A DUTY OF LOYALTY FOR PRIVACY LAW

NEIL RICHARDS[*] & WOODROW HARTZOG[**]

ABSTRACT

Data privacy law fails to stop companies from engaging in self-serving, opportunistic behavior at the expense of those who trust them with their data. This is a problem. Modern tech companies are so entrenched in our lives and have so much control over what we see and click that the self-dealing exploitation of people has become a major element of the internet's business model.

Academics and policymakers have recently proposed a possible solution: require those entrusted with people's data and online experiences to be loyal to those who trust them. But many have concerns about a duty of loyalty. What, exactly, would such a duty of loyalty require? What are the goals and limits of such a duty? Should loyalty mean obedience or a pledge to make decisions in people's best interests? What would the substance of the rules implementing the duty look like? And what would its limits be?

This Article suggests a duty of loyalty for personal information that answers these objections and represents a promising way forward for privacy law. We offer a theory of loyalty based upon the risks of digital opportunism in information relationships that draws upon existing—and in some cases ancient—precedent in other areas of American law. Data collectors bound by this duty of loyalty would be obligated to act in the best interests of people exposing their data and online experiences, up to the extent of their exposure. They would be prohibited from designing digital tools and processing data in a way that conflicts with trusting parties' best interests. We explain how such a duty could be used to set rebuttable presumptions of disloyal activity and to act as an interpretive guide for other duties. And we answer a series of objections to our proposed duty, including that it would be vague, be too narrow, entrench surveillance

* Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis.

** Professor of Law and Computer Science, Northeastern University. Thanks to Jack Balkin, Matt Bodie, Ryan Calo, Danielle Citron, Julie Cohen, Bob Gellman, Sue Glueck, Claudia Haupt, Cameron Kerry, Jesse Lieberfeld, Jon Penney, David Pozen, Andrew Tuch, Salome Viljoen, Ari Waldman, Rebecca Wexler, Tal Zarsky, Jonathan Zittrain, and the participants at the 2020 Privacy Law Scholars Conference at the George Washington University School of Law and law faculty workshops at Northeastern University and Washington University. Thanks also to Alissamariah Gutierrez, Alexis Johnson, Hannah McDonnell, and Alex Nally for their research assistance.

capitalism, create a problem of conflicting duties, and spell the end of surveillance-based "targeted advertising." The duty of loyalty we envision would certainly be a revolution in data privacy law. But that is exactly what is needed to break the cycle of self-dealing and manipulation ingrained in both the current internet and our society as a whole. This Article offers one pathway for us to get there.

TABLE OF CONTENTS

INTRODUCTION

It wasn't supposed to be like this. When the internet emerged in the mid-1990s, it was heralded as an unprecedented technology of human empowerment, creating a place where human beings could meet, learn, and

express themselves, transforming our society for the better.[1] It was also hailed as a realm of privacy, in which those empowered humans could read, connect, and communicate on their own terms, safely cocooned in bubbles of anonymity where, as the famous *New Yorker* cartoon put it, "no one knows you are a dog."[2]

Of course, a quarter of a century on, it hasn't quite worked out that way. The internet of the 2020s certainly provides many helpful services, but it has also become the greatest assemblage of corporate and government surveillance in human history. The internet allows unprecedented expression, but it is also plagued by hate speech, misinformation, and electoral manipulation. And where the internet promised human empowerment, all too often the tools of data science and behavioral science have been used to nudge behavior and to manufacture consent to boilerplate terms that no one reads. Far too frequently, corporate promises of empowerment have instead delivered manipulation, disempowerment, and distrust.[3]

This paper offers and examines one potential solution to some of these problems: imposing a duty of loyalty on companies that collect and process human information. Duties of loyalty are used in other areas of law as obligations to refrain from self-dealing. They are typically placed on trusted parties such as lawyers and other professionals, agents, guardians, and corporate directors.[4] But they have not yet been imposed as part of privacy law. In articles in 2016 and 2017, we suggested that loyalty is the key component in generating trust in modern "information relationships," ones in which human information changes hands, often as part of the delivery of a service such as search engine results.[5] Other scholars have proposed

1. *See generally* FRED TURNER, FROM COUNTERCULTURE TO CYBERCULTURE (2006).

2. *See* Michael Canva, *'NOBODY KNOWS YOU'RE A DOG': As Iconic Internet Cartoon Turns 20, Creator Peter Steiner Knows the Joke Rings as Relevant as Ever*, WASH. POST (July 31, 2013), https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html [https://perma.cc/GE7T-P2A4].

