerful data collectors.*

*In this short Essay, we propose a model for legislating data loyalty. Our model takes advantage of loyalty's strengths—it is well-established in our law, it is flexible, and it can accommodate conflicting values. Our Essay also explains how data loyalty can embolden our existing data privacy rules, address emergent dangers, solve privacy's problems around consent and harm, and establish an antibetrayal ethos as America's privacy identity.*

*We propose that lawmakers use a two-step process to (1) articulate a primary, general duty of loyalty, then (2) articulate "subsidiary" duties that are more specific and sensitive to context. Subsidiary duties regarding collection, personalization, gatekeeping, persuasion, and mediation would target the most opportunistic contexts for self-dealing and result in flexible open-ended duties combined with highly specific rules. In this way, a duty of data loyalty is not just appealing in theory—it can be effectively implemented in practice just like the other duties of loyalty our law has recognized for hundreds of years. Loyalty is thus not only flexible, but it is capable of breathing life into America's historically tepid privacy frameworks.*

## INTRODUCTION

American privacy law is in a rut. It has no privacy identity. Its traditional rules mandating transparency and consent are outdated,

© 2022 Woodrow Hartzog & Neil Richards. Individuals and nonprofit institutions may reproduce and distribute copies of this Essay in any format at or below cost, for educational purposes, so long as each copy identifies the authors, provides a citation to the *Notre Dame Law Review Reflection*, and includes this provision in the copyright notice.

* Professor of Law and Computer Science, Northeastern University.

** Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis. Portions and ideas in this Essay are adapted from and developed in much greater detail in the authors' other articles: *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492 (2020); *A Duty of Loyalty for Privacy Law,* 99 WASH. U. L. REV. 961 (2021); and *The Surprising Virtues of Data Loyalty,* 71 EMORY L.J. (forthcoming 2022).

The authors would like to thank Giuliana Green, Sara Hubaishi, Alexis Johnson, and Nina Sprenger for their research assistance. This research was supported by an award from the Notre Dame-IBM Tech Ethics Lab and by Notre Dame-IBM Tech Ethics Lab and by NSF award 1956393/1955227/1956435/2103439: "SaTC: Frontiers: Collaborative: Protecting Personal Data Flow on the Internet" as part of the ProperData project.

porous, and poorly enforced. It is a far cry from the "adequacy" necessary for a profitable and sustainable data trade with the European Union (EU) and Britain. It has, in short, proven no match for the likes of the modern tech giants and a world awash in data and devices. What's worse, while privacy reform appears to be on the agenda, many of the existing proposals—particularly those touted as "business-friendly"—are so weak as to risk codifying a privacy rights status quo that virtually everyone agrees is unacceptable.[1] In searching for a meaningful new approach to regulating data privacy, lawmakers have begun to seriously explore the idea that tech companies should be bound by a duty of loyalty to those who trust them with their data and online experiences.[2]

Scholars have proposed versions of a duty of loyalty for the past twenty years, but not all lawmakers are convinced.[3] Some may be

1 This is an argument we have been making for several years. *See e.g.*, Woodrow Hartzog & Neil Richards, Opinion, *There's a Lot to Like About the Senate Privacy Bill, if It's Not Watered Down*, THE HILL (Dec. 6, 2019), https://thehill.com/opinion/technology/472892-theres-a-lot-to-like-about-the-senate-privacy-bill-if-its-not-watered [https://perma.cc/W87Y-ZGPG]; Woodrow Hartzog & Neil Richards, Opinion, *It's Time to Try Something Different on Internet Privacy*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-0315-11e9-9122-82e98f91ee6f_story.html [https://perma.cc/W63X-UHCP].

2 *See, e.g.*, Data Care Act of 2019, S. 2961, 116th Cong. § 3(b)(2) (2019) (Duty of Loyalty—An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 101 (2019) (Duty of Loyalty. (a) In General.—A covered entity shall not—(1) engage in a deceptive data practice or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act); New York Privacy Act, S. 5642, 2019–2020 Reg. Sess. (N.Y. 2019) ("Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances."); *Commission Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020); Data Protection Act 2018, c. 123 (UK); An Act to Provide Facial Recognition Accountability and Comprehensive Enforcement, H.R. 117, 192d Gen. Ct., §2(a) (Mass. 2021) ("A covered entity shall be prohibited from taking any actions with respect to processing facial recognition data or designing facial recognition technologies that conflict with an end user's best interests.").

3 *See, e.g.*, Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020) [hereinafter Balkin, *The Fiduciary Model*]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) [hereinafter Balkin, *Information Fiduciaries*]; Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*]; Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*,

concerned that it is too vague, or that it would be bad for business. Others wonder what data loyalty would get us that we couldn't get from EU or California-style statutes. Others are uncertain about how a duty of loyalty would work and what specific legislation for data loyalty should look like.

In this short Essay, we propose a model for legislating data loyalty. Our model takes advantage of loyalty's strengths—it is well-established in our law, it is flexible, and it can accommodate conflicting values. Our Essay also explains how data loyalty can and should fit within the existing fabric of information privacy law, building on our research exploring how better privacy rules can protect and build trust in relationships between consumers and companies. It lays out the *what* and the *why* of data loyalty for legislators seeking a robust alternative to the failed "notice-and-choice" regime in the United States.

Our argument is simple—a duty of data loyalty is not just appealing in theory—it can be effectively implemented in practice just like the other duties of loyalty our law has recognized for hundreds of years. Loyalty is not only flexible, but it is capable of breathing life into America's historically tepid privacy efforts. It is a meaningful alternative to ineffective regimes that rely too much upon illusory notions of consent and restrictive notions of harm, while being flexible enough to confront new privacy challenges and accommodating mutually beneficial data practices. A properly implemented duty of loyalty could thus represent an answer to many of the problems of information privacy, creating real value for consumers, businesses, and our society as a whole.

---

46 J. CORP. L. 143 (2020); *see also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34 (2020); Lilian Edwards, *The Problem with Privacy: A Modest Proposal*, 18 INT'L REV. L. COMPUTS. & TECH. 309 (2004); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (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/L8DQ-SK79]; Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CANADIAN BUS. L.J. 419 (2001); 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 (2020); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 612 (2015); DANIEL J. SOLOVE, THE DIGITAL PERSON (2004); *but see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

## I. WHAT IS DATA LOYALTY?

Data loyalty is the simple idea that the organizations we trust should not process our data or design their tools in ways that conflict with our best interests. It borrows from notions of loyalty in fiduciary law, but it is distinct from them. The model we propose here would be crafted by legislators to the specific vulnerabilities and incentives in the relationships between consumers and the data-extractive companies they deal with every day.

Scholars have proposed duties of loyalty in a variety of forms—including loyalty duties for data collectors, "information fiduciaries," or fiduciary boilerplate—in part because loyalty represents a substantive check on the ability of companies to use human data to nudge, influence, coerce, and amass vast profits from the exploitation of human information.[4] It cannot be avoided by trickery, hidden fine print, or manipulative interfaces known as "dark patterns." At its core, it protects the expectations consumers bring to relationships with companies, and it builds trust in those relationships that allows them to flourish to the benefit of both parties.

In other work we have articulated a duty for loyalty for privacy law as the duty of data collectors to act in the best interests of those whose data they collect.[5] A duty of loyalty for privacy law is neither perfect nor a tool for all tasks. But loyalty has one great virtue: it places the focus for information age problems on the relationships that define our social lives rather than on the data which is the byproduct of those relationships. Loyalty shifts the law's attention from the procedural rules of privacy law that are too easy to manipulate ("Did you hide a vague sentence in the privacy policy?" "Did the consumer fail to hit the tiny opt-out button?") to the substantive question of what practices go too far. It is flexible and adaptable across contexts, cultures, and times. Loyalty can thus be a powerful response to what Shoshana

4 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3; Balkin, *Information Fiduciaries*, *supra* note 3; Richards & Hartzog, *Duty of Loyalty*, *supra* note 3; Scholz, *supra* note 3; *see also* WALDMAN, *supra* note 3; Haupt, *supra* note 3; Edwards, *supra* note 3; Savage, *supra* note 3; Zittrain, *supra* note 3, at 340; Barrett, *supra* note 3; Dobkin, *supra* note 3, at 1; Kerry, *supra* note 3; Kerr, *supra* note 3; Whitt, *supra* note 3; Brennan-Marquez, *supra* note 3, at 612; SOLOVE, *supra* note 3.

