

2022

The Surprising Virtues of Data Loyalty


Neil M. Richards

Washington University in St. Louis School of Law, nrichards@wustl.edu

Woodrow Hartzog

Boston University School of Law

Follow this and additional works at: https://openscholarship.wustl.edu/law_scholarship

 Part of the [Comparative and Foreign Law Commons](#), [Consumer Protection Law Commons](#), [Internet Law Commons](#), [Legal Studies Commons](#), [Privacy Law Commons](#), and the [Torts Commons](#)

Repository Citation

Richards, Neil M. and Hartzog, Woodrow, "The Surprising Virtues of Data Loyalty" (2022).
Scholarship@WashULaw. 545.
https://openscholarship.wustl.edu/law_scholarship/545

This Essay is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Scholarship@WashULaw by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.

THE SURPRISING VIRTUES OF DATA LOYALTY

Woodrow Hartzog*

Neil Richards**

ABSTRACT

Lawmakers in the United States and Europe are seriously considering imposing duties of data loyalty that implement ideas from privacy law scholarship, but critics claim such duties are unnecessary, unworkable, overly individualistic, and indeterminately vague. This paper takes those criticisms seriously, and its analysis of them reveals that duties of data loyalty have surprising virtues. Loyalty, it turns out, can support collective well-being by embracing privacy's relational turn; it can be a powerful state of mind for reenergizing privacy reform; it prioritizes human values rather than potentially empty formalism; and it offers solutions that are flexible and clear rather than vague and indeterminate. We propose five contexts in which specific rules should supplement a general duty of data loyalty: collection, personalization, gatekeeping, influencing, and mediation. Loyalty can be a key policy tool with which to take on the related problems of information capitalism, platform power, and the use of personal data to manufacture consent to objectionable data practices. In fact, loyalty may well be the critical missing piece of the regulatory toolkit for privacy.

* Professor of Law and Computer Science, Northeastern University.

** Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University. The authors would like to thank Lisa Austin, Jack Balkin, Ryan Calo, Bernard Chao, Ignacio Cofone, Richard Daynard, Josh Fairfield, Michael Froomkin, Nikolas Guggenberger, Sarah Holland, Pauline Kim, Kirsten Martin, Jeremy Paul, Bob Pollack, Kyle Rozema, Laruen Scholz, Andrew Selbst, David Simon, Andrew Tuch, Rory Van Loo, Paul Weidenbeck and the participants of paper workshops at Northeastern University School of Law, Washington University School of Law, the Information Society Project at Yale Law School, and the Privacy Law Scholars Conference. The authors would also like to thank Enyonam Edoh, Giuliana Green, Johanna Gunawan, Alissamariah Gutierrez, Alexis Johnson, and Nina Sprenger for their research assistance and the staff of the *Emory Law Journal* for their dedication and skill in the editing and publication process.

INTRODUCTION	986
I. LOYALTY FOCUSES ON RELATIONSHIPS	992
A. <i>Arms-Length Relationships vs. Relationships of Trust</i>	994
B. <i>Key Traits of Modern Information Relationships</i>	996
1. <i>Ongoing</i>	996
2. <i>Frequent</i>	997
3. <i>Constructed</i>	998
4. <i>Interactive</i>	999
5. <i>Responsive</i>	999
II. LOYALTY ACHIEVES WHAT CARE CANNOT	1000
A. <i>Loyalty Makes People’s Choices Less Dangerous</i>	1001
B. <i>Loyalty Complements Other Interventions</i>	1002
C. <i>Loyalty Avoids the Harm Trap</i>	1002
D. <i>Loyalty Animates Legislation and Enforcement Efforts</i>	1005
III. LOYALTY PRIORITIZES HUMAN VALUES	1008
A. <i>Data Loyalty’s Illusory Conflicts</i>	1009
B. <i>The Diverse Value-Forcing Function of Data Loyalty</i>	1012
IV. LOYALTY CAN BE BOTH FLEXIBLE AND CLEAR	1013
A. <i>“Best Interests” Standard Clarified by Specific Rules</i>	1015
B. <i>Five Areas for Subsidiary Data Loyalty Rules</i>	1024
1. <i>Loyal Collection</i>	1025
2. <i>Loyal Personalization</i>	1026
3. <i>Loyal Gatekeeping</i>	1027
4. <i>Loyal Influencing</i>	1029
5. <i>Loyal Mediation</i>	1032
CONCLUSION	1033

INTRODUCTION

Lawmakers in the United States and Europe are now seriously considering imposing a duty of loyalty on companies that process human information.¹ Such

¹ See, e.g., Data Care Act of 2019, S. 2961, 116th Cong. § 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 Leg., Reg. Sess., § 1102 (N.Y. 2019) (“Every legal entity . . . 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

duties of loyalty represent both an alternative to the failed “notice and choice” regime in the United States and a supplement to the more robust General Data Protection Regulation (GDPR) model in the EU.² Scholars have proposed duties of loyalty—in a variety of forms, including loyalty duties for data collectors, “information fiduciaries,” design rules, and fiduciary boilerplates—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 and experiences.³ Loyalty, thus, holds the potential to be a powerful response to what Julie Cohen calls “informational capitalism” and Shoshana Zuboff calls “surveillance capitalism”: the claiming of “human experience as free raw material for hidden commercial practices of extraction, prediction, and sales.”⁴

Yet, all is not well with the duty of loyalty, as it faces myriad critiques from regulators, companies, and even otherwise sympathetic academics. These critics assert that loyalty does little to deal with the *structural pathologies* of platform capitalism, and that backward-looking fiduciary models would *fall apart* at the massive scale at which platforms operate.⁵ They argue that a duty of loyalty is *unnecessary* because it would do little that existing consumer protection rules, data protection models, and duties of care do not already accomplish, and

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, at 18, COM (2020) 767 final (Nov. 25, 2020); Data Protection Act 2018, c. 12, § 123(1) (Eng.); An Act to Provide Facial Recognition Accountability and Comprehensive Enforcement, H. 117, 2021 Leg., 192d Gen. Ct. Mass., § 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.”).

² See *infra* note 12; *infra* Part II.D.

³ See, e.g., Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11 (2020) [hereinafter Balkin, *The Fiduciary Model of Privacy*]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186–87 (2016) [hereinafter Balkin, *Information Fiduciaries*]; Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 964–65 (2021); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 144–45 (2020); see also ARI EZRA WALDMAN, *PRIVACY AS TRUST: INFORMATIONAL PRIVACY FOR AN INFORMATION AGE* 79–92 (2018) (exploring the relationship between privacy and trust); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 35 (2020) (exploring the different possible fiduciary analogies in the information context).

⁴ JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* 6 (2019); SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019) (providing a definition for “surveillance capitalism” on a page titled “The Definition,” prior to the introduction).

⁵ E.g., Julie E. Cohen, *Scaling Trust and Other Fictions*, LPE PROJECT (May 29, 2019), <https://lpeproject.org/blog/scaling-trust-and-other-fictions/> [hereinafter Cohen, *Scaling Trust and Other Fictions*]; JULIE E. COHEN, *KNIGHT FIRST AMEND. INST., HOW (NOT) TO WRITE A PRIVACY LAW* 2, 8 (2021), <https://s3.amazonaws.com/kfai-documents/documents/306f33954a/3.23.2021-Cohen.pdf> [hereinafter COHEN, *HOW (NOT) TO WRITE A PRIVACY LAW*].

imposing a duty of loyalty might foreclose other approaches to platform regulation.⁶ They charge that it is *unworkable* because corporations cannot simultaneously owe duties both to their shareholders and to their customers.⁷ They claim that it is *redundant* because privacy laws modeled on Europe's GDPR already require a lawful basis for processing.⁸ These laws demand consideration of data subjects' rights and place substantive duties on data processors.⁹ Finally, and most frequently, critics of a duty of loyalty assert that it is *vague*—too burdensome, too likely to get watered down to empty formalities through the process of compliance, and inevitably too unclear about what it would actually require.¹⁰

Such critiques must be taken seriously. At first blush, their number and variety might leave data loyalty advocates feeling a little bit like Goldilocks holding her proverbial bowl of porridge: What's in the bowl is likely too hot or too cold, and in any event, is undoubtedly a bowl of mush. Well-intentioned but potentially devastating criticisms of this sort require thoughtful consideration and a comprehensive response. This essay represents that reflection and response. In our own work, we have articulated a duty of loyalty for privacy law as the duty of data collectors to act in the best interests of those whose data they collect.¹¹ While we borrow from fiduciary law and work on “information fiduciaries,” we have advocated for new relational frameworks tailored to the unique power imbalances between people and platforms.¹² We agree with the critics that a duty of loyalty for privacy law is neither perfect nor a tool for all tasks. However, when the criticisms of loyalty are taken seriously—when they are considered, evaluated, and responded to on the merits—loyalty reveals some surprising virtues as a relational approach that collectively prioritizes trusting parties' best interests.

Loyalty, it turns out, places the focus for information-age problems where it belongs: not primarily on the data, but on the human relationships that data can

⁶ Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 534–36 (2019).

⁷ *Id.* at 504.

⁸ COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, *supra* note 5, at 5–6.

⁹ *Id.* at 12.

¹⁰ *See, e.g.*, James Grimmelman, *When All You Have Is a Fiduciary*, LPE PROJECT (May 30, 2019), <https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary/>; COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, *supra* note 5, at 10–11.

¹¹ *See, e.g.*, Richards & Hartzog, *supra* note 3 (manuscript at 6–7); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1741 (2020) [hereinafter Hartzog & Richards, *Privacy's Constitutional Moment*].

¹² *See generally* Richards & Hartzog, *supra* note 3 (manuscript at 4, 6–7) (advocating for a trust-focused approach to privacy rules).

affect; not just on procedural requirements for data processing but also on substantive rules restricting dangerous applications; and not merely on the interests of individuals but also on the interests of groups with the same relational vulnerabilities. Loyalty can thus be a powerful state of mind with real analytical and political consequences. Even loyalty's supposed fatal flaw—its indeterminate vagueness¹³—is actually a great strength of flexibility and adaptability across contexts, cultures, and time. Simply put, loyalty as a relational approach allows us to deal substantively with the problem of platforms and human information at both a systemic and an individual level.

Our argument in this paper is ultimately a simple one: the concept of data loyalty has surprising virtues, including checking power and limiting systemic abuse. The critics of loyalty have provided the valuable service that generous and constructive criticisms of an idea often perform. They allow loyalty to be presented in a clearer, more refined, more detailed, and more realistic manner—one that is better suited to addressing some (but not all) of the many problems of information policy that cry out for solutions. Loyalty can thus be a key policy tool with which to take on the related problems of information capitalism, platform power, and the use of personal data to manufacture consent to objectionable data practices. In fact, it may well be *the* critical piece of the regulatory toolkit for privacy.

We develop our argument across four parts, each of which responds to one of the principal critiques of loyalty and each of which, in assessing those critiques carefully, identifies one of loyalty's surprising virtues. In Part I, we consider the critique that relational protections, like a duty of loyalty, would not solve the *right* problems for privacy law—specifically, that they would not be a meaningful check on the excesses of informational capitalism and would not address the root causes of corporate abuses of power facilitated by use of our data. We conclude that the relationships between people and platforms are a key element of these problems. One of the main virtues of a duty of loyalty is that it remedies the misguided approach by lawmakers and judges that treats all interactions between people and companies that offer online services as arms-length relationships. The power imbalances in these relationships, made worse by the remarkable power that digital technologies confer, are simply too great to ignore. A duty of loyalty could usher in privacy's relational turn.

¹³ See, e.g., Grimmelman, *supra* note 10 (explaining why the duty of loyalty's ambiguity can be problematic); cf. COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, *supra* note 5, at 10–11 (discussing the difficulties of applying traditional fiduciary values to a digital context).

In Part II, we consider the claim that a duty of loyalty would be *unnecessary*, whether because it would be coextensive with a duty of care or consumer protection law or because a European-style approach to data protection, modeled on the GDPR, would be equally protective. We consider these objections and make the case that data loyalty has several special virtues, including having its own distinct purpose and also being able to fulfill a necessary supportive function for data protection frameworks. Not only does a duty of loyalty offer substantive protections that a GDPR-style approach does not but that loyalty can also offer political and moral salience to rules that restrain the uses of human information that European data protection terms like “data minimization” and “legitimate interest” simply cannot. In this way, loyalty can be seen not just as a state of mind, but as one with potentially powerful rhetorical and political meaning that paves the way to a fruitful approach to technology regulation. A duty of loyalty could thus be the key ingredient in the regulatory recipe for data privacy.

In Part III, we address the critique that a duty of loyalty is *unworkable*, either because it conflicts with a corporation’s fiduciary obligation to prioritize shareholder interests over those of human customers or because of the potential clash of individual interests between multiple parties all trusting the same entity. We conclude that these potential conflicts are not only resolvable by lawmakers but also that a turn to relational protections—instead of deferring to informational self-determination¹⁴—would facilitate a substantive embrace of a broad array of human values over privacy law’s reflexive deference to individual choice, consent, and control. Data loyalty would also allow lawmakers to create a uniform definition of “best interests” and thereby prioritize a collective, systemic understanding of this concept over individual, idiosyncratic ones. In this way, a duty of loyalty could be highly functional and consistent with other legal rules across a host of areas.