3. *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 89 (2019); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012); YOCHAI BENKLER, ROBERT FARIS & HAL ROBERTS, NETWORK PROPAGANDA (2018); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

4. *See generally* The OXFORD HANDBOOK OF FIDUCIARY LAW 796 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) [hereinafter THE OXFORD HANDBOOK].

5. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 451–56 (2016) [hereinafter *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1185 (2017) [hereinafter *Privacy's Trust Gap*].

treating data collectors as "information fiduciaries."[6] This academic work has influenced lawmakers to the extent that a duty of loyalty has now become a serious option for national privacy reform. Leading federal privacy bills pending before Congress from both parties include proposed duties of loyalty, though they vary significantly in scope, specificity, and justification.[7]

All this work is both promising and important, but it fails to answer one critical question: what, exactly, would a duty of loyalty in privacy law require from those entrusted with our personal information? This is a

6. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/AF89-PM2M]; *Taking Trust Seriously*, *supra* note 5, at 457; *Privacy's Trust Gap*, *supra* note 5, at 1198; Woodrow Hartzog & Neil Richards, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579, 582 (2017); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 8 (2018); Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 591 (2015); Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RSRV. U. L. REV. 193, 193 (2016); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 113 (2019); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 339–40 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1058 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 1 (2018); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/2V6T-DPDY]; Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 446 (2001); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102–04 (2006); Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75, 75 (2019); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 611–12 (2015); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, J. CORP. L. 144, 144 (2020). *But see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 498 (2019).

7. *See* Data Care Act of 2019, S. 2961, 116th Cong. § 3(b)(2) (2019) ("Duty of Loyalty.—An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B)(i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user."); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 101 (2019) ("Duty of Loyalty: (a) In General.—A covered entity shall not—(1) engage in a deceptive data practice or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act"); New York Privacy Act, S. 5642, Reg. Sess. (N.Y. 2019) ("Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances."); SAFE DATA Act, S. 4626, 116th Cong. tit. II (including a host of loyalty-like specific protections, including provisions for algorithmic bias detection, data broker registration, filter bubble transparency, and, critically, abusive trade practices stemming from manipulative interface design).

crucially important question because without a sense of what a duty of loyalty would require, it will be impossible to evaluate whether one is a good idea, much less to implement a duty of loyalty in privacy law. To date, no scholarship has sufficiently answered this question—a question with challenging descriptive and normative dimensions. Thus, any account of a duty of loyalty must offer *normative reasons* for having the duty in the first place, specifying the values served by imposing such a duty of loyalty on companies in the context of what we have elsewhere called "information relationships."[8]

Lawmakers imposing a duty of loyalty must also make a separate normative decision about how robust these rules should be. Traditional fiduciary duties can be very demanding. Duties of this kind would offer maximum protection to data subjects in information relationships. But they could also make a company's ability to collect and use that data quite costly, particularly at scale. It is possible to imagine other kinds of loyalty duties that are simultaneously substantial but also less demanding than a full fiduciary obligation. This raises the question of whether robust fiduciary duties should apply to all data collectors or only the most powerful ones. How might the duty of loyalty be crafted to balance the well-being of people and the benefits of safe and sustainable information exchanges?

A satisfying account of duty of loyalty must also *describe the boundaries* of what the duty covers. For descriptive help, some lessons can be drawn from both the existing law of fiduciaries and the other relationships of trust that compel a duty of loyalty. But the relationship between people and their doctors, guardians, and financial advisors is quite different from the relationships between people and Facebook, Google, and TikTok.[9]

In this Article, we propose a duty of loyalty for privacy law that answers each of these normative and descriptive questions. We offer a theory based on the risks of opportunism that arise when people trust others with their personal information and online experiences. Put simply, under our approach, loyalty would manifest itself primarily as a prohibition on designing digital tools and processing data in a way that conflicts with a trusting party's best interests. Data collectors bound by such a duty of loyalty would be obligated to act in the best interests of the people exposing their data and engaging in online experiences, but only to the extent of their exposure.

Our basic claim is simple: a duty of loyalty framed in terms of the best interests of digital consumers is coherent and desirable and should become

8. For example, like those between technology companies such as social networks, cloud providers, and platforms. *See Taking Trust Seriously*, *supra* note 5, at 433.