5 *See, e.g.*, Richards & Hartzog, *Duty of Loyalty*, *supra* note 3; Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. (forthcoming 2022); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) [hereinafter Hartzog & Richards, *Privacy's Constitutional Moment*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019) [hereinafter Richards & Hartzog, *Pathologies of Digital Consent*]; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017) (book review).

Zuboff calls "surveillance capitalism," the claiming of "human experience as free raw material for hidden commercial practices of extraction, prediction, and sales . . . As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth."[6]

Data loyalty has three key features—it is a (1) *relational duty* (2) that *prohibits self-dealing* (3) at the *expense of a trusting party*. Let's break these three features apart.

### *A. A Relational Duty*

Lawmakers who decide they want to regulate privacy can begin their task by focusing on at least three different things. First, they could focus on the data itself, like what can be collected and whether datasets are deidentified. This is the approach that most federal and European privacy laws have taken to date with laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Second, there are structural concerns, like requiring companies to appoint a data privacy officer or focusing on monopoly power. This is the approach familiar to antitrust and corporate law. There's also a third option—lawmakers could focus on our relationships, like requiring confidentiality from physicians, lawyers, and other professionals.[7]

In addition to being one of the oldest contexts for privacy to flourish, relationships have a few distinct advantages for lawmakers looking to fight the excesses and abuses of data-hungry organizations. First, relational duties are acutely sensitive to the *power disparities* within information relationships. Tech companies control what we see, what we can click on, and what sorts of information they want to extract from their customers. They have incredible resources that help them predict and nudge our behavior and have the financial incentive to keep us ever more exposed. Duties of loyalty protect against self-dealing, while related duties of care placed on relationships protect against dangerous behavior and the risks of harm. The greater the power imbalance and the more vulnerable people are through exposure, so should the duty to which the trusted party is held be greater.[8]

Second, relational duties are a way out of *privacy's consent trap*. For years lawmakers, regulators, and companies have been obsessing over whether the consent people gave was a truly meaningful, informed, and revocable choice. People click "I Agree" buttons and slightly

6 SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER, at vii (2019).

7 *See* Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1697.

8 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3, at 13–14.

wince without reading the terms because it is impossible to do so, even when what they click states that they read and understand the terms. Consent is broken, but lawmakers have stuck to notice and consent regimes anyway, even though it is common knowledge that digital consent is rarely meaningful. Relational duties allow for a decoupling of choice and consent. These duties allow trusting parties 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.[9]

Finally, relationships open the possibility of more *robust enforcement rules* because they are voluntarily entered into and hold a unique place in the law as a result. The concept of contractual privity could also be used to extend relational duties beyond the initial trusting party and entrustee. Under a "chain-link" approach to relational privacy rules, lawmakers could directly—or using mandated terms in data-sharing contracts—link the disclosure of personal information to obligations of loyalty to protect information as it is disclosed downstream.[10] To create the chain of protection, contracts would be used to link each new recipient of information to a previous recipient who wished to disclose the information. At the same time, relational duties raise even fewer free expression issues than other forms of data regulation because they regulate relationships rather than information flows. In relationships, parties assume these duties by soliciting trust and voluntarily entering into these relationships. Moreover, protections for power-imbalanced relationships have a deep tradition in U.S. law in harmony with free expression frameworks. This is, for example, why lawyers do not have a First Amendment right to disclose client confidences, no matter how "newsworthy" they might be.[11]

For these reasons, shifting the focus of privacy law from data to relationships offers significant advantages for effective policy.

---

9 For an extended critique of consent-based models for data processing, see Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 5.

10 *See* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 658–61 (2012).

11 *Cf.* Balkin, *Information Fiduciaries*, *supra* note 3; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1057–58 (2000) (explaining that enforcement of contracts to maintain confidentiality create no First Amendment problems); Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887 (2006). *But see* Khan & Pozen, *supra* note 3.

### *B. That Prohibits Self-Dealing*

Many of the problems of surveillance capitalism come down to the problem of self-dealing, where an organization exploits an advantage over a trusting party to its own benefit.[12] The failures of American privacy law have enabled such corporate opportunism and manipulation of consumers using human information. This problem is particularly serious in the context of "personalized" technologies that promise to know us so that they can better satisfy our needs and wants. Insufficiently constrained by privacy law and driven to maximize quarterly profits by corporate law, companies can deploy a potent cocktail of techniques derived from cognitive and behavioral science to "nudge" or otherwise influence the choices we make.[13] These highly capitalized tech companies have not acted like the benevolent choice architects some had hoped for.[14] Technologies—and choice architecture—advertised as serving consumers have instead become weaponized, serving commodified consumers up to the companies and their commercial and political advertiser clients.[15]

Loyalty rules directly prohibit conflicted self-dealing. In so doing, they can change the incentives and business models of entire industries. Many critics believe that U.S. data privacy law has failed to change the corrosive business models that endanger, manipulate, mislead, misinform, and polarize people every day. The law, these critics suggest, merely prunes the edges of wrongdoing rather than getting to the core of the problem.[16] A duty of data loyalty would directly address this problem by taking self-dealing off the table as a general matter. More specific, subsidiary data loyalty rules for targeted advertising, web scraping, manipulative interfaces, and optimized human engagement metrics could revolutionize entire industries with clearer rules of the road. They could make certain abusive business models obsolete overnight. This would be a sharp contrast to the piecemeal and procedural approach of current U.S. data privacy law, which presupposes that all possible extraction models can be valid if they follow the right procedures and give people some semblance of control over their information. Data loyalty rules instead look directly to corporate profit motives and ask if they conflict with a trusting

12 *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); ZUBOFF, *supra* note 6.

13 *See* NEIL RICHARDS, WHY PRIVACY MATTERS 39–50 (2022).

14 *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 11–13 (2008).

15 *See* RICHARDS, *supra* note 13, at 46–49.

16 *See, e.g.*, Facebook, Inc., F.T.C. No. 1823109 (July 24, 2019) (Chopra, Comm'r, dissenting); Facebook, Inc., F.T.C. No. 1823109 (July 24, 2019) (Kelly, Comm'r, dissenting).

party's best interests. They require profit models to be based on the provision of valuable services rather than exploitation and extraction.

### *C. At the Expense of a Trusting Party*

Loyalty rules safeguard trusting parties from betrayal, looking to whether a trusting party has been disadvantaged by an organization's self-dealing. When organizations enrich themselves with trusting parties' data, people consistently end up paying with their time, attention, mental well-being, reputation, and significant life opportunities.[17] These costs include everything from notifications interrupting our attention to advance the interests of the platform, to manipulative advertising that causes people to buy (or vote) differently in ways that serve advertisers, to the well-documented emotional injuries wrought by engagement-driven social media. Crucially, these costs, impositions, and manipulations are made substantially more damaging by "personalization" enabled by self-dealing in personal data. Thus, it's not just a random notification or one serving your interests like a reminder to attend a meeting, but one teasing you out of the blue that someone you know may have done something cool. It's not just an ad or a political message, but one calculated to your precisely known psychology and vulnerabilities.[18] And it's not just social media telling you what your friends are doing, it's being done in a way that is calibrated to push your buttons to keep you scrolling (or doom-scrolling) with a reckless indifference to your mental health.[19]

The scope of protection that loyalty rules safeguard includes, but is broader than, recognized privacy harms like identity theft, emotional harms, breaches of confidence, and dangerous exposure.[20] It also includes more subtle individual and collective costs to our identity, our ability to create relationships, our collectively held truths, and the obscurity that protects our ability to share and move about freely. As

17 *See* Neil Richards & Woodrow Hartzog, *Against Engagement* (draft manuscript) (on file with authors).