Finally, in Part IV, we address the most frequent critique of a duty of loyalty for privacy law—that it is too *vague*. There are three different versions of what we might call the vagueness critique. The first is that if the duty of loyalty is interpreted too broadly, then it could prove unduly burdensome and costly to businesses. The second is that the indeterminacy of a duty of loyalty creates

¹⁴ By “informational self-determination,” we refer to the basic idea underlying data protection regimes (particularly in Europe) rooted in the Fair Information Practices—that human autonomy and dignity are advanced by giving people control over how their information is processed through the exercise of individual data rights like choice, access, correction, deletion, etc. For an early discussion of this concept in the U.S. context, see Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMPAR. L. 675 (1989).

room for companies to interpret their obligations in their weakest possible form, watering them down to mere compliance exercises that provide little protection for people and little hope for changing the incentives of abuse. The final version of this argument is simply that if a duty of loyalty is not clarified, companies might be left with no clue about what kinds of conduct are prohibited and what data practices and design choices are permissible.

We believe that all three versions of the vagueness critique can be meaningfully addressed with a properly articulated duty of loyalty. In fact, the novelty of data loyalty and the method by which relational duties become contoured to a relationship's unique vulnerabilities opens the door for clear rules targeting systemic abuses while preserving flexibility for the future. The fact that a duty of loyalty can be applied broadly across contexts is actually a virtue, as it is within other flexible, standards-based frameworks like negligence, reasonableness, unfairness, and legitimate interests.

Our response begins with a survey of our law's rich and long-standing experience with loyalty duties in other areas—such as guardians, trusts, professionals, and corporate shareholders—to show how lawmakers and judges have refined the duty to make it clearer and easier to implement in certain contexts while retaining its breadth and flexibility. Lawmakers use a two-step process to implement loyalty obligations in a fair and just way. First, they articulate a primary, general duty of loyalty for a group of actors. Next, courts and lawmakers go about the task of creating and refining what has 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, detailed standards, and highly specific rules.¹⁵

Using the two-step model from fiduciary law, we suggest certain subsidiary data loyalty rules targeting the five most likely areas ripe for disloyal and harmful self-dealing. These vulnerable areas include the following: First, there is *Collection*, the act of collecting, recording, and deciding to keep data about a person. Second, there is *Personalization*, the act of treating people differently based upon personal information or characteristics. Third, there is *Gatekeeping*, the extent to which trusted entities allow third parties to access people and their data. The fourth context is *Influence*, where companies leverage technologies to exert sway over people to achieve results. Finally, there is *Mediation*, which

¹⁵ For a more detailed examination of this two-step process, and an explanation of how it could apply in the data loyalty context, see generally Richards & Hartzog, *supra* note 3.

concerns the way that organizations design their platforms to facilitate people interacting with each other. Within these five contexts, we explore problems such as discriminatory and harmful microtargeting, design that facilitates online harassment, corrosive amplification of particular behavior, and abusive dark patterns. We propose possible subsidiary loyalty rules and standards to mitigate these kinds of disloyal behaviors. In this way, though it would not solve all problems of data and platform power, a duty of loyalty could be both broad enough to engage with many of those problems and specific enough to solve each of them effectively.

We conclude that clarifying the duty of loyalty is, in fact, the single most important factor enabling its potential as a key cog in a meaningful data privacy framework. Critics of a duty of loyalty have rightfully identified that the power of modern platforms is unprecedented and will require multiple new approaches to disrupt it. Lawmakers and scholars have been moving privacy law towards a particular relational focal point for a while now.¹⁶ It is time we give it a name: loyalty.

I. LOYALTY FOCUSES ON RELATIONSHIPS

From the beginning, U.S. privacy law has glossed over the ways that power imbalances in relationships jeopardize our privacy. Lawmakers and judges have largely ignored how relationships can be a key point of intervention. Samuel Warren and Louis Brandeis's foundational article *The Right to Privacy* rejected relational protections such as breach of confidence and contracts because the target of their proposed tort was complete strangers (particularly the new tabloid *Yellow Press*).¹⁷ Courts recognizing the tort under the common law similarly rejected relational approaches that followed Warren and Brandeis's lead and started focusing on privacy duties owed "to the world" via tort law, similar to negligence.¹⁸ Today, with a few exceptions such as HIPAA and a handful of

¹⁶ See, e.g., sources cited *supra* note 1; 12 U.S.C. § 5531(a) (2018); Complaint for Permanent Injunction and Other Equitable Relief at 20, Fed. Trade Comm'n v. Age of Learning, Inc., No. 2:20-CV-07996 (C.D. Cal. Sept. 1, 2020); Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (Apr. 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

¹⁷ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211 (1890) ("Thus, the courts, in searching for some principle upon which the publication of private letters could be enjoined, naturally came upon the ideas of a breach of confidence, and of an implied contract; but it required little consideration to discern that this doctrine could not afford all the protection required, since it would not support the court in granting a remedy against a stranger . . .").

¹⁸ See, e.g., Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 152 (2007) ("[T]he four torts [William] Prosser identified became widely

other confidentiality-based regimes, privacy and data protection law is generally agnostic to the power imbalances within relationships or even whether a relationship exists between people at all.¹⁹ The current U.S. approach to privacy flattens the power dynamics within relationships with a giant *caveat emptor* sign. Lawmakers permitted the failed “notice and choice” approach to privacy to flourish in the wake of the decay of contract law protecting consumers against boilerplate.²⁰ On this shaky foundation, the thin veneer of fair information practices that lacquered over this fault causes the law to ignore how companies betray the people who trust them with their data and online experiences every day.²¹

Even if it might have been rational for lawmakers and judges to ignore information relationships in the past, our modern ongoing involvement with the companies providing the apps and websites we use every day demands more scrutiny. Is the person-platform relationship akin to the ones we have with ordinary merchants like automobile or furniture dealers? Or is it more akin to our intimate relationships with people that we trust with deeply personal experiences and information, as well as our personal safety?²² The answer to this question will affect what our rules for these relationships should be.

Julie Cohen worries that relational privacy duties of loyalty, care, and confidentiality that have been proposed by some scholars fail to contend with the “speed, immanence, automation, and scale” of the affordances of the platform-consumer relationship.²³ We agree that the affordances of modern platforms and the business models motivated by them should be central to lawmakers’ and judges’ approach to modern privacy problems. Yet, we would suggest that one of the key virtues of data loyalty is that it accurately reflects

known as tort law’s way of protecting privacy. Breach of confidentiality was left out of the picture.”).

¹⁹ See, e.g., Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 659 (2012); Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 764 (2014); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection Law?*, 6 EUR. DATA PROT. L. REV. 492, 493, 495 (2020).

²⁰ Hartzog & Richards, *Privacy’s Constitutional Moment*, supra note 11, at 1690–91 n.6; Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 979 (2017).

²¹ MARGARET JANE RADIN, *BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW* 17 (2013); NANCY S. KIM, *WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS* 5 (2013); Scholz, supra note 3, at 149–50; Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN STATE L. REV. 587, 623 (2007); Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1643, 1645 (2011) [hereinafter Hartzog, *Website Design as Contract*]; Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM’N L. & POL’Y 405, 415–16 (2010) [hereinafter Hartzog, *The New Price to Play*]; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019).

²² See generally Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1874 (2019) (discussing the importance of sexual privacy to “sexual agency, intimacy, and equality”).

²³ Cohen, *Scaling Trust and Other Fictions*, supra note 5.

how the remarkable affordances of digital technologies result in wildly imbalanced relationships. These relationships go far beyond the standard merchant-customer dealings. They are a part of people's everyday lives and have an outsized impact on their well-being. When lawmakers treat all interaction between people and companies that offer online services as arms-length relationships, they ignore how the power of structure and scale create relational vulnerabilities.

A. Arms-Length Relationships vs. Relationships of Trust

Arms-length relationships are typically those where parties with relatively equal bargaining power act in service of their own self-interests in dealing with each other.²⁴ While the default presumption in market transactions is that parties are operating at arms-length, when one party has significant power over the other and an incentive to abuse that power, lawmakers often create duties and restraints within these imbalanced relationships to protect vulnerable parties.²⁵ These power imbalances can manifest in several ways, including large disparities in information or knowledge, reliance on expertise or promises, and discretion and control over the thing entrusted to one party in the relationship.²⁶

A duty of loyalty won't solve our modern data dilemma by itself, but our next generation of privacy rules will never be complete until they recognize that

²⁴ See, e.g., *Gen. Assurance of Am., Inc. v. Overby-Seawell Co.*, 893 F. Supp. 2d 761, 780–81 (E.D. Va. 2012), *aff'd*, 533 F. App'x 200 (4th Cir. 2013) (“[A] fiduciary relationship is not created ‘between mutually interdependent businesses with equal bargaining positions who dealt at arms-length.’ . . . Indeed, ‘[o]nly when one party figuratively holds all the cards—all the financial power or technical information, for example—have North Carolina courts found that the special circumstance of a fiduciary relationship has arisen.” (quoting first *Cardiovascular Diagnostics Inc. v. Boehringer Mannheim Corp.*, 985 F. Supp. 615, 619–20 (E.D.N.C. 1997); then *S.N.R. Mgmt. Corp. v. Danube Partners 141, LLC*, 659 S.E.2d 442 (N.C. Ct. App. 2008)); WEST'S TAX L. DICTIONARY *Arms Length* § A2960 (2021) (“Status of a transaction by unrelated parties, each acting in its own self interest. The term means a transaction made in good faith by parties with independent interests.”); 4C LARY LAWRENCE, ANDERSON ON THE UNIFORM COMMERCIAL CODE § 2A-108:31 (3d ed. 2021) (“The comparative bargaining power of the lessor and lessee is significant in determining whether the contract made by them is unconscionable. . . . When a contract is negotiated at arm's length in good faith between parties of equal bargaining power and contains no unusual provisions, the contract will not be regarded as unconscionable merely because one of the parties is disappointed with it.”); *N. Shipping Funds I, LLC v. Icon Cap. Corp.*, 921 F. Supp. 2d 94, 104 (S.D.N.Y. 2013) (“Generally, no fiduciary duties arise where parties deal at arm's length in conventional business transactions.” (quoting *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 592 F. Supp. 2d 608, 624 (S.D.N.Y. 2009))).

²⁵ See Daniel B. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, in THE OXFORD HANDBOOK OF FIDUCIARY LAW 3, 9 (Evan J. Criddle et al. eds., 2019).

²⁶ See, e.g., *id.* (“With regard to the ‘principal’ or beneficiary, a court is more likely to conclude that a relationship is ‘fiduciary’ if a principal places confidence and trust in the agent; if a principal lacks expertise, knowledge, sophistication, or experience; or if a principal depends or relies heavily upon the agent’s advice or judgment.”).

information relationships are imbalanced and susceptible to great abuse by the dominant party. This is one of the main privacy problems addressed by a duty of loyalty. Rather than treating all kinds of information relationships as equal and fungible, it would increase obligations and restrictions on dominant parties as they amass power. The more power a company has in a relationship, the more protective and loyal it must be. A duty of loyalty would add an additional layer to data privacy law. Privacy would no longer be primarily about the data; instead, it would have to consider the relationships between people and the companies to which they are exposed.²⁷

Although the ongoing interactions between people and platforms might not seem like a meaningful “relationship” in the traditional sense of the word, these relationships give rise to the same relational dynamics and abuses that trust rules are meant to address. At the outset, the interactions between people and platforms are firmly established as legal relationships. Courts consistently bind people who use websites and apps to the terms of use agreements imposed by companies.²⁸ Yet, technologically-mediated relationships between people and companies are more than mere legal formalities, even if they are different from the meaningful relationships we have with our friends, advisors, and employers. Julie Cohen has argued that “[t]he mere fact of an ongoing service relationship signifies relatively little in an era when relationships have been redefined as mass-market products and are mediated by standardized interfaces designed for large-scale, networked interconnection.”²⁹ That may be true, but we think these relationships also involve far more interplay, exposure, and personalization than standard commercial services and widgets. In critiquing applying design and consumer protection obligations in the language of trust, Cohen suggests that although in a sense she *trusts* her desk chair not to collapse when she sits in it, “it is far more useful to be able to speak concretely about such matters as material tolerances and manufacturing specifications—and to be able to invoke corresponding tort and regulatory frameworks—than it is to talk in airy generalities about the nature of my relationship to the chair manufacturer.”³⁰

We also agree with Cohen about the need to be more specific with the rules for tech companies, which we address below. But the relationships that people have with chair manufacturers, or even brick-and-mortar merchants and

²⁷ See, e.g., Richards & Hartzog, *supra* note 19, at 497 (imagining a future in which privacy focuses “directly on power imbalances in relationships rather than indirectly through data rules”).

²⁸ Hartzog, *Website Design as Contract*, *supra* note 21, at 1644–45; Hartzog, *The New Price to Play*, *supra* note 21, at 417.

²⁹ COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, *supra* note 5, at 10.

³⁰ *Id.*

providers of services in a pre-platform era, bear almost no resemblance to the relationship between people and platforms. Critics of a duty of loyalty have pointed out that treating platforms the same as a medical doctor, for example, strips away the affordances of the platform and the realities of scale.³¹ But it is the precise affordances of hardware and software that make the relationship between people and platforms highly imbalanced and unique in ways that compel relational rules, such as the duty of loyalty.