9. Khan & Pozen, *supra* note 6, at 498; *see also* Claudia Haupt, *Platforms As Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 35 (2020).

a basic element of U.S. data privacy law. Such a duty of loyalty would compel loyal acts and also constrain conflicted, self-dealing behavior by companies. It would shift the default legal presumptions surrounding a number of common design and data processing practices. It would also act as an interpretive guide for government actors and data collectors to resolve ambiguities inherent in other privacy rules. A duty of loyalty, in effect, would enliven almost the entire patchwork of U.S. data privacy laws. And it would do it in a way that is consistent with U.S. free expression goals and other civil liberties. A duty of loyalty along the lines we suggest might seem like a radical step for American privacy law, but we think it would be a necessary and important one if our digital transformation is to live up to its great but unfulfilled promises of human well-being and flourishing.

Our Article proceeds in five parts. Part I briefly describes the problem. We explain how the failures of American privacy law have enabled corporate opportunism and manipulation of consumers using human information. This has been a particular problem in the context of "personalized" technologies that promise to know us so that they can better satisfy our needs and wants. Insufficiently constrained by the law, companies can deploy a potent cocktail of techniques derived from cognitive and behavioral science to "nudge" or otherwise influence the choices we make. But these highly capitalized tech companies have not acted like the benevolent "choice architects"[10] some had hoped they might become. Technologies—and choice architecture—advertised as serving consumers have instead become weaponized, serving commodified consumers up to the companies and their commercial and political advertiser clients.

Part II justifies a duty of loyalty for privacy law. We explain how and why the existing American framework regulating trafficking in human information fails to comprehend—much less effectively regulate—the problems of profiling, sorting, nudging, and manipulation that plague the digital environment. Put simply, a legal model grounded in "notice and choice" cannot prevent data-based manipulation when notice is fictional, when choice can be manufactured by the tools of data and behavioral science, and when rules for individuals are used to regulate a problem with social dimensions. Part III offers a theory with which to understand and solve these problems: a duty of loyalty for data collectors. Duties of loyalty in American Law have typically taken one of two forms. When there is a relatively sophisticated trusting party who can communicate their wants and desires with an expert counselor, loyalty means *obedience*. Obedience

10. RICHARD THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008) (coining the phrase and advocating for it).

typically means follow the instructions of the trusting party, regardless of the likely consequences. Lawyers, doctors, and financial managers are good examples of this kind of duty of loyalty. Lawyers, for example, advise their clients but they are ultimately required to follow their clients' wishes, even when those clients are making what objectively appear to be mistakes. In other cases, however, where trusting parties are more vulnerable, or their instructions are harder to discern, loyalty means promoting the *best interests* of the vulnerable trusting party. Thus, the trustee of a teenage orphan or young adult can disregard the young person's wishes to spend trust money on sports cars and sneakers in favor of investing the money in housing or education. Each approach has its virtues and vices, but given the nature of the digital landscape, the relative unsophistication of most digital consumers, and the technical, legal, and economic power differentials between consumers and platforms, we suggest that the "best interests" form of loyalty is best suited to protect digital consumers. The best-interests approach would have the additional benefit of ridding trusting consumers of the burdens of privacy self-management and other "privacy work."[11] Part III also builds out the substance of what a best-interests duty of loyalty might entail. The core mandate of such a duty would be a prohibition on designing technologies and processing data that conflicts with the trusting parties' best interests, up to the limits of the relationship between the parties. We also explain how the duty of loyalty can be manifested in three different ways: as rules governing behavior, as default presumptions against particular potentially harmful actions, and as an interpretive guide for other duties.

Part IV tackles the problem of practical implementation. We explain how and why a properly crafted duty of loyalty can do important work toward mitigating opportunism, filling critical gaps in the United States' regulation of tech companies, and emboldening a relational approach to privacy law. First, we explore *when* a duty of loyalty should arise. We argue that it should apply when three factors are met: (1) when trust is invited within the context of an information relationship; (2) by one with control over the disadvantaged party's mediated experiences and data; and (3) the weaker party exposes their vulnerabilities, trusting they will not be harmed. Second, we explore possible frameworks for such a duty of loyalty, including a general duty of loyalty for all activities of certain large and powerful data processors, some context-specific ad hoc duties of loyalty, and specific rules to encourage loyal behavior in practice.

11. *See* ALICE MARWICK, THE PRIVATE IS POLITICAL: NETWORKED PRIVACY AND MARGINALIZATION (forthcoming); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013).

In Part V, we anticipate and confront a series of objections to our proposed duty, including that it would be vague, be too narrow, entrench surveillance capitalism, create a problem of conflicting duties, and spell the end of surveillance-based "targeted advertising." While we note that these objections are certainly worth addressing head-on in law and policy, we draw inspiration from how the law has handled similar objections in related areas to deal with these issues.