18 This is precisely what happened in the Cambridge Analytica scandal, in which Facebook data was used to create finely calibrated psychological profiles of voters identified by their real names, suggesting which kinds of arguments would be most effective at getting them to act in the ways that the paying political advertisers wanted them to. *See* RICHARDS, *supra* note 13, at 25–26.

19 These are the allegations Facebook whistleblower Frances Haugen presented under oath before lawmakers in the United States and around the world in 2021. *See, e.g.*, Billy Perrigo, *Inside Frances Haugen's Decision to Take on Facebook*, TIME (Nov. 22, 2021) https://time.com/6121931/frances-haugen-facebook-whistleblower-profile/ [https://perma.cc/L8QN-6GD5].

20 *See, e.g.*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

such, it protects against the full range of betrayals that powerful parties in an information relationship can engage in.

* * *

Loyalty duties are thus quite straightforward when understood as relational duties that prevent self-dealing at the expense of a trusting party. They accord with basic notions of fairness and decency—if you have power over someone who trusts you, you shouldn't betray them or manipulate them to serve your own interests. It is undoubtedly for these reasons that our law has placed duties of loyalty on relationships with power imbalances for centuries in a wide variety of contexts.

## II. WHY DATA LOYALTY?

One common question that proposals for a duty of data loyalty often face is, "What does a duty of loyalty get you that other approaches to regulation do not?" This is an excellent question that asks why a duty of loyalty might be the right regulatory tool rather than some other approach. We believe that duties of data loyalty offer four important advantages that other approaches do not.

First, loyalty represents a central policy commitment that could be the missing ingredient to embolden existing U.S. privacy frameworks. Second, it is substantially more capable than a traditional data protection approach when it comes to modern privacy problems like algorithmic discrimination, manipulation, oppression, and shaming that are caused by unceasing digital contact and the astonishing scale and power of modern technology platforms. Third, loyalty helps solve privacy law's harm problem in a way that is consistent with the direction of current Supreme Court doctrine. Finally, data loyalty has a straightforward and strong rhetorical appeal; it offers a clear explanation for better privacy rules, it could help define America's privacy identity, and it could be used to gather broad popular support for stronger privacy rules.

### *A. To Embolden Existing Data Privacy Frameworks*

Law professor Ryan Calo is fond of saying that technology law's biggest problem is that we lack the political will to enforce the rules we already have.[21] We believe that this problem persists in privacy law as

21 *See, e.g.*, Ryan Calo, *Artificial Intelligence and the Carousel of Soft Law*, 2 IEEE TRANSACTIONS ON TECH. & SOC'Y 171, 171 (2021) ("But ultimately what is missing is not knowledge about the content of ethics as much as political will."); *Enlisting Big Data in the Fight Against Coronavirus: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2020) (statement of Ryan Calo, Law Professor, University of Washington) ("It is also

well. Many privacy regulators lack the same political will and support from lawmakers and the executive branch to enforce existing data rules in a robust way. Many privacy rules are also vague, leaving their interpretation (and enforcement based upon that interpretation) up in the air. For example, what constitutes an "unfair trade practice," a "reasonable expectation of privacy," or the collection of "more data than is necessary" is a perennial topic of debate.

One of the reasons why U.S. data privacy frameworks tend to wilt is that they lack a clear touchstone to guide interpretation that would lead to effective enforcement. The collection of U.S. privacy statutes, enforcement actions, and common law remedies adhere to basic commitments like "do not lie," "do not harm," and "follow the Fair Information Practices (FIPS)."[22] But such edicts tend not to interrogate the wrongful motives of data processors and do little to force companies into any practice beyond bare compliance.

A duty of loyalty could change that. Lawmakers should use loyalty duties to embolden and revitalize *existing* approaches to regulating data privacy, such as robust implementation of data minimization requirements, rules against unfair and deceptive trade practices, and expansion of products liability theories of accountability. Data loyalty can empower lawmakers to use tools that have already been developed, by expanding the contexts in which rules should be followed, who must follow them, and the level of adherence necessary for compliance.

Take as an example data minimization, the idea that organizations should only collect, maintain, and use data that is necessary to fulfill a designated and legitimate purpose. Data minimization rules are a fundamental commitment of data protection and data security laws. They are scattered throughout U.S. law, including the California Consumer Privacy Act,[23] the Wiretap Act,[24] and are implicitly a part of

---

important to note that a lack of political will is sometimes the greater hurdle than a lack of information.").

22 *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 15 (2018); Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1704 & n.66; Richards & Hartzog, *Duty of Loyalty*, *supra* note 3, at 42.

23 CAL. CIV. CODE § 1798.100(c) (2018) ("A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not processed in a manner that is incompatible with those purposes.").

24 18 U.S.C. § 2518(5) (2018) ("No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. . . . Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to

the data security requirements of Section 5 of the FTC Act.[25] Data minimization, if robustly interpreted and enforced as a way for companies to remain loyal to trusting parties, could be a remarkably effective tool for regulators since it targets both collection and use of data and is meant to counter abusive purpose creep by companies.[26] If data loyalty became a guiding obligation for data minimization rules, it would give regulators and judges interpreting potential violations an additional layer of interrogation. Data loyalty would compel an examination of a company's motives *and* the potential adverse consequences to consumers in determining if more data than necessary was collected or if the use of data deviated too far from its original purpose. Such foundational support would prevent an arid and strictly textual analysis by explicitly forcing regulators and judges to look at the big picture of exploitative motives of organizations and the trusting parties' wellbeing.

Another example would be laws based on the Fair Information Practices, the most common standard for privacy laws worldwide. Under current U.S. privacy law, perhaps the most important question for regulators and compliance professionals is whether consumers have been given "notice and choice." In principle, this is a good thing, emphasizing consent to data practices and evoking the gold standard of "knowing and voluntary" consent familiar to lawyers and medical researchers. But in practice, under current American law, "notice and choice" all too often means just that consumers have merely vague "notice" of data practices that are buried in the fine print and illusory "choice" with respect to these practices such as a take-it-or-leave-it choice about whether to use the service.

In practice, such rules not only place few constraints on companies, but they also represent a kind of cookbook to create and justify even deeply disloyal data practices by checking the boxes of fictional notice and illusory consent. This is likely why companies like Amazon have been engaged in aggressive lobbying in many state capitols to get weak notice-and-choice (and only weak notice-and-

interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.").

25 *See* FTC, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (2014) ("The Commission has also provided educational materials to industry and the public about reasonable data security practices. These materials explain that, while there is no single solution, such a program follows certain basic principles. . . . [Among them,] companies should limit the information they collect and retain based on their legitimate business needs so that needless storage of data does not create unnecessary risks of unauthorized access to the data.").

26 *See, e.g.*, DANIEL SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (forthcoming 2022).

choice) laws on the books.[27] But here, too, a duty of loyalty could help. If data loyalty became a guiding obligation for data processing, notice-and-choice requirements would become more than a checkbox compliance exercise at best and a cookbook for manipulation at worst. Instead, "notice" would become an obligation of honesty, ensuring that consumers actually understood what was happening with their data before they agreed to it, and preventing companies from all sorts of self-interested practices where meaningful understanding was not present. "Choice" would mean knowing and voluntary agreement to particular data practices among reasonable alternatives that do not conflict with a trusting party's best interests, rather than a "choice" about whether to live in the modern world or not.

In these ways, by reorienting the question for companies from "What can we get away with" to "Are we being loyal to our human customers," a duty of data loyalty could breathe new life into existing regimes that are moribund at best and exploitation-enabling at their worst.

### *B. To Address Emergent Dangers*

A second benefit of data loyalty is that it can safeguard consumers against novel and emerging digital risks. Data loyalty duties can *go beyond* the standard data processing concerns and traditional privacy harms. In crafting such rules, lawmakers should look to the ways in which the affordances of modern technologies endanger people by bestowing power in trusted entities. Data loyalty duties should scrutinize how those organizations have incentives to use the power human information gives them in self-interested ways that conflict with a trusting party's best interests. Duties crafted in this way would meaningfully respond to concerns about manipulative user interfaces (sometimes called "dark patterns"), the wrongful extraction of human labor by dominant platforms, algorithmic discrimination, and protection against third parties and other users while using a service. Duties of data loyalty can thus go beyond often hard-to-quantify injuries of individual pieces of data and address the structural power imbalances and inequalities that characterize the relationships between individual harried consumers and the richest corporations in the history of the world.