B. Key Traits of Modern Information Relationships

The relationship between people and platforms has at least five traits that, when combined, make it highly imbalanced and worthy of intervention at the relational level: the relationship (1) is *ongoing*, (2) is high *frequency*, (3) occurs within an *interactive* environment, (4) operates within an environment completely *constructed* for the individual, and (5) operates within an environment that is *responsive* to the individual by the dominant party.³² Let's break these traits apart.

1. Ongoing

When people buy chairs, or ages ago, when they bought CD-ROMs containing software in stores, such transactions are what we might think of as discrete. Although Office Depot or Adobe hoped customers would return, barring returns or malfunctions, the relationship between customer and manufacturer or software developer typically had some distance and downtime. Those days are long gone.³³ Platforms leveraging browsers, apps, and cloud computing have obliterated the concept of discrete one-time interactions.³⁴

³¹ See, e.g., Cohen, *Scaling Trust and Other Fictions*, *supra* note 5 (“The information fiduciaries proposal abstracts speed, immanence, automaticity, and scale away from that encounter and then assumes they never mattered in the first place. In the process, it both sacrifices the fiduciary arrangement’s most essential characteristics and fails to reckon adequately with the characteristics of the platform-consumer relationship that are most problematic.”); Khan & Pozen, *supra* note 7, at 514 (imagining a doctor who relies on third-party marketing for her income).

³² For an interesting approach to how laws might accommodate duties of loyalty and care in parties that demand high degrees of trust but are not traditionally recognized as fiduciaries, see Ethan J. Leib, *Friends as Fiduciaries*, 86 WASH. U. L. REV. 665, 691 (2009) (“[F]iduciary law is about signaling to fiduciaries that they ought not to be self-interested in transactions with and for their beneficiaries; it is generative of trust where costs of distrust are especially high.”).

³³ See Scholz, *supra* note 3, at 198 (“The ideal of the one-off consumer transaction is dead. Instead of selling or licensing goods and services to consumers, firms today seek to build ongoing, evolving relationships with consumers based on constant contact. This trend is likely to continue, as the always-on devices that comprise the Internet of Things proliferate and cover an increasing number of everyday objects.”).

³⁴ See *id.* at 151–54 (explaining that platforms track and collect customers’ information).

Virtually every interaction requires an account creation with an intention of an always-evolving delivery of services, often accompanied by email, app, or operating system notifications. A platform's ideal scenario is that once a person signs up for a platform, they regularly visit and never leave. Systems are, to use the parlance of Silicon Valley, "optimized for engagement." Data and attention continue to be given by consumers, and patches and updates continue to be delivered by developers with no planned end date.³⁵ Such a never-ending story warrants rules matched to the nature of the relationship and ideally designed to foster long term, sustainable, profitable relationships between people and platforms.

2. *Frequent*

In addition to wanting to be with you forever, platforms want to be with you *constantly*. People may go shopping in physical stores at most once or a few times a week. They might take occasional advantage of an offline service like babysitting or dry cleaning. But, on average, people interact with apps and websites nearly a hundred times *every day*.³⁶ Popular apps often get checked multiple times within the same hour or minute.³⁷ While we may commonly use the same tool tens or hundreds of times a day (think how often you pick up a pen, sit in a chair, or drink from a cup), we might think it strange to browse the aisles of a store or call our financial advisor ten times a day, every day, for years on end. But how many times have you checked your phone today? For Facebook, Amazon, Google, Twitter, and a host of other dominant platforms, failure to check in regularly is seen as a problem, and constant interaction from the user is a rewarded metric. Here, too, the practice of notifications pushed to the customer allow the frequency of interactions to be maintained. People can be engaged in ongoing relationships without having to interact with them all the time, but platforms ideally want both a long duration and a high frequency of

³⁵ See, e.g., Alex Heath, *Facebook's Lost Generation*, VERGE (Oct. 25, 2021, 7:00 AM), <https://www.theverge.com/22743744/facebook-teen-usage-decline-frances-haugen-leaks>.

³⁶ *Americans Check Their Phones 96 Times a Day*, ASURION (Nov. 21, 2019), <https://www.asurion.com/about/press-releases/americans-check-their-phones-96-times-a-day/>; Gabrielle Pickard-Whitehead, *66% of Americans Check Phone 160 Times a Day, Here's How Your Business Can Benefit*, SMALL BUS. TRENDS (Mar. 3, 2020), <https://smallbiztrends.com/2020/03/2020-mobile-phone-usage-statistics.html>; see also LEE RAINIE & KATHRYN ZICKUHR, PEW RSCH. CTR., *AMERICANS' VIEWS ON MOBILE ETIQUETTE 12* (2015), <https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity/> (noting a high number of smartphone users check their phone apps "continuously"); *Average Time Spent Daily on Social Media (Latest 2022 Data)*, BROADBAND SEARCH, <https://www.broadbandsearch.net/blog/average-daily-time-on-social-media> (last visited Apr. 26, 2022) ("On average, [we] spend . . . two hours and twenty-seven minutes[] on social media each day.").

³⁷ See, e.g., *supra* note 36; Trevor Wheelwright, *2022 Cell Phone Usage Statistics: How Obsessed Are We?*, REVIEWS.ORG (Jan. 24, 2022), <https://www.reviews.org/mobile/cell-phone-addiction/>.

engagement. For ad-driven businesses on an engagement business model, this is the gold mine that generated the Facebook and Google fortunes, among the fortunes of many others.³⁸

3. *Constructed*

It is no secret that companies design their sales infrastructure to influence their customers and clients.³⁹ Grocery stores place milk and eggs at the opposite side of the store from the entrance to encourage people to walk the aisles.⁴⁰ Office designers make conference rooms totally transparent for when you want everyone to see who you are meeting with, or completely opaque for when you do not.⁴¹ It happens online as well. As Joel Reidenberg noted in his foundational article *Lex Informatica*, companies leverage the power of information technologies to create policy rules that affect people.⁴²

But the extent to which tech companies control mediated environments is so great that it deserves sustained scrutiny. Our dealings with platforms occur *entirely* on their terms.⁴³ They control *who* has access, *what* they see and do, *when* they see it and take action, *where* they receive signals and make choices, and *why* particular people see specific things and are given preconstructed options.⁴⁴ In unmediated relationships, people have a degree of flexibility to work within a structured environment. They can choose from an endless array of physical actions and social interactions and even change the structure of the environment themselves, like moving the physical location items, modifying the placement and content of signs, and switching between modes of communication like writing or speaking.

But in digital environments, people can only click on the options they are given. They can only address the audience they have been presented in the

³⁸ See, e.g., Sarah Frier, *Facebook Really Wants You to Come Back*, Bloomberg (Jan. 31, 2018, 5:00 AM), <https://www.bloomberg.com/news/features/2018-01-31/facebook-really-wants-you-to-come-back>.

³⁹ See WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 34–35 (2018) (explaining that design shapes perceptions, behavior, and values).

⁴⁰ *Id.* at 35.

⁴¹ *Id.*

⁴² Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554–55 (1998) (“Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations. Even user preferences and technical choices create overarching, local default rules.”).

⁴³ *Cf.* HARTZOG, *supra* note 39, at 1 (explaining tech companies leverage design to control privacy settings); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1000–03 (2014).

⁴⁴ See HARTZOG, *supra* note 39.

format provided. Structures are designed to eliminate accidents and serendipity, save for the emergent behavior of automated outputs powered by machine learning. And tech companies keep a tight leash on their bots. Our ability to interrogate, analyze, question, tinker, learn, and otherwise calibrate our dealings with tech companies is virtually nonexistent.⁴⁵ As human users of these technologies, we are essentially powerless. Data subject rights of access, rectification, and deletion like those offered by the GDPR in theory empower us a little, but in practice these rights are difficult to exercise at scale; since they are limited only to personal data, data subject rights do very little to improve our agency within constructed environments outside of personal data transparency and management.⁴⁶

4. *Interactive*

When people read newspapers or magazines, watch television, or listen to the radio, they are essentially passive. There is no give and take between the mind and the medium. The flow of information is one way. It would be a stretch to call these interactions relationships, even when we have subscription contracts with them.⁴⁷ But of course, the relationship between people and platforms is highly interactive. We create detailed accounts and profiles. We search, amass networked connections, post pictures and status updates, press buttons, tweak settings, adjust sliders, arrange layouts, and project information streams that we don't even know about. We essentially do uncompensated work that creates huge value for them. And of course, all this interactivity can be further quantified, optimized, and utilized to benefit the platform.

5. *Responsive*

The final component of modern information relationships is that the *ongoing, frequent, constructed*, and *interactive* nature of the exchanges between people and platforms enables companies to design their mediated environment to be acutely *responsive* to people's choices and profiles. News feeds, suggested products, and information change on the fly according to previous clicks, and profiles created from personal data accumulate over time. Our mediated environments are tweaked based on individual data and up-to-the-second

⁴⁵ See *id.* chs. 2 & 6.

⁴⁶ See Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023).

⁴⁷ See, e.g., Hartzog, *The New Price to Play*, *supra* note 21, at 405–06.

wisdom from constant experiments on us through A/B testing designed to maximize engagement and keep our eyes glued to the screen.⁴⁸

This powerful incentive for such “growth hacking” makes the uniquely intertwined relationship between platforms and people incredibly dangerous.⁴⁹ It is far from what should be considered arms-length. Arms-length relationships might have one or two of the traits listed above. But no legal, commercial, or social relationship on earth, from merchants to professionals to employers to loved ones, features the same potent combination of traits as modern technologically-mediated information relationships. Platforms cannot be arms-length when they are already living in in our heads.

We do not mean to imply that information relationships present wholly unique problems. Rather, our analysis of the affordances of information technologies suggests that it would be a mistake to treat these relationships as arms-length, even if they are cabined to some extent by consumer protection and data protection rules. They are too one-sided and prone to abuse to tolerate any arms-length fiction. A duty of loyalty is not sufficient to solve all our privacy problems. But it is necessary so long as the affordances of the tools, incentives for self-dealing, and legal contracting status of the parties places people in danger every time they create an account online. In this way, a surprising virtue of a loyalty approach is that it reveals how modern information relationships do not resemble anything approaching arms-length transactions. Once lawmakers fix this problem and embrace the relational turn in privacy law, several different possibilities open up, including supporting public governance, new substantive rules, and a less individualistic approach to privacy.

II. LOYALTY ACHIEVES WHAT CARE CANNOT

A second set of critiques surrounding a duty of loyalty is that it would be unnecessary. These criticisms take a variety of forms. Responding to Jack Balkin’s proposal to impose common law fiduciary duties (including a duty of loyalty) on platforms, Lina Khan and David Pozen have suggested that imposing fiduciary duties like loyalty on platforms might (1) do little in practice and (2)

⁴⁸ See, e.g., Calo, *supra* note 43.

⁴⁹ The term “growth hacking” has been adopted to refer to aggressive strategies by tech companies to grow their user base quickly and significantly. For more information on growth hacking, see RAYMOND FONG & CHAD RIDDERSEN, *GROWTH HACKING: SILICON VALLEY’S BEST KEPT SECRET* (2017); Timo Herttua, Elisa Jakob, Sabrina Nave, Rambabu Gupta & Matthäus P. Zylka, *Growth Hacking: Exploring the Meaning of an Internet-Born Digital Marketing Buzzword*, in *DESIGNING NETWORKS FOR INNOVATION AND IMPROVISATION* 151, 151–61 (2016); René Bohnsack & Meike Malena Liesner, *What the Hack? A Growth Hacking Taxonomy and Practical Applications for Firms*, 62 *BUS. HORIZONS* 799 (2019).

forestall other, more radical approaches to the consumer protection problems raised by platforms, including those involving competition law.⁵⁰ There are other forms of this critique, too, suggesting that loyalty duties are unnecessary because (3) a duty of care placed on data collectors would be sufficient, or that (4) an American version of Europe's GDPR could solve the problem.⁵¹ Each of the four variants of the "loyalty is unnecessary" argument are worth addressing briefly in turn because doing so reveals the surprising virtue that loyalty is not only necessary but also potentially inspirational. Loyalty, in other words, represents a state of mind with revolutionary potential for privacy reform.

A. Loyalty Makes People's Choices Less Dangerous

First, with respect to Khan and Pozen's suggestion that imposing fiduciary duties like a duty of loyalty on platforms might do little in practice,⁵² we must respectfully disagree, at least as regards the version of a duty of loyalty we articulate in this paper and in other work. As privacy law scholarship has documented at length, the current default model of U.S. privacy law is one of "notice and choice," under which firms are subject to three principal rules: (1) do not lie about data practices, (2) do not cause unreasonable harm (reasonable harm is just fine), and (3) do follow the Fair Information Practices, most notably "notice and choice."⁵³ In practice, these rules mean that companies can largely do what they want with human data as long as they have a vague privacy policy, do not cause significant economic or other harm, and do not lie about what they are doing in their often inscrutable privacy notices. A duty of loyalty would change this situation considerably by placing an enforceable obligation on companies to act in the best interests of their human customers, rather than allowing them to rely on vague terms and conditions hidden in a privacy policy to justify whichever data practices serve their own purposes most efficiently. This would mean that humans making choices could rest easy that one of the choices they were given would allow betrayal or manipulation by the company. Because betrayal or manipulation would be taken off the table, they could

⁵⁰ Khan & Pozen, *supra* note 6, at 534–35. Pozen and Khan are particularly alarmed by a proposal by Jack Balkin and Jonathan Zittrain to create a "grand bargain" for platforms in which fiduciary duties would be imposed in exchange for a preemption of state privacy laws (and, Pozen and Khan fear, for competition regulators paying less attention to the anticompetitive effects of platform size and power). *Id.* at 535.

⁵¹ See Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 11, at 1713 (discussing proposals for a U.S. GDPR); see also Khan & Pozen, *supra* note 6, at 522, 535 (alleging the redundancy of information fiduciary proposals).

⁵² Khan & Pozen, *supra* note 6, at 534.

⁵³ See, e.g., HARTZOG, *supra* note 39, at 58; Richards & Hartzog, *supra* note 20, at 1463, 1471; Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 11, at 1704; Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883 (2013).

choose knowing that all choices were safe ones, rather than ones that exposed them to unforeseeable dangers at the hands of the company. Placing duties of loyalty on information collectors would thus “be a revolution in privacy law.”⁵⁴

B. Loyalty Complements Other Interventions

Second, we must also disagree with Khan and Pozen’s claim that the imposition of a duty of loyalty would foreclose other promising means of addressing the relatively unchecked power of platforms over our lives and the economy.⁵⁵ We believe that a duty of loyalty must be one piece of a much larger regulatory response—not merely to the problems of platform power and unchecked informational capitalism but also to the problems of the information revolution as a whole. The challenges of the industrial revolution were not checked by a single legal rule like negligence, workplace safety, speed limits, food labeling laws, or a prohibition on unfair and deceptive trade practices.⁵⁶ Similarly, it defies both the insights of legal history and common sense to think that a duty of loyalty, or any other rule in isolation, would solve the problems of the information revolution. Indeed, in other work, we have argued in detail that our approach to these problems must be multipronged and explicitly include what we call “corporal” regulation, involving corporate and competition law, as any part of a solution to the problems of platform power.⁵⁷ (We also note in conclusion that Khan and Pozen’s critique was tailored to Jack Balkin’s “information fiduciary” model—a proposal that involves the imposition of state-law fiduciary duties on platforms and has substantial differences from the duty of loyalty we articulate here and in other papers.)⁵⁸

C. Loyalty Avoids the Harm Trap

Third, with respect to the suggestion that a duty of loyalty would add little that a duty of care would not already cover, such a suggestion misunderstands the critical differences between duties of care and duties of loyalty. To be sure,

⁵⁴ Richards & Hartzog, *supra* note 3 (manuscript at 72).

⁵⁵ Khan & Pozen, *supra* note 6, at 513–14.

⁵⁶ See, e.g., Judson MacLaury, *Government Regulation of Workers’ Safety and Health, 1877-1917*, U.S. DEPT OF LAB., <https://www.dol.gov/general/aboutdol/history/mono-regsafefintrotoc> (last visited Apr. 26, 2022); Xaq Frohlich, *The Informational Turn in Food Politics: The U.S. FDA’s Nutrition Label as Information Infrastructure*, 47 SOC. STUD. SCI. 145 (2017); Dee Pridgen, *The Dynamic Duo of Consumer Protection: State and Private Enforcement of Unfair and Deceptive Trade Practices Laws*, 81 ANTITRUST L.J. 911, 912–14 (2017) (discussing the development of state and federal trade practice laws, which began well after the end of the Industrial Revolution in the United States).

⁵⁷ See Hartzog & Richards, *Privacy’s Constitutional Moment*, *supra* note 11, at 1742–45.

⁵⁸ Khan & Pozen, *supra* note 6, at 501.

duties of loyalty and care share a common genealogy: they, along with the duty of confidentiality, are the three most basic fiduciary duties.⁵⁹ It follows from this fact that the three duties have distinct components. The duty of care requires that fiduciaries take care not to cause *harm* to those they owe fiduciary duties—most often, the vulnerable parties that the law steps in to protect like wards, shareholders, and professional clients.⁶⁰ Its cousin negligence, one of the common law’s many responses to the Industrial Revolution, imposes a weaker duty as against the whole world not to act unreasonably and thus cause harm.⁶¹ Duties of care and negligence are therefore rooted in reasonable behavior and harm avoidance—I have to act in a way that is reasonable under the circumstances, so as not to cause you harm, and if I fail to do that, you can sue me to remedy the harm I caused.

Loyalty is different from care. It is not about my state of mind with respect to the injury I cause. Loyalty is instead about avoiding *betrayal*. It is about my state of mind with respect to your best interests, and it is about not exploiting conflicts of interest for my own advantage.⁶² For instance, a clear example of disloyalty would be when Target Corporation famously discovered that its pregnant customers did not like receiving coupons that revealed Target’s data scientists had figured out they were pregnant.⁶³ Target changed its marketing practices to hide the coupons in a sea of intentionally irrelevant ones (like wine glasses and lawn mower blades) so that its customers would use the coupons instead of freaking out, and then become habituated Target customers once the baby arrived and they ran out of energy.⁶⁴ Such use of sensitive information about current customers is legal under current U.S. law.⁶⁵ It has nothing to do with any duty of care, but it would be a clear violation of a duty of loyalty.

At bottom, then, care is about avoiding harm while loyalty is about avoiding betrayal.⁶⁶ The legal wrong in a breach of care is the resulting economic,

⁵⁹ See Balkin, *Information Fiduciaries*, *supra* note 3, at 1207–08; Haupt, *supra* note 3, at 36.

⁶⁰ Balkin, *Information Fiduciaries*, *supra* note 3, at 1207–08.

⁶¹ WILLIAM L. PROSSER, *HANDBOOK OF THE LAW OF TORTS* 183 (1941).

⁶² Balkin, *Information Fiduciaries*, *supra* note 3, at 1208.

⁶³ Charles Duhigg, *How Companies Learn Your Secrets*, *N.Y. TIMES MAG.*, Feb. 19, 2012, at 30.

⁶⁴ *Id.* For an elaboration of this point, see NEIL RICHARDS, *WHY PRIVACY MATTERS* 33–37 (2022).

⁶⁵ *See generally* Paul Ohm, *Sensitive Information*, 88 *S. CAL. L. REV.* 1125 (2015) (exploring the category of sensitive information in data privacy frameworks).

⁶⁶ To complete the set, the legal wrong in a breach of a duty of confidentiality is an improper *disclosure* of confidential information. *See* Richard Painter, *Fiduciary Principles in Legal Representation*, in *THE OXFORD HANDBOOK OF FIDUCIARY LAW* 265, 269–71 (Evan J. Criddle et al. eds., 2019); TAMAR FRANKEL, *FIDUCIARY LAW*, 107–08 (2008) (“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

physical, or other kind of harm, but the legal wrong of disloyalty is, first and foremost, the damage done to the relationship itself. This is a particularly significant distinction for privacy law because plaintiffs in privacy and data breach lawsuits have struggled to articulate diffuse but real informational injuries. This situation has been made worse in recent years as courts have substantially tightened the rules for what counts as a legally cognizable “concrete” injury under Article III standing doctrine.⁶⁷ A new and stringent requirement of “concreteness” makes it more difficult to prove harm and threatens the ability of legislatures to authorize novel forms of legal remedies. Crucially, though, loyalty does not have this problem—not merely because the legal injury in loyalty cases is the disloyalty itself but also because this injury is one that has been already recognized by courts as legally sufficient within standing doctrine.⁶⁸ To the extent the tightening of standing doctrine means that only long-recognized claims can be brought in federal court, another surprising virtue of a duty of loyalty is that it is an old common-law doctrine, and thus, breaches of loyalty are undeniably concrete and actionable.

In sum, then, duties of loyalty and duties of care are distinct. Duties of care are about acting reasonably to avoid harm, but the focus of loyalty is on the sanctity of a relationship and removing an incentive and ability to wrongfully profit by taking advantage of a power disparity. We believe that privacy law has room for both duties of care and of loyalty, but they should not be conflated because they serve different purposes. Critically, because loyalty duties are rooted in betrayal rather than harm, they have significant consumer protection advantages that care duties do not.⁶⁹

entrustors.”).

⁶⁷ *E.g.*, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547–49 (2016).

⁶⁸ To get a bit technical, in *Spokeo* terms, then, a breach of a legally-imposed duty of loyalty would be a “concrete” 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.” *Id.* at 1549. But because a breach of a duty of loyalty has been recognized as such a basis for centuries, duties of loyalty do not raise this *Spokeo* problem. *See, e.g.*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 860–61 (2022); 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.”). By contrast, although duties of care in general would be concrete, statutory causes of action rooted in novel theories of harm would seem to have to run through the *Spokeo* test.

⁶⁹ *See* Data Care Act of 2019, S. 2961, 116th Cong. §§ 2–3(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

D. *Loyalty Animates Legislation and Enforcement*

Fourth, and finally, while the notion of a U.S. GDPR may have intuitive appeal in theory, we believe that any such law would be insufficiently protective in practice. There are several reasons for this conclusion, but the most important one is that U.S. privacy rights against companies are different from those in the European Union. In the United States, such rights would likely be consumer protection rights protecting economic interests and could be whittled down in the legislative process by tech company lobbying efforts. By contrast, the GDPR rests upon a solid constitutional footing of fundamental rights to privacy that are simply not present under current American law. In sharp contrast to the United States, E.U. fundamental rights law has long protected privacy as an explicit constitutional right.⁷⁰ Today, the E.U. Charter recognizes two separate fundamental rights to privacy: a right to “respect for his or her private and family life,” in Article 7, and a separate right to “protection of personal data,” in Article 8.⁷¹ Moreover, these European rights are subject to the doctrine of “horizontal effect.” Under this doctrine, a member state can violate a person’s fundamental rights when it fails to protect it sufficiently against violations by other members of society.⁷² Thus, the GDPR’s guarantee of privacy and data protection rights against companies is more than mere commercial regulation—because it is the direct implementation and extension of constitutional rights, the GDPR should be understood as having constitutional status.

Similarly, as we have just noted, American privacy plaintiffs have struggled to overcome the hurdles of limited remedies and procedural obstacles like Article III standing doctrine. Again, by contrast, European data protection plaintiffs have achieved a remarkable string of victories vindicating rights under the GDPR and its precursor, the Data Protection Directive, establishing the “right to be forgotten” and invalidating both data retention rules and inadequate cross-border transfer agreements.⁷³ Crucial to these results has been the

or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act.”).

⁷⁰ *E.g.*, Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

⁷¹ Charter of Fundamental Rights of the European Union arts. 7–8, Nov. 26, 2012, 2012 O.J. (C 326).

⁷² Stephen Gardbaum, *The “Horizontal Effect” of Constitutional Rights*, 102 MICH. L. REV. 387, 395, 397 (2003) (describing the European horizontal effect doctrine as “impos[ing] constitutional duties on private actors as well as on government”).

⁷³ Case C-131/12, *Google Spain v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González*, ECLI:EU:C:2014:317, ¶¶ 91, 94 (May 13, 2014); *see, e.g.*, Case C-293/12 and Case C-594/12, *Digital Rts. Ireland Ltd. v. Minister for Comm’ns, Marine and Nat. Res. & Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238, ¶¶ 66–71 (Apr. 8, 2014); Case C-362/14, *Maximillian Schrems v. Data Prot. Comm’r*, ECLI:EU:C:2015:650, ¶ 102 (Oct. 6, 2015).

European Court of Justice (CJEU), the highest court for questions of E.U. law. In these and other cases, the CJEU has simultaneously established these new data protection rights while also establishing its own relevance as a major player in the new European constitutional order.⁷⁴ As Bilyana Petkova has argued, the CJEU's decisions have enshrined data protection as "the main tenet of constitutional identity" in the European Union.⁷⁵ This is why European data protection law often seems so strikingly powerful to American observers compared to domestic consumer privacy rights.⁷⁶ As much as anything, then, the GDPR is a state of mind for Europeans. 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 termed "GDPR-lite."⁷⁷

To be sure, a GDPR-like approach has undeniable virtues, even in a weakened "GDPR-lite" form. The European model of data protection regulation is the product of great wisdom, experience, and effort. Its framework has proven resilient and durable across the decades, and data protection rules can be formidable and empowering when done properly. It also offers an emerging global standard for interoperable data sharing. But the data protection model has some real weaknesses as well. It can treat data processing as something inevitable or even virtuous, with the effect of normalizing surveillance and processing. To the extent that data protection rights are usually long on procedural requirements, they are often short on the kinds of substantive prohibitions that would take certain kinds of invidious data uses off the table. And data protection rules focus primarily on the data itself, rather than on the relationships and in the contexts in which those data are collected, used, and disclosed.⁷⁸ Perhaps, then, it should be no surprise that EU regulators are starting to flirt with imposing substantive loyalty duties upon the largely procedural GDPR baseline. In the European Union, regulators have proposed a new draft data governance act that includes a duty of loyalty for data. And in post-Brexit

⁷⁴ Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security*, BROOKINGS (Aug. 5, 2020), <https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/>.

⁷⁵ Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 140, 154 (2019).