27 *See* Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, REUTERS (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/ [https://perma.cc/LE8N-PBCM].

### *C. To Solve Privacy's Harm Problem*

Third, and related to the problem of emergent dangers, a duty of data loyalty would help lawmakers solve one of privacy law's most difficult problems: the problem of cognizable harm. Many privacy rules require some kind of economic, physical, emotional, or other kind of concrete and traditionally recognized harm to be legally cognizable. However, loyalty rules look to the trusted party's inequitable conduct of wrongfully exploiting an advantage gained by an information relationship. The exploitation of the relationship against a trusting party's interests can itself be the wrong, such as in a case of conflict of interest, even if no other tangible harm manifests.[28]

In privacy cases, this is significant because American plaintiffs in privacy and data breach lawsuits have struggled to articulate diffuse but real informational injuries, and this situation has been made worse in recent years as courts have tightened the rules for what counts as a legally cognizable injury under Article III standing doctrine.[29] Critically, loyalty duties do not have this problem—not just because the legal injury in loyalty cases is the disloyalty itself, but because this injury is one that has been already recognized by courts as legally sufficient within standing doctrine.[30]

The focus of loyalty is on the integrity of a relationship and removing an incentive and ability to wrongfully profit by taking advantage of a power disparity. Because loyalty duties are rooted in betrayal rather than harm or injury, they have significant consumer

28 *See* TAMAR FRANKEL, FIDUCIARY LAW 107–08 (2011) ("The duty of loyalty supports the main purpose of fiduciary law: to prohibit fiduciaries from misappropriating or misusing entrusted property or power. Thus, the duty of loyalty is manifested by important preventative rules. Such rules prohibit actions even though they are not necessarily injurious to entrustors.").

29 *See, e.g.*, TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2214 (2021); Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016).

30 To get a bit technical for a moment, in *TransUnion*/*Spokeo* terms, then, a breach of a legally imposed duty of loyalty would be a "concrete" and "traditionally recognized" intangible harm. To satisfy this requirement, *Spokeo* requires courts "to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo*, 578 U.S. at 341. *Ramirez* uses a slightly different formulation—asking whether an intangible injury bears "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Ramirez*, 141 S. Ct. at 2204. But because a breach of a duty of loyalty has been recognized as a basis for lawsuits for centuries, duties of loyalty simply do not raise concreteness problems. *See also* Citron & Solove, *supra* note 20. By contrast, although duties of care in general would be concrete, statutory causes of action rooted in novel theories of harm (including procedural data protection requirements) would seem to have to run through the *Spokeo* test, with an uncertain likelihood of success.

protection advantages over existing privacy rules that demand proof of injury.[31]

### *D. To Define America's Privacy Identity*

Finally, a duty of data loyalty could offer a defining value for America's privacy law identity, rather than forcing it to adopt a watered-down and sometimes ill-fitting version of the European GDPR approach. While American privacy law is weak, permissive, and seemingly rudderless, in Europe, privacy law is on firmer ground. Privacy and data protection are both considered fundamental human rights in the EU.[32] The GDPR is the manifestation of these rights, a commitment to the idea that people should be able to determine their informational fates for themselves. Bilyana Petkova has argued that data protection is "the main tenet of constitutional identity" in the EU.[33] This is why European data protection law often seems so strikingly powerful to American observers compared to domestic consumer privacy rights. As much as anything, then, for Europeans the GDPR is a state of mind. And it is why a U.S. version of the GDPR would inevitably be both a weak and inadequate version of the real GDPR, something we have elsewhere called a "GDPR-lite."[34]

A duty of loyalty could fill this definitional role for U.S. privacy law. It could supply a political lodestar for privacy reform that defines America's privacy identity on its own terms rather than those of the EU. Lawmakers should not underestimate loyalty's rhetorical potential. A rallying cry requiring companies to "act in our best interests" could motivate American privacy reform in the way that "the right to be let alone" did at the turn of the twentieth century. Technocratic terms like "data minimization" and "legitimate interests of the data controller" do little for public imagination or comprehension. By contrast, loyalty is clear, it is easy to understand, and it is potentially robust enough to counterbalance spurious industry claims about the importance of "innovation" or the idea that commercial data processing carries First Amendment value. GDPR-style ideas like requiring companies to undergo data protection impact assessments can feel wonky and feeble, but every person in America likely knows how it feels to be betrayed.

---

31 *See, e.g.*, H.R. 117, 192d Gen. Ct., §2(a) (Mass. 2021) ("A covered entity shall be prohibited from taking any actions with respect to processing facial recognition data or designing facial recognition technologies that conflict with an end user's best interests.").

32 *See, e.g.*, U.N. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221; Charter of Fundamental Rights of the European Union arts. 7–8, 2000 O.J. (C 364).

33 Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 140, 154 (2019).

34 For an extended version of an argument along these lines, see Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1727–32.

If companies owe us duties of loyalty, then "innovative" uses of data to exploit us start to resemble betrayal and fraud, and claims of First Amendment protection for manipulative uses of data look appropriately laughable. Loyalty also has the virtue of placing the obligation for ethical data processing right where it belongs, ensuring those to whom we expose our data vulnerabilities do not betray us. A duty of loyalty in privacy law would be important not just as a set of rules, but as an *idea* capable of rallying democratic support for strong rules.

Finally, loyalty can be good for business. At a U.S. Senate hearing in 2020, Senator Brian Schatz expressed the idea that duties of loyalty are only needed for bad businesses, because good businesses know that the best way to make money over the long term is to be loyal to their customers.[35] On the other hand, if disloyalty is permitted by the law, the pressures on business to show quarterly profits create strong short-term and short-sighted incentives to cheat and behave in disloyal ways. This in many respects is the story of the contemporary digital economy, a story that data loyalty offers the potential to change for the better.

## III. A MODEL FOR LEGISLATING DATA LOYALTY

One undeniable virtue of creating a duty of data loyalty is that it would not be necessary to invent it from whole cloth. Loyalty duties have a long and established pedigree in our law, most famously in the law of fiduciaries. A duty of data loyalty could draw heavily from this tradition and its proven ability to protect against the power imbalances in relationships in a fair, principled, and meaningful way.

Fiduciary law scholars have identified a two-step process lawmakers use to implement loyalty obligations in such a fair and just way.[36] Lawmakers initially articulate a primary, general duty of loyalty. Next, courts and lawmakers go about the task of creating and refining what have been referred to as "subsidiary" duties that are more specific and sensitive to context. These subsidiary duties target the most opportunistic contexts for self-dealing and typically result in a mix of overlapping open-ended rules, maxims, more specific standards, and highly specific rules.

---

35 *See Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2020) (statement of Sen. Brian Schatz).

36 *See, e.g.*, Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 419 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) ("The duties of loyalty and care, which we might call the *primary* fiduciary duties, are typically structured as broad, open-ended standards that speak generally. . . . By contrast, the *other* fiduciary duties, which we might call the *subsidiary* or *implementing* fiduciary duties, are typically structured as *rules* or at least as *more specific standards* that speak with greater specificity.").

Thus, we propose that a duty of data loyalty should be implemented on two levels. The first level is a broad and general prohibition on substantial conflicts with the trusting party's best interests. This would prevent the most egregious forms of disloyalty across the board, and it would also serve to orient the company's incentives generally against betrayal rather than micromanaging specific instances. The second level of a duty of loyalty would be more specific and, where necessary, restrictive. This would involve the articulation of specific and substantive subsidiary duties targeting particular contexts and actions that provide clear rules and less wiggle room to ensure accountability and keep the frameworks from becoming watered down. Though this two-step approach, a duty of data loyalty could provide both general applicability as well as sensitivity to individual contexts.

### *A. First, a General Catchall Duty*

We propose a general rule of data loyalty as follows:

*Organizations shall not process data or design systems and tools in ways that significantly conflict with trusting parties' best interests that are implicated by their exposure.*

Let's break this proposed duty down a little.