⁷⁶ See, e.g., Aarti Shahani, *3 Things You Should Know About Europe's Sweeping New Data Privacy Law*, NPR (May 24, 2018, 11:37 AM), <https://www.npr.org/sections/alltechconsidered/2018/05/24/613983268/a-cheat-sheet-on-europe-s-sweeping-privacy-law> (discussing the GDPR and its robust protection for consumer data privacy and noting concerns that GDPR will "hurt businesses that rely on data collection").

⁷⁷ For an extended version of an argument along these lines, see Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 11, at 1727–32.

⁷⁸ *Id.* at 1717–21.

Britain (where the GDPR still applies), the British Information Commissioner's Office has imposed a duty of loyalty on those who process children's data.⁷⁹

This analysis points us towards the first of the surprising virtues of a duty of loyalty for privacy law. Loyalty is not ineffective or redundant. On the contrary, loyalty is both powerful and distinctive. Loyalty can be a state of mind for American privacy reform, one that could offer the same vitality and political salience in American legal culture that the fundamental right of data protection possesses in Europe. As we have seen, the GDPR is the manifestation of data protection as a fundamental human right, which itself is a commitment to the idea that people should be able to determine their informational fates for themselves. But when it comes to data privacy in the United States, we lack an equivalent coherent guiding light. "The right to be let alone" worked for a while, but it has crumbled under its capaciousness. "Do not lie" and "do not harm" are bedrock ideals, but they are also the status quo—and it is clear that the status quo is inadequate. "Follow the fair information practices" (FIPs), while necessary, is about as inspirational as a CVS receipt.⁸⁰ And we have already seen that a U.S. version of the GDPR would be insufficient.

A duty of loyalty could fill this role for U.S. privacy law. Of course, loyalty cannot solve all privacy problems on its own. But it can do three important things. First, loyalty can supplement public governance of privacy rules by authorizing *effective private rights of action* for breaches of the duty—ones that sidestep the standing doctrine problems that have plagued harm-based theories of relief.⁸¹ Second, loyalty could supply an *interpretive lodestar* to U.S. privacy law, an equivalent to Europe's robust protection of existing data protection rules, and one that even improves upon some of the limitations of the European approach.

Third, and perhaps most important, loyalty could supply a *political lodestar* for privacy reform more generally. In contrast to technocratic terms like "data minimization" and "legitimate interests of the data controller," loyalty is clear, it is easy to understand, and it is potentially robust enough to counterbalance industry claims about the importance of "innovation" or the seductive but false

⁷⁹ See *Commission Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, at 18–19, COM (2020) 767 final (Nov. 25, 2020); INFO. COMM'RS OFF., *AGE APPROPRIATE DESIGN: A CODE OF PRACTICE FOR ONLINE SERVICES 9–10* (2020).

⁸⁰ See generally Hartzog, *supra* note 20 (presenting a balanced view of the strengths and shortcomings of FIPs).

⁸¹ Scholz, *supra* note 3, at 197 ("If public regulation is needed to further protect consumers, as is likely, the information-sharing and norm-sharing function of fiduciary duties, as described above, will aid in the development of appropriate consumer protection laws through the information-forcing . . .").

idea that commercial data processing carries First Amendment value. 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. In this way, loyalty can be a state of mind; one that has revolutionary potential to stimulate meaningful privacy reform.

III. LOYALTY PRIORITIZES HUMAN VALUES

One of the most prominent critiques levied against the idea of imposing duties of data loyalty on companies is Khan and 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.”⁸² Khan and Pozen reject the idea of conflicting loyalties as well as the possibility of prioritizing the interests of customers over shareholders, which they contend would conflict with the dominant understanding of corporate law.

Responding to this criticism highlights another surprising virtue of data loyalty: it prioritizes people over profits and, in doing so, facilitates a substantive embrace of a broad array of human values over privacy law’s reflexive deference to individual choice, consent, and control. Lawmakers and industry love “notice and choice” proceduralism because it allows them to avoid the difficult task of prioritizing human interests and making substantive interventions. If preferences vary wildly, then this fallacy tempts us, and surely an approach rooted in choice would solve the problem. But lawmakers imposing a duty of loyalty cannot avoid this task. In essence, lawmakers embracing a properly conceptualized duty of loyalty would center human values at the heart of our information rules while simultaneously clarifying the order of operations regarding duties owed to different parties.

⁸² Khan & Pozen, *supra* note 6, at 534. The authors also note that “the 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.” *Id.* at 529.

A. *Data Loyalty's Illusory Conflicts*

As an initial matter, the “divided loyalties” argument against relational duties is debatable and, at most, can be fixed by lawmakers without substantially remaking corporate law.⁸³ Andrew Tuch argues that Khan and Pozen “significantly overstate the threat that corporate and fiduciary law pose for the information fiduciary model.”⁸⁴ Tuch explains that “imposing user-regarding 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.”⁸⁵

Tuch also argues that “the plausible outcome of an information fiduciary regime is exactly the opposite of what Khan and Pozen fear. Under 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.”⁸⁶ In other words, the loyalty that directors owe to shareholders takes a backseat to all other legal obligations placed upon the corporation, including duties of loyalty to customers.⁸⁷ In fact, if a duty of data

⁸³ See, e.g., Balkin, *The Fiduciary Model of Privacy*, *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.”).

⁸⁴ Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897, 1902, 1909–10 (2021). Tuch argues that corporate law only imposes duties on *directors*, not corporations, and the information fiduciaries proposal imposes duties on *corporations*, not directors. *Id.* Relational duties would not create a set of inconsistent obligations among a *single* fiduciary. The issue of parallel fiduciary obligations owed by corporations as a whole to clients and directors to shareholders is routine. 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. *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 clearly that directors must act ‘within the law.’”).

⁸⁵ *Id.* at 1902 (“The criticism rests on a partial understanding of corporate law doctrine and theory. The criticism sees conflicting obligations where none plausibly 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.”).

⁸⁶ *Id.*

⁸⁷ *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,

loyalty owed by platforms to people is made positive law, a director that acts with the intent to act in conflict with a customer's best interests or who 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 customers.⁸⁸

It is thus indisputable that lawmakers can place duties of data loyalty on corporations. But, if they do so, they must prioritize loyalties. This would resolve any lingering "divided loyalty" concerns regarding shareholders, as well as conflicting loyalties between customers and third-party vendors. Self-interested actions would be allowed, but only if they don't conflict with a customer's best interests regarding their data and mediated experiences. Duties of data loyalty thus face no problems from other state laws. Moreover, a federal law imposing data loyalty obligations would avoid the Khan and Pozen conflicting loyalty argument for a second reason: it is an elementary principle of U.S. constitutional law that a federal duty of loyalty would take precedence over any state duties by operation of the Supremacy Clause. The federal minimum wage law is consistent with shareholder fiduciary duties, and a federal duty of loyalty would be as well.

But what about conflicts between different kinds of customers? James Grimmelmann noted that platforms like eBay serve both buyers and sellers, serving up potentially conflicting loyalties.⁸⁹ To Grimmelmann's example, we could also add Uber and Lyft serving drivers and passengers, AirBnb serving renters and leasers, and even Google serving advertiser and human users of its services. This, too, is a common problem in the law of fiduciaries, which has developed several ways to deal with such inevitable conflicts. Andrew Gold explains that "conflicts 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).⁹⁰ The "best interests" polestar of loyalty, by design, accommodates all kinds of self-serving behavior. It simply makes self-serving

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.").

⁸⁸ See *id.* at 1919 n.120 (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))).

⁸⁹ Grimmelmann, *supra* note 10.

⁹⁰ Andrew S. Gold, *The Fiduciary Duty of Loyalty*, in *THE OXFORD HANDBOOK OF FIDUCIARY LAW* 385, 390, 398 (Evan J. Criddle et al. eds., 2019).

behavior allowable only in instances where it aligns with the best interests of the primary trusting party.⁹¹ Even among the same type of customer, a reasonable critique of applying a novel duty of loyalty to large tech companies is that these entities would be obligated to act in the best interests of billions of individuals, whose “best interests” might differ from person to person. There are several steps that lawmakers might take to help resolve this looming conflict.

The first step would be to limit the scope of the duty to the extent of the vulnerability. Trusted parties must be loyal when collecting and processing people’s data and making design choices that affect their mediated experiences. Under this rule, consideration of a trusting party’s best interests would be limited to what was entrusted, the purpose of exposure and the relationship, and whether a trusted party’s actions relating to that exposure are self-serving and adversarial to a human customer’s wishes or well-being. So, for example, under such an approach, Snapchat would not generally be responsible for making sure their app users were responsible drivers, but they would be prohibited from taking money from car insurance companies to create a mini-game asks people to upload pictures of them driving so that insurance companies could track them and increase their premiums for dangerous drivers. Snapchat would also be prohibited from creating algorithms that amplified other people’s driving videos solely for the purpose of distorting how popular the driving game was and to juice engagement metrics.⁹² However, Snapchat degrading or blocking an app user’s driving videos would *not* count as a breach of loyalty because deleting posts in this context would not increase their vulnerabilities from exposure. Limiting a trusting party’s “bests interests” to those affected by its exposure of data and attention would help keep loyalty-bound companies from having to serve as general-purpose caretakers for trusting parties.

Regarding the difficulties of accounting for the “best interests” of millions of unique trusting parties, lawmakers could also follow tort law’s move to a more objective standard: the reasonable customer. Not only would a reasonable customer standard help companies better determine the scope of their duties but it would also inject a normative element into the analysis. A reasonable customer

⁹¹ 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.”).

⁹² James Grimmelmann, *Speech Engines*, 98 MINN. L. REV. 868, 929–31 (2014) (resenting a “subjective dishonesty” standard for search engines); Grimmelmann, *supra* note 10 (arguing that since a search engine “requires substantial discretion to determine what its users consider relevant” (because different people might want different things), the legal system should defer to search engines’ best judgments).

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 the risks of abuse. The duty would be the most robust where the volume of data collected, the company's role in mediating other transactions and relationships, and the potential for manipulation are 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 can craft a unique and tailored approach that borrows from how duties of loyalty operate in other contexts without being bound by them.

B. The Diverse Value-Forcing Function of Data Loyalty

In fact, the need to clarify how a duty of loyalty would work within information relationships could help bring a substance and normative commitment that has been missing in privacy law. Lawmakers who embraced a data loyalty approach would be forced to make substantive decisions about who is protected, who is duty-bound, and what specific conduct is prohibited in service of specific goals beyond just informational self-determination.

For years, lawmakers have avoided the hard questions of whether privacy law should serve any goal beyond giving people control over their personal information and respecting their choices about their data. But informational capitalism is jeopardizing so much more than that, including our civil rights, intellectual self-development, mental well-being, life opportunities, relationships, capacity for self-governance, and even our environment. A myopic approach prioritizing individuals' (often illusory) choices obscures these larger, collective harms. An approach to data loyalty that required fealty only to individual choice would doom us to the same fate. Not only must any data loyalty framework explicitly exist alongside deeper, structural, collective changes imposed by public governance, but also any determination of people's "best interests" must include a consideration of the common good. Notice, choice, and consent regimes, and even more demanding individualistic, harm-based regimes are only peripherally concerned with systemic, collective harms, if at all. Zeynep Tufekci explains helpfully that "[d]ata privacy is not like a consumer good, where you click 'I accept' and all is well. [It] is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices."⁹³ People aren't

⁹³ Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES (Jan. 30, 2018), <https://www.nytimes.com>.

generally motivated to consider collective risks or risks to vulnerable groups that they are not a part of when giving consent to data practices, any more than people who might “choose not to wear a mask” as permitted by law during a pandemic might consider the public health consequences. Framing things in individual rights terms can cause us to miss the public and social consequences of our actions.⁹⁴

Along similar lines, a properly crafted duty of loyalty would also help free privacy law from its overly individualistic focus by protecting against systemic harms felt by entire groups, given the scale on which platforms operate.⁹⁵ One way to do this, while simultaneously resolving the problem of billions of possibly divergent “best interests,” is for lawmakers to specifically prioritize interests that are held collectively by groups of customers, with certain individually held interests holding sway only to the extent they do not conflict with collective user interests.⁹⁶ Thus, while there will inevitably be (as is often the case in law) hard cases at the margins, the claim that data loyalty conflicts with other duties is not just incorrect but also points to the surprising virtue that loyalty duties promote human values in all their complexity.

IV. LOYALTY CAN BE BOTH FLEXIBLE AND CLEAR

Of all the objections to a duty of loyalty for privacy law, the most frequent and prominent is that the duty is just too vague.⁹⁷ In a hearing on the future of transatlantic data flows called by the U.S. Senate Committee on Commerce, Science, and Transportation, Senator Wicker asked of a panelist who advocated for a duty of loyalty in privacy law, “Where is there a working duty of loyalty 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.]”⁹⁸ James Grimmelman also suggests

com/2018/01/30/opinion/strava-privacy.html.

⁹⁴ See RICHARDS, *supra* note 64, at 77–78; see also Evan Selinger & Woodrow Hartzog, *The Inconsistency of Facial Surveillance*, 66 LOY. L. REV. 33, 42 (2020) (exploring how individually-motivated “informed consent” regimes fail to adequately protect vulnerable and marginalized groups).

⁹⁵ See Julie E. Cohen, *Scaling Trust and Other Fictions*, *supra* note 5.