#### 1. A No-Conflict Rule for Data and Design

Organizations gain a power advantage over trusting parties in two different ways: collecting and processing data and controlling our mediated experiences.[37] If the duty of loyalty is to accomplish anything, it should prohibit the conflicted design of digital tools and data processing. Avoiding conflicts is loyalty's core mandate and the logical starting point for lawmakers, judges, industry, and civil society. A general rule against conflicted design and data processing could serve as the foundation for a host of regulatory regimes, self-regulatory efforts, and guidance to the public to encourage and nurture its trust.

A general no-conflict rule has the remarkable advantage of directing lawmakers (and trusted parties themselves) to interrogate not just actions but *motives* and *gains*.[38] Established fiduciary no-conflict rules

37 *See, e.g.*, RICHARDS, *supra* note 13; HARTZOG, *supra* note 22.

38 *See* Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513, 557–58 (2015) (quoting Lionel Smith, *The Motive, Not the Deed*, *in* RATIONALIZING PROPERTY, EQUITY AND TRUSTS: ESSAYS IN HONOUR OF EDWARD BURN 53, 67 (Joshua Getzler ed., 2003) ("[T]he motives of the fiduciary are the crucial element in determining whether

> do not require the fiduciary to act in any particular way but are instead thought to establish boundaries within which the fiduciary may reasonably be expected to act loyally, at least to the extent that the rules isolate biasing factors that might induce the fiduciary to subjugate the interests of beneficiaries to the interests of others.[39]

## 2. People Over Profits

Some lawmakers are reluctant to adopt duties of data loyalty because they fear creating a conflict with the duties of loyalty that directors of organizations owe to shareholders.[40] This is an illusory conflict and, at most, is resolvable by lawmakers without substantially remaking corporate law.[41] The supposed conflict between trusting parties and shareholders has been wildly overstated.[42] Fiduciary law scholar Andrew Tuch explains that "imposing user-regarding

---

the fiduciary has acted loyally, and the requirement of motive is quite specific—the fiduciary 'must act (or not act) in what *he perceives to be* the best interests of the beneficiary.'")).

39 *Id.* at 557.

40 One of the most repeated critiques levied against the idea of imposing duties of data loyalty on companies is Lina Khan and David Pozen's claim that relational rules might create conflicting loyalties. The authors assert that "[t]he tension between what it would take to implement a fiduciary duty of loyalty to users, on the one hand, and these companies' economic incentives and duties to shareholders, on the other, is too deep to resolve without fundamental reform." Khan & Pozen, *supra* note 3, at 529, 534 ("[T]he information-fiduciary proposal could cure at most a small fraction of the problems associated with online platforms—and to the extent it does, only by undercutting directors' duties to shareholders, undermining foundational principles of fiduciary law, or both.").

41 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3, at 23 ("Management's fiduciary obligations to shareholders *assume* that the corporation will attempt to comply with the legal duties owed to those affected by the corporation's business practices, even if this reduces shareholder value.").

42 *See* Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897, 1902 (2021) (arguing that Khan and Pozen "significantly overstate the threat that corporate and fiduciary law poses for the information fiduciary model."). Tuch argues that corporate law only imposes duties on *directors*, not corporations, and the information fiduciaries proposal imposes duties on *corporations*, not directors. *See id.* at 1909. Relational duties would not create a set of inconsistent obligations among a *single* fiduciary. *See id.* at 1910. The issue of parallel fiduciary obligations owed by corporations as a whole to clients and directors to shareholders is routine. *See id.* Not only is the "likelihood of fiduciary breach that Khan and Pozen point to in claiming tension between Balkin's proposal and corporate law . . . theoretically remote," it is "in practical terms, nonexistent." *Id.* at 1915. Additionally, if lawmakers obligate a duty of loyalty, then directors are bound to privilege it over shareholder interests. *See id.* at 1916–17 ("Delaware law altogether avoids tension with regimes such as Balkin's. Delaware corporate law requires directors to exercise their discretion within legal limits imposed on the corporation; it does not license or excuse non-compliance with corporate obligations, even if directors believe that doing so would maximize shareholder value. And Delaware law offers no suggestion that a corporation's duties or responsibilities should be diluted or otherwise shaped by the content of directors' duties. Instead, case law indicates that directors must act 'within the law.'" (footnotes omitted)).

obligations on corporations will not create untenable frictions between duties to users and duties to shareholders. . . . [T]he primary criticism—that Delaware corporate law undermines the information fiduciary regime—should be dismissed."[43]

If lawmakers were to adopt data loyalty rules, then corporate law would in fact demand that directors adhere to them first and foremost.[44] In other words, the loyalty that directors owe to shareholders takes a backseat to legal obligations placed upon the corporation, including duties of loyalty to customers.[45] In fact, if a duty of data loyalty owed by platforms to people is made positive law, a director that acts with the intent to act in conflict with users' best interests or fails to act in the face of a known loyalty obligation may be liable for breach to shareholders of their fiduciary obligation as well as their duty to users.[46]

If data loyalty is going to work, then trusting parties must be prioritized over other loyalties owed by organizations, such as loyalty duties owed by firms to shareholders. Prioritizing trusting parties over shareholders would resolve any lingering "divided loyalty" concerns, as well as conflicting loyalties between users and third-party vendors. Self-interested actions would be allowed, but only if they didn't conflict with trusting parties' best interests regarding their data and mediated experiences. And of course, it is an elementary principle of U.S.

---

43 *Id.* at 1902 ("The criticism rests on a partial understanding of corporate law doctrine and theory. The criticism sees conflicting obligations where none exist and identifies strategies for resolving these apparent conflicts that are unknown to corporate law. . . . I also argue that Khan and Pozen's arguments are not merely mistaken but, if accepted, may do harm. Applying their case to financial conglomerates—more apt analogues for social media companies than the '[d]octors, lawyers, accountants, and the like' to whom scholars often draw their comparison—shows that Khan and Pozen's arguments, if accepted, would have pernicious effects on broad spheres of corporate regulation." (quoting Khan & Pozen, *supra* note 3, at 506)).

44 Tuch argues that "[u]nder the information fiduciary model, corporate law would require compliance with user-regarding obligations, creating incentives for directors to favor users' interests over those of shareholders." *Id.*

45 *Id.* at 1917–18 ("Reflecting corporate law's attitude toward legal compliance, former Harvard Law Dean Robert Clark identifies the corporation's purpose as to 'maximize the value of the company's shares, subject to the constraint that the corporation must meet all its legal obligations to others who are related to or affected by it.' . . . Even the most ardent advocates of shareholder primacy have not suggested that corporate law requires, or should require, corporations or directors to maximize shareholder value in violation of a corporation's legal obligations." (quoting ROBERT CHARLES CLARK, CORPORATE LAW 17–18 (1986))).

46 *See id.* at 1918–19 (citing *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 67 (Del. 2006); *see also* Stone v. Ritter, 911 A.2d 362, 369–70 (Del. 2006) ("The failure to act in good faith may result in liability [for directors] because the requirement to act in good faith 'is a subsidiary element[,]' i.e., a condition, 'of the fundamental duty of loyalty.'") (citing Guttman v. Huang, 823 A.2d 492, 506 n.34 (Del. Ch. 2003)).

constitutional law that a federal duty of loyalty would take precedence over any state duties by operation of the Supremacy Clause.

Data loyalty would still allow companies to profit and flourish. The "best interests" polestar of loyalty, by design, accommodates all kinds of self-serving behavior. It simply makes self-serving behavior allowable only in instances where it aligns with the best interests of the primary trusting party.[47]

3. The Collective Best Interests of Trusting Parties

There are a few different ways to deal with inevitable conflicts between trusting parties as well. The first would be to impose a reasonableness and fairness approach, or a duty of impartiality between people who expose themselves to organizations.[48] In trying to accommodate the best interests of billions of individuals, whose "best interests" might differ from person to person, lawmakers could also follow tort law's move to a more objective standard: the reasonable user. Not only would a reasonable user standard help companies better determine the scope of their duties, but it would also inject a normative element into the analysis.