⁹⁶ Gold, *supra* note 90, at 385, 390, 398 (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”).

⁹⁷ Grimmelman, *supra* note 10.

⁹⁸ *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. (Dec. 9, 2020), <https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows> (statement of Sen. Wicker at 2:05:42–02:07:48). 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

that when applied to digital platforms, it becomes clear that “the rule against self-dealing is either absurdly under-inclusive, absurdly over-inclusive, or both.”⁹⁹ More generally, when the topic of data loyalty comes up even in casual conversation, people often express skepticism over a duty of loyalty because they view it as remarkably vague.¹⁰⁰

There are three different versions of this critique. First, if the duty is interpreted too broadly, it could prove unduly burdensome and costly to businesses.¹⁰¹ Second, the indeterminacy of a duty of loyalty creates room for companies to interpret their obligations in their weakest possible form, watering them down to mere compliance exercises with little protection for people and little hope for changing incentives for abuse.¹⁰² Third, if a duty of loyalty isn’t clarified, then companies might be left with no clue about what kinds of conduct are prohibited and what data practices and design choices are permissible.¹⁰³ Once again, this is a form of the Goldilocks Problem—it’s too hot, it’s too cold, or even if it’s just right, it’s still a bowl of mush.

We understand the impulses behind these arguments. Robust rules inevitably come with high compliance costs. Companies have a long history of exploiting the indeterminacy of privacy rules to their advantage and fighting for rules that allow for threadbare compliance without meaningful accountability.¹⁰⁴ They will undoubtedly try to do the same for a duty of loyalty. And courts have taken an interest in ensuring companies have proper notice of what is expected of them from privacy rules.¹⁰⁵ But we think all three concerns around vagueness can be meaningfully addressed with a properly articulated duty of loyalty.

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 Article. Also, thank you for reading so deeply in our paper—and its footnotes.

⁹⁹ Grimmelmann, *supra* note 10.

¹⁰⁰ See @JulesPolonetsky, TWITTER (Mar. 23, 2021, 11:30 PM), <https://twitter.com/JulesPolonetsky/status/1374564164568559616?s=20> (“Due to years of regulation, we know what fiduciary means in other sectors. Do we know what exactly what a browser fiduciary should do with ads/tracking? Block all ads, if user wishes or surveys of users support?”).

¹⁰¹ Richards & Hartzog, *supra* note 3 (manuscript at 63–64).

¹⁰² *Id.* at 64.

¹⁰³ *Id.* at 64–65.

¹⁰⁴ See Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. (manuscript at 18–19) (forthcoming 2022) [hereinafter Waldman, *Privacy*]; ARI EZRA WALDMAN, *INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER* (2021) [hereinafter WALDMAN, *INDUSTRY UNBOUND*].

¹⁰⁵ See *LabMD, Inc. v. Fed. Trade Comm’n*, 894 F.3d 1221, 1237 (11th Cir. 2018) (holding that an FTC cease and desist order was unenforceable because it “[did] not enjoin a specific act or practice” about how to accomplish an overhaul of a data security program); *Fed. Trade Comm’n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 255 (3d Cir. 2015) (concluding that the applicable FTC cybersecurity standard was precise enough to

This reveals a final surprising virtue of data loyalty: its flexibility, which is just like the flexibility of other standards-based frameworks like negligence, unfairness, Fourth Amendment reasonableness, and legitimate interests. Because of this flexibility, a duty of loyalty can be responsive to bigger structural power concerns and emergent problems driven by the affordances of new tools.¹⁰⁶ Data loyalty is not in opposition to robust public governance approaches; it can be a complement to public governance, serving as a catchall to keep things from falling through the cracks. As we discuss below, loyalty is typically implemented on two separate levels. The first, more general level is a broad duty applying to all interactions within an information relationship. The second, more specific level is through the articulation of detailed and substantive subsidiary rules. This second level targets particular contexts and actions that provide clear rules and less wiggle room, to ensure accountability and keep the frameworks from becoming watered down.

A. “*Best Interests*” Standard Clarified by Specific Rules

Of course, organizations will inevitably try to dilute the effectiveness of privacy rules. Ari Waldman has detailed the many different ways that organizations leverage the substance and structure of privacy law and the lawmaking process to lower the costs of regulation on their business model.¹⁰⁷ But a two-tiered duty of loyalty that features flexible general standards and context-specific rules would appear to be more resistant to sabotage and co-option than either specific rules or broad duties would be in isolation.¹⁰⁸ The layered structure of data loyalty, combined with the fact that loyalty is amenable to robust enforcement mechanisms like private causes of action and equity interventions like disgorgement, injunctions, and estoppel, make it more likely to have bite, as well as provide ample opportunities for broad standards to become refined, just like negligence has over time.

inform the relevant inquiry to be carried out by the company).

¹⁰⁶ Richards & Hartzog, *supra* note 3 (manuscript at 39) (discussing structural power concerns).

¹⁰⁷ See WALDMAN, *INDUSTRY UNBOUND*, *supra* note 104, at 99–160; Waldman, *Privacy*, *supra* note 104, at 12–33.

¹⁰⁸ Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, in *THE OXFORD HANDBOOK OF FIDUCIARY LAW* 419, 421 (Evan J. Criddle et al. eds., 2019) (“[B]y making use of an integrated mix of overlapping open-ended standards, more specific standards, and rules, fiduciary law improves upon the familiar trope of rules versus standards as competing governance strategies. . . . Fiduciary law’s combination of the primary duties of loyalty and care (open-ended standards) plus specific subsidiary duties (more specific standards and rules) provides the flexibility of standards plus the specification of rules while minimizing their respective disadvantages.”).

Over time, all standards creep towards rules, and a duty of loyalty for privacy law would be no different. Standards like the FTC's unfairness authority or the "reasonable expectation of privacy" component of the Fourth Amendment cover a wide range of possible behaviors but over time have come to target very specific kinds of behavior such as pretexting, dangerous data security practices, wiretapping, and other kinds of surreptitious surveillance.¹⁰⁹ A duty of loyalty in privacy law would require work and tending, but that is true of all meaningful legal principles. We also note in passing that the FTC's unfairness authority and the Fourth Amendment prohibition on unreasonable searches and seizures might be the two most important principles in U.S. privacy law—despite the fact that both are over a century old.

However, the virtues of standards do not obviate the need for clear subsidiary rules. A general standard like a prohibition on conflicted self-dealing can serve as a catchall, but clear rules are required to hold organizations accountable and make rules implementable. They can also single out particularly egregious examples of disloyal conduct to make them clearly prohibited, as the canons of legal ethics do in prohibiting commingling client funds, making business deals with clients, and even having sex with clients. All of these are disloyal, but our canons of ethics mark them out as forbidden just to be clear.¹¹⁰ We also emphatically agree with Julie Cohen's claim that "while problems of trust and market domination each undeniably contribute to the dysfunctions that surveillance-based business models create, responding adequately to those dysfunctions requires moving beyond reactive conceptions of data protection toward a governance model organized around problems of design, networked flow, and scale."¹¹¹ Cohen argued that a meaningful privacy framework should be "framed in terms of concrete requirements that must be satisfied by firms collecting, processing, and exchanging personal information."¹¹²

To clarify a duty of loyalty for privacy law, lawmakers should limit the duty to the extent of people's exposure and provide for the creation of specific subsidiary rules containing the concrete requirements called for by Cohen and others.¹¹³ In our previous work on trust, we have defined the concept of trust as the willingness to make oneself vulnerable to the actions of others.¹¹⁴ As a key

¹⁰⁹ Richards & Hartzog, *supra* note 3 (manuscript at 44, 64).

¹¹⁰ See Anthony E. Davis & Judith Grimaldi, *Sexual Confusion: Attorney-Client Sex and the Need for a Clear Ethical Rule*, 7 NOTRE DAME J.L. ETHICS & PUB. POL'Y 57 (1993).

¹¹¹ COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, *supra* note 5, at 13.

¹¹² *Id.*

¹¹³ See, e.g., *id.*; Waldman, *Privacy*, *supra* note 104.

¹¹⁴ Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV.

component of trust, our duty of loyalty would be properly limited to the extent of that vulnerability. To determine the extent of people's exposure, we must examine what is entrusted to companies that collect people's data: people's *data* and their *mediated experiences*. These concepts require a little explanation.¹¹⁵

When people expose themselves to organizations through modern, powerful digital technologies, they entrust more than just discrete pieces of information. It is not as simple as merely giving your phone number to the cashier at Best Buy. For such atomized transactions, we might simply hew to a purpose limitation rule and prohibit using the number for things like robocalls, spam marketing, or using your number as a universal ID through which to hand over all sorts of other information about you. Given the jaw-dropping quantity and quality of information that can be extracted through modern apps and websites, people expose their *narratives* and *identities* to those services. In the process, they can endanger their individual and collective well-being by empowering trusted parties and their "partners" to gain knowledge about them, judge them, make decisions affecting them, and exert power over them in ways that are contrary to their best interests. So, the relevant question for organizations bound by a duty of loyalty would be what the *affordances* are of the data entrusted to them.¹¹⁶ In other words, what actions do the data make significantly easier or harder? Data systems lower the cost of information storage, search, and delivery. This makes every choice to create data a moral act. Loyalty would demand that organizations refrain from acting upon an affordance of the data that conflicts with a reasonable trusting party's best interests.

Similarly, those entrusted with people's mediated experiences should look to the affordances of mediated technologies to determine the scope of their loyalty obligations. All of our experiences online are mediated by the company whose services we are using. That company chooses what we see, what we can click, and what we expose and determines how, when, and where that information is viewed. When people use a website or app, they are entrusting things of value to companies that can be easily taken advantage of, including

431, 433 (2016).

¹¹⁵ See 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, 89 (2019) ("So, the 'what' of fiduciary power extends to information derived from the underlying relationship. . . . '[R]elational knowledge'—special information that fiduciaries acquire about their beneficiaries—is key to the economic logic and the law supporting these relationships.").

¹¹⁶ For more information on affordances, see, for example, James J. Gibson, *The Theory of Affordances*, in PERCEIVING, ACTING, AND KNOWING: TOWARD AN ECOLOGICAL PSYCHOLOGY 67, 67–72, 76 (Robert Shaw & John Bransford eds., 1977).

their attention, their labor, and their time.¹¹⁷ While structures in the physical world are routinely leveraged against people in extractive and manipulative ways (like the placement of eggs in the back of the supermarket), modern platform designers have distinctly more power over people interacting in the digitally mediated environments they create.¹¹⁸ In pre-structured, mediated environments, there is no improvisation. You click the buttons and fill in the text boxes that you are given, or you get out. Mediated environments are astonishingly opaque because device screens have limited viewing space and there are no physical constraints limiting what happens behind the curtains. People cannot see all the options available, only what is presented, and they often do not understand how or why what is on their screen came to be there or that different people using the same service are seeing different things. Platforms have massive incentives to extract labor and data and the ability to change and optimize design on the fly to keep you engaged.

Ryan Calo argues that “society is only beginning to understand how vast asymmetries of information coupled with the unilateral power to design the legal and visual terms of the transaction could alter the consumer landscape.”¹¹⁹ Calo identifies three phenomena of what he calls “digital market manipulation,” all intimately related to data, that supercharged the potential for abuse in online markets: (1) the “mass production of bias” through big data, (2) the possibility of far greater consumer intelligence through “disclosure ratcheting,” and (3) the move from ends-based to means-based ad targeting and interface design.¹²⁰

Thus, when it comes to digital environments, it is not as simple as grocery stores putting the milk at the back of the building to force you to walk through the whole store, which will increase the odds of an impulse purchase. For such localized and static tactics, we might simply hew to the rule against unfair and deceptive trade practices to keep stores honest and people safe while allowing for optimized choice architecture, even if it is slightly extractive and slightly coercive. But modern platforms can use the affordances of digital tools to extract so much *data*, *attention*, and *labor* from people; these tools endanger people’s individual and collective well-being by empowering trusted parties to have complete control over what they see, what they can click, and what they can accomplish online. So, the relevant question for organizations bound by a duty of loyalty is what are the *affordances* of specific user interfaces? In other words,

¹¹⁷ See, e.g., ALICE MARWICK, THE PRIVATE IS POLITICAL: NETWORKED PRIVACY IN SOCIAL MEDIA (forthcoming) (including a discussion on the concept of “privacy work”).

¹¹⁸ HARTZOG, *supra* note 39; Calo, *supra* note 43, at 1006–07.

¹¹⁹ Calo, *supra* note 43, at 1006–07.

¹²⁰ *Id.*

what outcomes do specific design choices make significantly more or less likely? Design choices accomplish two things: they convey signals and make tasks easier or harder. Every technological design choice makes a certain reality more or less likely, which makes every design choice a moral act. Loyalty would demand that organizations refrain from design choices that foreseeably extract data, labor, or attention from trusting parties or prey on trusting parties' limited resources or cognition for coercive purposes that conflict with a trusting party's best interests.

Lawmakers could conceptualize the “best interests” of trusting parties in several different ways. Andrew Gold explains that when the law centers “best interests” around human well-being, “attending to someone’s best interests is not easily reducible to a simple formula.”¹²¹ He notes, “We can focus on how a person experiences her life, for example whether she is happy; we can focus on whether she has been able to satisfy her preferences, whatever those may be; or, we can focus on whether her life measures up well against some good or group of goods that is considered valuable.”¹²² Gold comments that “quite possibly, overall well-being involves some combination of success in each of these areas, and the key question is the difficult question of how to weigh the different components. Each individual theory has its proponents and detractors.”¹²³ While the general open-ended nature of what constitutes one’s best interest certainly must be addressed, the flexibility of this standard provides room for lawmakers to sufficiently tailor this duty to the contours of the relationship between people and the organizations they trust with their data and online experiences.

We recommend two ways to limit what constitutes a person’s “best interests” within the context of data loyalty. First, the “best interests” should be limited to the interests affected by the entrustment of data and attention, instead of an overall well-being standard. Organizations would be directed to ask which 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 used trusting parties location data to allow pharmaceutical companies to target them 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

¹²¹ Andrew S. Gold, *Purposive Loyalty*, 74 WASH. & LEE L. REV. 881, 899 (2017).

¹²² *Id.*

¹²³ *Id.* at 894–95.

isolated contexts make exploitation of vulnerable parties easier and compound incentives for companies to engineer exposure for financial gains.¹²⁴

Second, although a virtue of loyalty is that it does not demand a strict showing of harm (as we have seen, the violation is to the integrity of the relationship), when considering ways an action can be adverse to the interests of a trusting party, trustees should look to the foreseeable dangers of exposure.¹²⁵ A great place to start is the scholarly work identifying and explaining various kinds of privacy harms by Danielle Citron, Daniel Solove, Ryan Calo, and others.¹²⁶

Another key aspect of loyalty is that, in conjunction with a duty of care, it can animate a number of different broad subsidiary duties, such as duties of candor, good faith, nondelegation of key services, and confidentiality.¹²⁷ But, once again, 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. 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.”¹²⁸ He notes that “[b]y 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.”¹²⁹

This two-tiered approach allows lawmakers to tailor rules to specific relationships, allowing for the avoidance of specific foreseeable conduct while

¹²⁴ Ariel Fox Johnson, *Behavioral Ads Are Bad for Kids*, COMMON SENSE (May 10, 2021), <https://www.commonensemedia.org/kids-action/articles/behavioral-ads-are-bad-for-kids>.

¹²⁵ See, e.g., Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1097 (2019) (“In addition to expanding the notion of legally cognizable digital harms, an effective information fiduciary framework should expand the definition of what a privacy harm is.”).

¹²⁶ See, e.g., Citron & Solove, *supra* note 68, at 830–61 (breaking down privacy harms into physical, economic, reputational, and emotional harms, and describing issues of chilling effects, discrimination, thwarted expectations, control, data quality, informed choice, vulnerability, disturbance, and autonomy harms); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

¹²⁷ See Whitt, *supra* note 115, 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.”).

¹²⁸ Sitkoff, *supra* note 108, at 419.

¹²⁹ *Id.*

maintaining flexibility for new and changed rules in the future.¹³⁰ 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.

A look at duties of loyalty in other contexts can help shed some light on how such a duty might be conceptualized in privacy law. For example, a Massachusetts law laying out the duties of a guardian ad litem requires that a guardian “shall act at all times in the ward’s best interest and exercise reasonable care, diligence and prudence.”¹³¹ California law provides that “[t]he trustee has a duty to administer the trust solely in the interest of the beneficiaries.”¹³² A similar prohibition could be articulated for a duty of loyalty in positive terms (hypothetically, “a covered entity must act at all times in the trusting parties’ best interests regarding their data”) or in terms of a “no-conflict” rule (for example, “a covered entity shall be prohibited from taking any actions with respect to processing data or designing user interfaces that conflict with trusting parties’ best interests.”).

Enacting legislation should also either provide for subsidiary duties or delegate rulemaking authority to entities like the FTC for future subsidiary rules. Looking to the content of subsidiary duties in other contexts might be helpful for lawmakers enacting rules for data loyalty. In areas like agency law, the duty of loyalty has been built out with more specific subsidiary duties governing “self-dealing, material benefit, competition with the principal, and use of the principal’s property.”¹³³ In the law of trusts, subsidiary loyalty and care duties include administering the trust according to its terms but petitioning the court if doing so would harm the beneficiaries, collecting and protecting the trust property and keeping it separate from other properties, extensive record-keeping

¹³⁰ Sitkoff gives the prudent investor rule as an example of how subsidiary rules develop in trust law. *Id.* at 420–21 (“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 with the prudent investor rule to discern the application of a duty of care.”).

¹³¹ MASS. GEN. LAWS ch. 190B, § 5-209(a) (2010).

¹³² CAL. PROB. CODE § 16002 (West 2010).

¹³³ Sitkoff, *supra* note 108, at 429.

and disclosure requirements, duties to bring and defend claims to the trust, and a duty to be cost-sensitive in the administration of the trust.¹³⁴ In corporate law, subsidiary fiduciary duties address issues like the usurpation of corporate opportunity, management's role during contests for corporate control, actions that might impair the efficacy of shareholder voting or meetings, the need for internal monitoring and compliance, and requires to disclosure information to shareholders.¹³⁵ Nonprofit law includes subsidiary fiduciary obligations such as accounting for profits, rules against competition and usuring opportunities, prudent investment requirements, and rules against private inurement.¹³⁶ Bankruptcy, investment advice, and employment law impose similar subsidiary duties regarding accounting for property and profits, prudence, and non-competition.¹³⁷ For lawyers, as we have seen, subsidiary duties elaborate on the general duty of loyalty to address conflicts of interest, confidentiality, identification of and communication with clients, and familiarity with client affairs.¹³⁸ In health care, subsidiary fiduciary duties apply safeguarding client confidences, informed consent, and conflicts of interests.¹³⁹ Even public fiduciary law has built out the duty of loyalty with subsidiary obligations. The Emoluments Clauses of the U.S. Constitution are, in effect, loyalty rules, as are conflict of interest, disclosure, and antibias rules for judges and prohibitions under the Vienna Convention on Diplomatic Relations on diplomats to refrain from commercial activity abroad for personal profit.¹⁴⁰

For privacy law, subsidiary data loyalty rules might look like tailored versions of non-privacy fiduciary duties such as disclosure of material facts, consent, accounting for property (access and portability rights), confidentiality, and the full suite of the FIPS. This could apply some of the most significant obligations compelled by the GDPR. A duty of loyalty, combined with a duty of care, could help effectuate the most robust versions of existing data privacy rules—such as data minimization, purpose limitation, and legitimate basis for processing requirements—bound together and safeguarded by an anti-betrayal ethos.

Since deference to the data subjects' interests is also central to data protection regimes and rules requiring disclosure, and accounting and record-

¹³⁴ *Id.* at 430.

¹³⁵ *Id.*

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.* at 431–32.

keeping requirements are designed to hold trusted parties accountable for loyal behavior, a duty of loyalty would be an effective mechanism to animate the best of data protection frameworks. Loyal and careful organizations also do not take advantage of their superior position to lie to or harm those that trust them. So, heightened prohibitions against unfair and deceptive conduct would also make strong subsidiary duties.

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 have detailed in prior work, companies turning people's own cognitive and resource limitations against them to wrongfully extract data and labor is an endemic problem online.¹⁴¹ Subsidiary rules prohibiting abusive trade practices would prohibit trustees from materially interfering with the ability of trusting parties to understand the terms of the relationship and lower the risk associated with exposure and engagement. Rules against abuse would also prohibit trustees from taking unreasonable advantage of a trusting party's lack of understanding about the material risks, costs, or conditions of the service or the inability of trusting parties to protect their interests within the relationship. Finally, anti-abuse rules could prohibit trustees from taking unreasonable advantage of the reasonable reliance by trusting parties on an trustee's representation to act in the trusting party's 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 way for third party abuse and imposes more externalities than benefits for trusting parties) or affect recognition (the use of machines to read emotional states so as to enhance technology-based persuasion).¹⁴² Lawmakers could craft even more rules designed for specific parties, such as a rule that "social media platforms may not deploy affect recognition technologies on photos or videos submitted by trusting

¹⁴¹ Richards & Hartzog, *supra* note 114, at 470–71.

¹⁴² For an exploration of the dangers of affect recognition systems, see, e.g., KATE CRAWFORD, *ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE* 176–79 (2021); Kate Crawford, *Artificial Intelligence Is Misreading Human Emotion*, ATLANTIC (Apr. 27, 2021), <https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/>; Luke Stark & Jesse Hoey, *The Ethics of Emotion in Artificial Intelligence Systems*, in FACCT '21: PROCEEDINGS OF THE 2021 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 782, 787–88 (2021), <https://doi.org/10.1145/3442188.3445939>.

parties.” There might be disclosure mandates, process requirements, prohibitions on conduct, or obligated tasks. But fundamentally, each such rule should target specific areas where trusted parties have an incentive to engage in self-dealing.¹⁴³

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 could be meaningful complements or the next best thing to broad and strong relational obligations.¹⁴⁴ Many of these rules, such as generally applicable 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, as argued in Part I, that a duty of loyalty would act as an important animating force, interpretive guide, and catchall provision to bring more coherence, flexibility, and accountability through enforcement than these rules would as standalone laws.

Lawmakers also could create subsidiary rules built around wrongful gains by companies, as opposed to rules focused on harm to individuals.¹⁴⁵ This is because loyalty is about mitigating the lopsided power advantage certain trusted parties have that gives them both significant incentives and abilities for wrongful self-dealing. While the ultimate goal is to prevent outcomes adverse to the trusting party, the direct goal of a duty of loyalty is to preserve the integrity and reliability of relationships of trust by short-circuiting through law the ability of powerful parties to take wrongful advantage of their dominant position.

B. Five Areas for Subsidiary Data Loyalty Rules

Scholars and lawmakers have identified a number of different contexts where the incentives for self-dealing by the powerful party in an information relationship are overwhelming, making these contexts particularly suitable for subsidiary data loyalty rules.¹⁴⁶ In this section, we synthesize these contexts into

¹⁴³ See Gold, *supra* note 90, at 401 (“Different opportunism risks will then justify different loyalty content and approaches to legal decision-making.”).

¹⁴⁴ Richards & Hartzog, *supra* note 114, at 435–36.

¹⁴⁵ See, e.g., Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 659, 677–78 (2019) (arguing for restitution as the best fit for privacy infringement).

¹⁴⁶ See, e.g., Balkin, *Fiduciary Model of Privacy*, *supra* note 3, at 15 (“The nature of fiduciary obligations depends on . . . the potential dangers of abuse, manipulation, self-dealing, and overreaching by the more powerful party.”); Scholz, *supra* note 3, at 197; Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 17 (2018) (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 125, 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

five main areas to provide even more specificity to the kinds of subsidiary rules that could give protection to those contexts that are the ripest for abuse. First, trustees should be loyal when *collecting* information. Even in relationships of trust, data should only be collected when it is in the best interests of trusting parties. Second, trustees should be loyal when *personalizing* (i.e., treating people differently based upon personal information or characteristics). Third, trustees should be loyal when *gatekeeping*, avoiding conflicts when allowing government and other third-party access to trusting parties and their data. Fourth, trustees should be loyal when *influencing* trusting parties, such as when they leverage personal data and digital tools to exert sway over people to achieve particular results. Fifth and finally, trustees should be loyal when *mediating* interactions between their human customers, 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 an overlapping web of subsidiary loyalty rules to mitigate these kinds of disloyal behavior.

1. *Loyal Collection*

A duty of loyalty should begin 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.¹⁴⁷ Combined with the storage limitation principle, which holds that organizations should not keep data longer than needed 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.¹⁴⁸

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

threats that they face.”)

¹⁴⁷ *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 (last visited Apr. 26, 2022).

¹⁴⁸ *Id.*; David A. Zetoony, *Does the CCPA Require Data Minimization with Regard to the Collection and Use of Information?*, GREENBERGTRAURIG (Oct. 26, 2020), <https://www.gtlaw-dataprivacydish.com/2020/10/does-the-ccpa-require-data-minimization-with-regard-to-the-collection-and-use-of-information/>.

data protection frameworks that impose data minimization requirements, organizations must typically ensure that the data they are processing is adequate (sufficient to fulfill the stated purpose), relevant (has a relevant link to that purpose), and necessary (collecting and holding only that which is needed for that purpose). But there is a fair amount of uncertainty as to how to interpret these requirements. The U.K. Information Commissioner's Office explains that "[t]he UK GDPR does not define [what is adequate, relevant, and limited]. Clearly, though, this will depend on your specified purpose for collecting and using the personal data. It may also differ from one individual to another."¹⁴⁹ A duty of loyalty could provide a value-laden baseline that not only requires an examination of the purpose of the collection but also elevates the interests of those affected by the collection. It is likely that *more* data of specific kinds or in specific contexts might be collected within trusted relationships than would otherwise be acceptable for parties outside of information relationships, but this collection should come with much stricter obligations. Of course, loyal collection also means that trusted parties must often refrain from collecting entire kinds of information. While parties at arm's length might act opportunistically in collecting as much data as possible, trusted parties remain loyal by leaving all data that does not serve trusting parties' best interests on the table. Moreover, to the extent that we might be concerned about the later stages of Zuboff's theory of surveillance capitalism, in which data are collected to predict and persuade, a robust regime of loyal collection would ensure that we remain only at the first stage, in which data are collected to improve the quality of service in the loyal customer's interest.¹⁵⁰

2. *Loyal Personalization*

The modern Internet routinely and systemically treats people differently based upon their personal information or characteristics. Targeted and behavioral advertising are the most infamous examples of this, but first-party product and streaming recommendations, news feeds, default settings, layouts, and more are all designed to automatically look and act differently based on a person's personal characteristics. Some of this personalization, such as targeted recommendations for networked connections based upon intentionally revealed data (for example, 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

¹⁴⁹ *Data Minimisation*, *supra* note 147.