Our proposal adopts a collective approach to "best interests," to better avoid conflicts between trusting parties and help free privacy law from its overly individualistic focus. Allowing lawmakers and regulators to focus on the collective best interests of "trusting parties," they can better respond to systemic harms detected sporadically by individuals but strongly at the group level. We recommend that lawmakers specifically prioritize interests that are held collectively by groups of users, with certain individually held interests holding sway only to the extent they do not conflict with collective user interests.[49]

A more collective best interests approach would be an improvement over the individual self-determination model, which does not compel people to consider the common good or threats to

47 *See* John H. Langbein, *Questioning the Trust Law Duty of Loyalty: Sole Interest or Best Interest?*, 114 YALE L.J. 929, 932 (2005) ("[A] transaction prudently undertaken to advance the best interest of the beneficiaries best serves the purpose of the duty of loyalty, even if the trustee also does or might derive some benefit. A transaction in which there has been conflict or overlap of interest should be sustained if the trustee can prove that the transaction was prudently undertaken in the best interest of the beneficiaries.").

48 Andrew S. Gold, *The Fiduciary Duty of Loyalty*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 36, at 398 ("[C]onflicts among best interests obligations [owed to multiple beneficiaries] are unavoidable. Where such conflicts exist, one answer is to find that loyalty must manifest itself as fairness and reasonableness. Another answer is to impose a duty of impartiality," which would demand "due regard" (though not necessarily equality). (footnotes omitted)).

49 *Id.* (discussing the hierarchy of obligations approach to how "common shares might ordinarily benefit from fiduciary obligations while preferred shares will only benefit in exceptional [circumstances]").

groups they are not a part of. When people give consent to data practices, they usually aren't motivated to reflect upon how their decision will affect vulnerable groups that they are not a part of.[50] This is similar to some people's indifference to public health when they "choose" not to wear a mask during a pandemic.

A reasonable user approach would also be consistent with the parallel duty of care and sensitive to the fact that tech companies deal in bulk and batched relationships. A reasonableness, context-sensitive approach would require loyalty obligations that are proportional to risk of abuse. The duty would be the most robust where the volume of data collected is highest and organization's power over people is the greatest. Because this duty of loyalty would be new and novel for privacy law and would need to be tailored to the unique characteristics of modern information relationships, lawmakers have the ability to craft a unique and fitting approach that borrows from how duties of loyalty operate in other contexts without being bound by it.

4. Limited to Trusting Parties' Exposure

In our previous work on trust, we defined the concept of trust as the willingness to make oneself vulnerable to the actions of others.[51] Our proposed general duty of loyalty would be limited to the extent of that vulnerability. Specifically, the "best interests" should be limited to the interests affected by the entrustment of data, labor, and attention, instead of an overall well-being standard. Organizations would be directed to ask what interests were implicated by the affordances of the data and design of user interfaces. So while it might be disloyal for a company to design a system that leveraged trusting parties' geolocation to allow pharmaceutical companies to target people when they are currently in the hospital (and thus vulnerable), it would probably not be disloyal for that company to generally allow pharmaceutical companies to place advertisements on their app or website. Systems that allow for such microtargeted advertising based on highly detailed profiles rather than isolated contexts make exploitation of vulnerable parties easier and compound incentives for companies to engineer exposure for financial gains.[52]

In conjunction with a duty of care, a duty of loyalty animates a number of different broad subsidiary duties, such as duties of candor,

50 *See, e.g.*, Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 5, at 1498; Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33, 44 (2020).

51 Richards & Hartzog, *Taking Trust Seriously*, *supra* note 5, at 448.

52 *See, e.g.*, JOSEPH JEROME & ARIEL FOX JOHNSON, ADTECH AND KIDS: BEHAVIORAL ADS NEED A TIME OUT (2021).

good faith, nondelegation of key services, and confidentiality.[53] But legislatures and courts often go further and create or delegate authority for the creation of a series of clearer subsidiary obligations that are more like rules than vague standards.[54]

This two-tiered approach allows lawmakers to tailor rules to specific relationships to avoid specific foreseeable conduct while maintaining flexibility for new and changed rules in the future.[55] As applied to privacy law, it would allow lawmakers to target large platforms or social media companies that presented specific problems of gatekeeping for third parties or self-dealing due to two-way markets without applying the same specific rules to traditional e-commerce or media streaming companies bound by a general duty of loyalty. Companies not bound by specific subsidiary rules would still be bound by a general duty of loyalty.

### *B. Second, Rules for Subsidiary Implementing Duties*

Lawmakers can create specific subsidiary rules to help resolve objections that a duty of data loyalty is just too vague.[56] Enacting

---

53 *See* Whitt, *supra* note 3, at 94–95 ("Additional fiduciary obligations recognized by courts of equity over many centuries include the duty of candor, duty of good faith, duty not to delegate the services to others, and the duty of confidentiality. Typically they are subsumed as 'subsidiary' or 'implementing' obligations under either the duty of care or of loyalty. However, in some legal quarters the duty of confidentiality has been deemed an important supportive component of the 'primary' fiduciary duties. . . . [T]he duty of confidentiality deserves special status in the digital environment as an 'enabling' obligation that strengthens the more well-established fiduciary duties of care and of loyalty." (footnotes omitted)).

54 Robert Sitkoff explains that

> [t]he duties of loyalty and care, which we might call the *primary* fiduciary duties, are typically structured as broad, open-ended standards that speak generally. . . . By contrast, the *other* fiduciary duties, which we might call the *subsidiary* or *implementing* fiduciary duties, are typically structured as *rules* or at least as *more specific standards* that speak with greater specificity.

Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 36, at 419.

55 Sitkoff gives the prudent investor rule as an example of a how subsidiary rules develop in trust law. *Id.* at 421 ("Structurally the prudent investor rule is an elaborated standard that, by focusing on risk-and-return and diversification, gives specific content to the open-ended, primary duty of care, called prudence in trust parlance, as applied to the investment function of trusteeship . . . . [W]ithin the fiduciary fields that do include an investment function, the prudent investor rule encompasses the accumulated learning on what the duty of care requires in fiduciary investment. In consequence, rather than start from scratch in every fiduciary investment matter, fiduciaries, beneficiaries, and courts may look to the elaboration within the prudent investor rule to discern the application of the duty of care.").

56 In a hearing on the future of transatlantic data flows called by the U.S. Senate Committee on Commerce, Science, & Transportation, Senator Wicker asked of a panelist who advocated for a duty of loyalty in privacy law, "[w]here is there a working duty of loyalty

legislation should also either provide for subsidiary duties or delegate rulemaking authority for future subsidiary rules. These subsidiary data loyalty rules might take a page from and model information privacy versions of nonprivacy fiduciary duties such as disclosure, consent, accounting for property (access and portability rights), confidentiality, and the full suite of fair information practice principles. This would apply some of the most significant obligations compelled by the GDPR. A duty of loyalty, combined with a duty of care, could spur on specific rulemaking for concepts like data minimization and legitimate basis requirements that would be bound together by an antibetrayal ethos.

But lawmakers need not stop there. One of the most important subsidiary duties to stem opportunistic behavior would be a robust prohibition on abusive trade practices. As we detailed in prior work, companies leveraging people's own cognitive and resource limitations against them to wrongfully extract data and labor is an endemic problem online.

Subsidiary rules prohibiting abusive trade practices would prohibit entrustees from materially interfering with the ability of trusting parties to understand the terms of the relationship and the risk associated with exposure and engagement.[57] Rules against abuse would also prohibit entrustees from taking unreasonable advantage of trusting parties' lack of understanding about the material risks, costs, or conditions of the entrustees' service or the inability of trusting

---

in place in law somewhere that we can look to? When we're able to be specific in those instances, then we're getting somewhere. But beyond that, it's hard actually to define [a duty of loyalty]." *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2020) (statement of Sen. Roger Wicker, Chairman, S. Comm. on Com., Sci., & Transp.). Senator Wicker is the sponsor of one of the most prominent proposals for an omnibus federal privacy law in the United States. The Senator actually expressed tentative support for a duty of loyalty, even though such a duty does not explicitly appear in the bill he sponsored. And in full disclosure, the panelist was one of the authors of this Essay. Also, thank you for reading so deeply in our paper—and in its footnotes. *See also* James Grimmelmann, *When All You Have Is a Fiduciary*, LAW & POL. ECON. PROJECT (May 30, 2019), https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary [https://perma.cc/V5PB-4D6B] (arguing that when applied to digital platforms "the rule against self-dealing is either absurdly under-inclusive, absurdly over-inclusive, or both").