¹⁵⁰ See Richards & Hartzog, *supra* note 3 (manuscript at 13).

interests. Ariel Dobkin argues in favor of antidiscrimination rules for those bound by duties of loyalty and care, which would prohibit companies in information relationships from “discriminating between or against users based on characteristics like race or gender.”¹⁵¹ Dobkin adds that “[t]he set of data points available to companies often includes these qualities and many others. There are three main methods by which a company might discriminate based on these characteristics: (1) access to services, (2) prices, and (3) digital redlining.”¹⁵²

Some fear that rules requiring loyal personalization might jeopardize the entire enterprise of targeted and behavioral advertising. However, such fears are overblown. Balkin responds to this concern: “This conclusion does not follow unless we assume that all targeted advertising is inherently abusive and inconsistent with the best interests of end users. Since much of modern advertising is based on increasing efficiencies in locating and reaching interested audiences, this would be a very surprising conclusion.”¹⁵³ Instead, Balkin argues, “[W]e should ask what practices of advertising, targeted at end users, do not betray their trust or operate against their interests. Only this kind of targeted advertising should be permitted.”¹⁵⁴

We agree with Balkin and would save the existential debate around targeted advertising for a different day. Our point here is merely to emphasize that subsidiary rules built around the concept of loyal personalization could firmly and clearly address a systemic problem that traditional data protection frameworks have been unable to solve.

3. *Loyal Gatekeeping*

Entrustees have a remarkable ability to give third parties 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 governments demand evidence for investigations, trials, and intelligence. Entrustees have financial incentives to build portals and facilitate

¹⁵¹ Dobkin, *supra* note 146, at 26.

¹⁵² *Id.*

¹⁵³ Balkin, *The Fiduciary Model of Privacy*, *supra* note 3, at 27.

¹⁵⁴ *Id.* at 28 (“A rule that allowed only contextual targeted advertising but not behavioral advertising would, at a stroke, transform the landscape of surveillance capitalism, but it would still allow targeted ads How companies engage in behavioral advertising depends on background legal restrictions on collection and use.”).

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 does not significantly turn 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 often the 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 them bypass encryption protections, and Cambridge Analytica's massive Facebook data exfiltration—all involved gatekeeping issues.¹⁵⁵ Facebook's system for facilitating third-party applications' access to their customer base was a clear example of making collective user interests subservient to growth metrics, as the company touted to its human customers the virtues of being able to control their audiences while obscuring the true risk of exposure and the steps needed to limit it.¹⁵⁶ Similarly, although companies typically have little choice in respecting legal process compelling customer data, a duty of loyalty would justify rules that mandated additional process for certain kinds of relationships.¹⁵⁷ Kiel Brennan-Marquez argues the following:

Fourth Amendment doctrine must abandon the pretense that all private actors are alike. The implication of *A*'s decision to share information with *B* should not be uniform across contexts. Rather, it should depend on what *type* of "third party" *B* is, on *B*'s role in the world vis-à-vis *A*. In many settings, it is perfectly acceptable—indeed, it serves an important public function—for *B* to help investigate *A*'s illicit activity.

¹⁵⁵ Kennedy Elliott & Terri Rugar, *Six Months of Revelations on NSA*, WASH. POST (June 5-6, 2013), <https://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/m/>; *The Cambridge Analytica Files*, GUARDIAN, <https://www.theguardian.com/news/series/cambridge-analytica-files> (last visited Apr. 26, 2022); Arjun Kharpal, *Apple v. FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM); <https://www.cnn.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html>.

¹⁵⁶ *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

¹⁵⁷ See, e.g., Balkin, *The Fiduciary Model of Privacy*, *supra* note 3, at 19 ("Under the fiduciary model, the question is not whether consumers reasonably expect that a particular type of data will be kept private. Rather, the question is whether the relationship between end users and digital companies is a fiduciary relationship of trust. If so, then the question becomes whether the digital business can freely disclose this information to others consistent with their fiduciary obligations. If not, then the government needs to obtain a warrant. The fiduciary model helps preserve our security from the government as we hand over more and more information about ourselves to digital businesses.").

But there is also an important class of cases in which *B* is not a run-of-the-mill private actor, but rather an information fiduciary, beholden to *A*'s interests first and foremost.¹⁵⁸

In these ways, a duty of loyal gatekeeping could help reduce the exposure of customers to third parties who would almost certainly not have their best interests at heart. And a requirement that a loyal entrustee make sure that the trusting party is protected from third-party access in the entrustee's control would be both well within the heartland of a duty of loyalty and also important enough to safeguard through subsidiary rules.

4. *Loyal Influencing*

Technologies are artifacts built to act upon the world. Every conscious design decision made in the creation of a website or app is meant to facilitate a particular kind of behavior.¹⁵⁹ In addressing the ethics of "nudging," Cass Sunstein explains the following:

When people make decisions, they do so against a background consisting of choice architecture. A cafeteria has a design, and the design will affect what people choose [to eat]. The same is true of websites. Department stores have architectures, and they can be designed so as to promote or discourage certain choices by shoppers (such as leaving without making a purchase).¹⁶⁰

The structure of digital technologies affects people's choices even if the effect is not intended by designers. When designers create drop-down menus, privacy settings, "I agree" buttons, and other features that implicate privacy, they influence people's behavior. They can't avoid it.¹⁶¹ Given their power, interface designers and other choice architects should be loyal in exercising their influence.

The most prominent example of disloyal influence involves organizations leveraging "dark patterns" or "malicious interfaces," which are user interface elements meant to influence a person's behavior against their intentions or best

¹⁵⁸ Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 616 (2015).

¹⁵⁹ Cf. LANGDON WINNER, *THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF TECHNOLOGY* 124 (1986) (explaining the politics of artifacts).

¹⁶⁰ Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. REGUL. 413, 417 (2015).

¹⁶¹ *Id.* at 421 ("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.").

interests.¹⁶² Companies deploy “effort traps” to make deleting an account confusing and difficult. They make “cancel” buttons hard to see and press, obscure important details in tiny fonts or walls of boilerplate, and 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. (“Are you sure you want to delete and miss valuable offers? Your friends will also be so sad to see you go!”)

Jamie Luguri and Lior Strahilevitz recently published some of the first comparative evidence quantifying the effectiveness of dark patterns. The scholars explain that “dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces.”¹⁶³ 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, . . . and aggressive dark patterns nearly quadrupled the percentage of consumers signing up. In social science terms, the magnitudes of these treatment effects are enormous.”¹⁶⁴

¹⁶² See, e.g., HARTZOG, *supra* note 39, at 161; Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 44 (2021); Calo, *Digital Market Manipulation*, *supra* note 43, at 1005–06; Gregory Conti & Edward Sobiesk, *Malicious Interfaces and Personalization’s Uninviting Future*, IEEE SEC. & PRIV., May–June 2009, at 72–73, <http://www.rumint.org/gregconti/publications/j3pri.pdf>; Johanna Gunawan, David Choffnes, Woodrow Hartzog & Christo Wilson, *Towards an Understanding of Dark Patterns Privacy Harms*, in CHI WORKSHOP, WHAT CAN CHI DO ABOUT DARK PATTERNS? 1, 1 (2021), <https://darkpatternsindesign.com/position-papers/>; 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/>; Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, in PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 1, 1, 8–9 (2018), <http://dl.acm.org/citation.cfm?doi=3173574.3174108>; 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 PROC. ACM HUM-COMPUT. INTERACTIONS 1, 4 (2019); Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern . . . Dark? Design Attributes, Normative Considerations, and Measurement Methods*, in PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, *supra*, at 1, 13, <http://arxiv.org/abs/2101.04843>; 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, 248–49 (2016); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the “Privacy Paradox,”* 31 CURRENT OP. PSYCH. 105, 105, 107–08 (2020).

¹⁶³ Luguri & Strahilevitz, *supra* note 162, at 46 (emphasis omitted).

¹⁶⁴ *Id.* They add, “We 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.” *Id.* at 47.

These findings have important implications for lawmakers considering subsidiary rules for dark patterns, particularly for a duty of loyalty. Luguri and Strahilevitz found evidence that the robustness of dark patterns matters in a powerfully counterintuitive way. As they explain, “aggressive dark patterns generate a powerful customer backlash whereas mild dark patterns usually do not. Therefore, counterintuitively, the strongest case for regulation and other legal interventions concern subtle uses of dark patterns.”¹⁶⁵ (This also, incidentally, explains why Target’s subtle hiding of habit-inducing baby formula coupons in marketing to women it knew to be pregnant to avoid tipping them off was both effective and problematic.¹⁶⁶) Legal remedies that require demonstrable injury, such as duties of care and prohibitions on unfair trade practices, will likely struggle to redress the more subtle forms of manipulation that Luguri and Strahilevitz highlighted as the most dangerous and profitable for companies. Lawmakers, after all, have struggled for years to articulate when attempts at persuasion become harmful.¹⁶⁷

But trusting parties do not need to be injured for trustees to violate a duty of loyalty. Subsidiary rules around disloyal attempts to influence would address the most pernicious and dangerous dark patterns head-on.¹⁶⁸ Lawmakers should focus on how the design (plus data science plus behavioral science) is meant to take advantage of a person’s limitations or vulnerabilities to benefit the designer in a way that is against the trusting party’s best interests.¹⁶⁹

¹⁶⁵ *Id.* at 46–47.

¹⁶⁶ See *supra* notes 63–64 and accompanying text.

¹⁶⁷ See Luguri & Strahilevitz, *supra* note 162, at 99–102 (analyzing constitutional issues presented by dark pattern regulation); 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.”).

¹⁶⁸ 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 162, at 99.

¹⁶⁹ 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, *Fixing Social Media’s Grand Bargain* 4 (Hoover Working Grp. on Nat’l Sec., Tech., & L., Aegis Series Paper No. 1814, 2018), https://www.hoover.org/sites/default/files/research/docs/balkin_webready.pdf.

5. *Loyal Mediation*

Certain kinds of organizations design their platforms so that their customers interact not just with the organization itself but also with each other. In other words, they mediate people's social and market experiences with other people using their service. Often, the interests of the platforms and their customers do not diverge regarding how their experiences with each other are mediated. Some people want to share pictures of their dogs on Instagram while some people want to see pictures of other people's dogs, and Instagram has the incentive to make this possible so everyone can be happy sharing and viewing each other's dogs (or, not).

But things can go off the rails quickly if 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 alleged 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 strategic roadblocks that make it difficult to report harmful speech and hide from other users—leads to acute individual harms like harassment 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 people.¹⁷⁰

A duty of loyalty cannot solve all 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.¹⁷¹ They are disloyal when they exert this power to optimize growth in ways that conflict with the best interests of their customers. 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 others are 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 and firm's obligations.

¹⁷⁰ See, e.g., DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 83–85 (2014) (explaining that individuals who share the virtual harm they are receiving with law enforcement typically do not receive much assistance).

¹⁷¹ See, e.g., *id.* at 66–68; HARTZOG, *supra* note 39, at 161–62.

CONCLUSION

If, at this point, you are thinking that the conception of loyalty we have articulated in this paper sounds quite different from traditional duties of loyalty, you would be right. Traditional fiduciary models are ill-equipped to simply be dropped onto online platforms. In her book *Between Truth and Power*, Julie Cohen argues that legal changes that “simply adopt yesterday’s methods are unlikely to succeed. Just as the most effective institutional changes of a previous era engaged directly with the logistics of commodification and marketization, so institutional changes for the current era will need to engage directly with the logistics of dematerialization, datafication, and platformization.”¹⁷² The critics of a duty of loyalty have correctly identified that the power of modern platforms is unprecedented and will require multiple new approaches to disrupt it.

But the critiques that focus on the affordances and tools used by these organizations also reveal a number of surprising virtues of data loyalty, including its core, fundamental purpose: to limit the ability of one party in a relationship to exploit the massive power advantage they have over the other for self-gain. In this Article, we have tried to highlight those virtues to plot a new vision for data loyalty, one that looks beyond individualistic approaches to privacy to remedy systemic problems of power in relationships. This new vision works to reinforce public governance efforts rather than serve as an alternative to them. And it is capable of inspiring a public tired of being betrayed and commodified to demand rules that compel loyal behavior and put their interests first. Relational rules like data loyalty will not be sufficient, but they will be necessary to mitigate the vulnerabilities within the information relationships that will continue to be a part of our daily lives for the foreseeable future. Loyalty, it turns out, can be a powerful state of mind for reenergizing privacy reform; it embraces privacy’s relational turn, prioritizes human values, and offers solutions that are flexible and clear, rather than vague and indeterminate. And while loyalty, to be sure, will be only one piece of the puzzle of making the best of our information revolution, it may just be the key piece that makes all the others work.

¹⁷² COHEN, *supra* note 4, at 270.