57 We propose that lawmakers adapt language from the Consumer Financial Protection Bureau's authority to regulate abusive trade practices along these lines: "Abusive trade practice" means any conduct by a covered entity that 1) materially interferes with the ability of a trusting party to understand a term or condition of the agreement between covered entities and trusting party relating to the processing of personal data or effect or functionality of a system, tool, or user interface deployed by the covered entity; or 2) takes unreasonable advantage of: a) a lack of understanding on the part of the trusting party of the material risks, costs, or conditions of the covered entity's product or service; or b) the inability of the trusting parties to protect their interests in selecting or using a covered entity's product or service; or c) the reasonable reliance by the trusting party on a covered entity's representation to act in the interests of the trusting party.

parties to protect their interests within the relationship. Finally, anti-abuse rules would prohibit entrustees from taking unreasonable advantage of the reasonable reliance by trusting parties on entrustees' representations to act in the trusting parties' interests.

Lawmakers might also consider rigid prohibitions on specific practices like the deployment of unreasonably dangerous automated tools or the use of personal data to train those automated systems. They could create subsidiary rules for inherently dangerous practices and technologies that, at the systemic level, are in fundamental conflict with the best interests of trusting parties, such as microtargeting, a practice that paves the path for third party abuse and imposes more externalities than benefits for trusting parties; and affect recognition, a fundamentally misguided, mistaken, and oppressive tool.[58] Lawmakers could craft even more rules designed for specific parties such as "social media platforms may not deploy affect recognition technologies on photos or videos submitted by trusting parties." There might also be disclosure mandates, process requirements, prohibitions on conduct, or obligated tasks. Each rule should target specific areas where trusted parties have an incentive to engage in self-dealing.[59]

Lawmakers could, of course, impose all these rules even without couching them within an umbrella duty of loyalty. We have proposed in previous research that trust-building and trust-enforcing rules irrespective of a relationship between the parties could be meaningful complements or the next best thing to broad and strong relational obligations.[60] Many of these rules, such as data protection obligations, should have sibling rules that apply regardless of whether data controllers are in an information relationship with a trusting party. But we believe that a duty of loyalty would act as an important animating force, interpretive guide, and catchall provision that would bring more coherence, flexibility, and accountability through enforcement than these rules would have as stand-alone laws.

Nonetheless, we propose specific subsidiary rules within information relationships to maximize the advantages of a relational approach to privacy. Scholars and lawmakers have identified different contexts where the incentives for self-dealing by the powerful party in

---

58 For an exploration on the dangers of affect recognition systems see, e.g., KATE CRAWFORD, ATLAS OF AI (2021); Kate Crawford, *Artificial Intelligence Is Misreading Human Emotion*, THE ATLANTIC (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/ [https://perma.cc/T6AV-J25T]; LUKE STARK & JESSE HOEY, THE ETHICS OF EMOTION IN ARTIFICIAL INTELLIGENCE SYSTEMS (2021).

59 *See* Andrew S. Gold, *The Fiduciary Duty of Loyalty*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 36, at 401 ("Different opportunism risks will then justify different loyalty content and approaches to legal decision-making.").

60 *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 5.

an information relationship are overwhelming, making these contexts ripe for subsidiary data loyalty rules.[61] We synthesize these contexts into five main areas: Entrustees should be loyal when *collecting* information, being sure to collect only information for purposes that do not conflict with a trusting party's best interests. Entrusees should be loyal when *personalizing*, i.e., treating people differently based upon personal information or characteristics. Entrustees should be loyal *gatekeepers*, avoiding conflicts when allowing government and other third-party access to trusting parties and their data. Entrustees should be loyal when trying to *influence* trusting parties, such as when they leverage personal data and digital tools to exert sway over people to achieve particular results. Finally, entrustees should be loyal in the ways they *mediate* interactions between users of their platform, specifically in the creation and administration of systems that govern how people are allowed to interact with each other. These contexts often overlap and involve issues like discriminatory microtargeting, harmful amplification of misinformation, failure of process for content moderation, and abusive dark patterns. We propose that lawmakers create subsidiary loyalty rules and standards to mitigate these kinds of disloyal behaviors.

### 1. Loyal Collection

A duty of loyalty should attach the moment a trusted party invites disclosure and makes the decision to collect personal information. In this way, data loyalty could embolden the fair information principle of data minimization. This principle holds that data collectors should only identify the minimum amount of personal information needed to fulfill a legitimate purpose and collection and hold that much information and no more.[62] Combined with the storage limitation principle, which holds that organizations should not keep data longer than they need it for their stated purpose, data minimization is a central pillar in data protection regimes around the world, but it too often fails to find traction.[63]

---

61 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3; Scholz, *supra* note 3, at 197; Dobkin, *supra* note 3, at 17 (identifying four major ways of breaching an information fiduciary duty: "manipulation, discrimination, third-party sharing, and violating a company's own privacy policy"); Barrett, *supra* note 3, at 1100 ("[A]n information fiduciary framework should also address manipulation and discrimination in order to ensure that people are protected from the full array of modern digital threats that they face.").

62 *See Principle (c): Data Minimisation*, INFO. COMM'RS OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/#data_minimisation [https://perma.cc/6TTU-BJ8H].

63 *See id.*; Council Regulation 2016/679, art. 5(e) 2016 O.J. (L 119) 1 (EU) (providing the GDPR's storage limitation principle).

Data loyalty could provide a normative vision for when companies have exceeded their duty to minimize collection and retention—when it conflicts with a trusting party's (or collective trusting parties') best interests. Under general data protection frameworks that impose data minimization requirements, organizations must typically ensure that the data they are processing is adequate (sufficient to fulfil the stated purpose), relevant (has a relevant link to that purpose), and limited to what is necessary (collecting and holding only that which is needed for that purpose).[64] A duty of loyalty could provide a value-laden baseline that requires an examination of not just the purpose of the collection but also elevates the interests of those affected by the collection. While parties at an arm's length might act opportunistically in collecting as much data as possible, trusted parties remain loyal by leaving all data that, if collected, would conflict with the trusting parties' best interests on the table.

2. Loyal Personalization

The modern Internet routinely and systemically treats people differently based upon personal information or characteristics. Targeted and behavioral advertising is the most prominent example of this, but first-party product and streaming recommendations, news feeds, default settings, layouts, and more are all designed automatically to look and act differently based on people's personal characteristics. Some of this personalization, such as targeted recommendations for networked connections based upon intentionally revealed data such as where you work or attended high school, would probably be loyal. Other personalization systems, however, such as those that wrongfully discriminate or have a disparate impact on protected, marginalized, or vulnerable groups of people, would likely conflict with that trusting collective's best interests. Subsidiary rules built around the concept of loyal personalization could firmly and clearly address a systemic problem in a way that traditional data protection frameworks have been unable to mitigate.

3. Loyal Gatekeeping

Entrustees have a remarkable ability to facilitate third party access to trusting parties and their data. They can do so through their APIs, advertiser portals, fusion centers, and government backdoors. This access is the source of most major platforms' power. And everyone wants a piece of the users. Advertisers clamor for their attention. Data brokers and companies training AI models lust for their data. And

64 Council Regulation 2016/679, art. 5(c) 2016 O.J. (L 119) 1 (EU) (providing the GDPR's data minimization principle).

governments demand evidence. Entrustees have financial incentives to build portals and facilitate access for third parties. Some access granted by trustees to third parties is not in conflict with trusting parties' best interests. For example, contextual advertising usually doesn't significantly leverage people's own data or limitations against them, nor does it usually expose trusting parties to significant privacy harms. Protocols for interoperability to help people transfer data from one place to another also serve the interests (and wishes) of trusting parties.

However, certain lax gatekeeping practices would be disloyal because of how they endanger trusting parties by obscuring risk and breaking promises while facilitating access to third parties for organizational gains or to avoid costs. The three most resonant privacy scandals in the past decade, the government surveillance revelations by Edward Snowden, the FBI's request that Apple help it bypass encryption protections, and Cambridge Analytica's massive Facebook data exfiltration, all involved gatekeeping issues. Subsidiary rules built around the concept of loyal gatekeeping would help resolve longstanding debates around what obligations trusted organizations have regarding third-party access through portals, APIs, interfaces, and the automated scraping of websites. And in combination with a duty of confidentiality, subsidiary rules could also help clarify when sharing a trusting party's data with third parties is disloyal.

### 4. Loyal Influencing

Technologies are artifacts built to act upon the world. Every single design decision made in the creation of a website or app is meant to facilitate a particular kind of behavior.[65] The structure of digital technologies will affect people's choices even if the effect is not intended by designers. When designers create a drop-down menu, privacy settings, "I agree" buttons, and any other feature that implicates people's privacy, they are influencing them. They can't avoid it.[66] Given their power, they should be loyal in exercising their influence.

The most prominent example of disloyal influence involves organizations leveraging "dark patterns" or "malicious interfaces"

65 *See, e.g.*, LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY 94 (1986).

66 *See* Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REGUL. 413, 421 (2015) ("Human beings . . . cannot wish [choice architecture] away. Any store has a design; some products are seen first, and others are not. Any menu places options at various locations. Television stations come with different numbers, and strikingly, numbers matter, even when the costs of switching are vanishingly low; people tend to choose the station at the lower number, so that channel 3 will obtain more viewers than channel 53.").

which are user interface elements meant to influence a person's behavior against their intentions or best interests.[67] Companies deploy effort traps to make deleting an account confusing and difficult. They make "cancel" buttons hard to see and press, they obscure important details in tiny fonts or walls of boilerplate, and they leverage our deeply entrenched and empirically validated overconfidence regarding risk, deference for conformity, endowment effects, status quo bias, and other biases and mental shortcuts to manipulate us to their ends. Jamie Luguri and Lior Strahilevitz have observed that "dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces."[68]

---

67 *See, e.g.*, HARTZOG, *supra* note 22, at 148, 162; Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Gregory Conti & Edward Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, IEEE PRIV. & SEC., May/June 2009, at 72, 73; JOHANNA GUNAWAN, DAVID CHOFFNES, WOODROW HARTZOG & CHRISTO WILSON, TOWARDS AN UNDERSTANDING OF DARK PATTERN PRIVACY HARMS (2021); Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/ [https://perma.cc/4VBK-HEEG]; COLIN M. GRAY, YUBO KOU, BRYAN BATTLES, JOSEPH HOGGATT & AUSTIN L. TOOMBS, THE DARK (PATTERNS) SIDE OF UX DESIGN (2018); Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROCEEDINGS ACM HUM.-COMPUT. INTERACTION 81 (2019); ARUNESH MATHUR, JONATHAN MAYER & MIHIR KSHIRSAGAR, WHAT MAKES A DARK PATTERN. . . DARK? (2021); Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 4 PROC. ON PRIV. ENHANCING TECHS. 237, 248 (2016); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105, 107–09 (2020).

68 Luguri & Strahilevitz, *supra* note 67, at 46 (emphasis omitted). Luguri and Strahilevitz found that

> [r]elatively mild dark patterns more than doubled the percentage of consumers who signed up for a dubious identity theft protection service, which we told our subjects we were selling, and aggressive dark patterns nearly quadrupled the percentage of consumers signing up. In social science terms, the magnitudes of these treatment effects are enormous.

*Id.* They further found that

> the most effective dark pattern strategies were hidden information (smaller print in a less visually prominent location), obstruction (making users jump through unnecessary hoops to reject a service), trick questions (intentionally confusing prompts), and social proof (efforts to generate a bandwagon effect). Other effective strategies included loaded questions and making acceptance the default. . . . In many cases, consumers exposed to dark patterns did not understand that they had signed up for a costly service. These results confirm the problematic nature of dark patterns and can help regulators and other watchdogs establish enforcement priorities.

*Id.* at 47.

Lawmakers have struggled for years to articulate when attempts at persuasion become harmful.[69] But trusting parties do not need to be injured for entrustees to violate a duty of loyalty. Subsidiary rules around disloyal attempts to influence would address the most pernicious and dangerous dark patterns head-on.[70] Lawmakers should focus on how the design is meant to take advantage of a person's limitations or vulnerabilities to benefit the designer in a way that is against the best interests of the trusting party.[71]

5. Loyal Mediation

Certain kinds of organizations design their platforms so that their users interact not just with the organization itself, but with each other. In other words, they mediate people's social and market experiences with other people using their service. Sometimes this is a great experience for people who use these services. But things can go off the rails quickly as companies feel pressured to achieve continual and endless growth. They create systems that reward virality and the most outrageous or venomous hot takes instead of the ostensible purpose of meaningful social interaction and social, emotional, and intellectual nourishment. They optimize their algorithms and interfaces to reward our most impulsive and petty reactions. Amplification of certain kinds of information combined with strategically reduced or increased transaction costs to speak, report harmful and dangerous speech, and hide from other users leads to acute individual harms like harassment[72]

---

69 *See id.* at 104; *see also* Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in A Digital World*, 4 GEO. L. TECH. REV. 1, 3 (2019) ("[A]t its core, manipulation is hidden influence—the covert subversion of another person's decision-making power. In contrast with persuasion, which is the forthright appeal to another person's decision-making power, or coercion, which is the restriction of acceptable options from which another person might choose, manipulation functions by exploiting the manipulee's cognitive (or affective) weaknesses and vulnerabilities in order to steer his or her decision-making process towards the manipulator's ends.").

70 Luguri and Strahilevitz recommend a multi-factor test to help determine when dark patterns cross the line

> that looks to considerations such as (i) evidence of a defendant's malicious intent or knowledge of detrimental aspects of the user interface's design, (ii) whether vulnerable populations—like less educated consumers, the elderly, or people suffering from chronic medical conditions—are particularly susceptible to the dark pattern, and (iii) the magnitude of the costs and benefits produced by the dark pattern.

Luguri & Strahilevitz, *supra* note 67, at 99.

71 Balkin has proposed looking to "techniques of persuasion and influence that (1) prey on another person's emotional vulnerabilities and lack of knowledge (2) to benefit oneself or one's allies and (3) reduce the welfare of the other person." JACK M. BALKIN, HOOVER INST., FIXING SOCIAL MEDIA'S GRAND BARGAIN 4 (2018).

72 *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

as well as systemic harms like polarization, reduced ability to engage in self-governance, negative public health outcomes, and chilling effects for large groups of vulnerable users.

A duty of loyalty cannot solve all of the complex problems of content moderation or harassment. As we have maintained, a duty of loyalty is merely one important tool in a larger toolkit. But companies do have remarkable power to influence how people using their systems interact with each other.[73] When they use this power in a way that conflicts with the best interests of their users in order to optimize growth, they are being disloyal. Subsidiary rules for loyal mediation are, of course, complicated because of the potentially conflicting interests amongst actors and those potentially adversely affected by the act. One trusting party wants to speak while the other(s) is made worse because of it. This is where our proposed systemic focus and the traditional fiduciary law method of developing a hierarchy of loyalties would help clarify lawmakers' actions.

## CONCLUSION

Duties of data loyalty will take time and effort to meaningfully implement as a part of U.S. privacy law. Data loyalty is a significant and necessary departure from privacy law's ineffective notice and consent approach. But lawmakers can confidently embrace loyalty and other relational duties as part of a holistic approach to mitigating the power and abuses of data collectors. If done clearly, carefully, and with commitment, lawmakers can chart a bold new vision for our privacy rules that is capable of nurturing a sustainable and flourishing future for those who share their personal information as well as those entrusted with it.

73 *Id.* at 25; *see also* Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1695.