I. CORPORATE DATA OPPORTUNISM

Trust is the key to modern social, economic, and political life, but it is nearly impossible without loyalty. As we have argued in prior work, the essence of trust is the willingness to accept vulnerability to the actions of others.[12] Such exposure is necessary to participate in a digital networked society in which our finances; our communications; our secrets; and indeed our personal, social, economic, and political lives are mediated by entities that we have no real choice but to expose ourselves to. But while these relationships have become essential to basic participation in our society, they raise the spectre of betrayal based upon misplaced trust. How then, can we resolve the paradox of practically needing to trust but also rationally fearing to trust?

Loyalty is the key to enabling meaningful trust; it allows the trusting party to live their life without worrying that the trusted party will take advantage of their exposed vulnerabilities.[13] It allows the people in our society to trust their lawyers and search engines, their taxi and Lyft drivers, and their airlines and newspapers. Loyalty allows human social and economic relationships to flourish because it is about building the conditions necessary for exposure and reliance. As such, it is about much more than merely avoiding harm. Loyalty thus has a moral dimension as well as a purely utilitarian one. James Penner has explained that "[t]o wrong is bad, but to wrong someone by taking advantage of their vulnerability, a vulnerability you were entrusted to protect, is worse."[14] This moral justification is the heart of the reason we should consider loyalty obligations for companies we entrust with our data and our online experiences. At base, loyalty is about preventing opportunistic behavior, which is both harmful from a utilitarian perspective *and* wrong from a moral one. Tech companies have many opportunities to exploit the human information with which they

12. *Taking Trust Seriously*, *supra* note 5, at 433; *Privacy's Trust Gap*, *supra* note 5, at 1213.
13. *Privacy's Trust Gap*, *supra* note 5, at 1213.
14. James Penner, *Fiduciary Law and Moral Norms*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 781, 796.

are entrusted. And some have run amok with it, using data received by trusting customers to sort, nudge, and even manipulate them.[15]

American privacy law has failed to address the problem of information-based exploitation of consumers. For decades, its dominant approach to regulating human information has been one of "notice and choice."[16] Under this regime, companies are largely free to exploit human information as long as they disclose their intentions somewhere in a privacy "notice" and give consumers some "choice" about whether they wish to share their data.[17] We will have more to say about this part of the law below in Part II, but it suffices to note here that privacy law does not place substantive duties such as loyalty on companies that collect or exploit human information. This allows companies to invite consumers to trust them with one hand, while the companies insist that there is an arms-length transaction to regulators with the other.[18] What is more, there are substantial market and profit incentives to exploit human information; indeed, for most venture-funded and all publicly traded companies, these goals may be mandated by contract and corporate law.[19]

In short, companies are currently engaging in self-serving exploitative behavior that has yet to be appreciated by the general public, and that behavior is being encouraged by both the law and the market. This Part briefly lays out three distinct kinds of this self-serving exploitation of humans and their information: (1) profiling and sorting, (2) nudging, and (3) manipulation. It does so to survey the gap that we think a duty of loyalty for data collectors might fill.

A. Profiling and Sorting

Scholars across the disciplines of law, sociology, science and technology studies, surveillance studies, and history have extensively documented the ways that companies and governments use human information to profile and sort humans. Historian Sarah Igo has carefully illustrated how privacy disputes throughout modern American history have usually been struggles over the social, economic, and political power that human information

15. For a deeper exploration into the corrosive effect of the platform business models of "informational capitalism," see COHEN, *supra* note 3, at 89.

16. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1691 (2020).

17. *Id.*

18. *See generally* RADIN, *supra* note 3; NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS (2013).

19. Jennifer Cobbe & Elettra Bietti, *Rethinking Digital Platforms for the Post-COVID-19 Era*, CTR. FOR INT'L GOVERNANCE INNOVATION (May 12, 2020), https://www.cigionline.org/articles/rethinking-digital-platforms-post-covid-19-era [https://perma.cc/36MA-KFAP].

confers.[20] *The Panoptic Sort*, sociologist Oscar Gandy's classic sociological study of consumer profiling from the early 1990s, similarly showed how companies well before the internet were eagerly seeking human information to identify potential marketing targets.[21] Gandy explained that companies used panoptic surveillance techniques to discriminate between customers to identify "high-quality targets of opportunity."[22] A quarter of a century on, Surveillance Studies pioneer David Lyon explained how the use of advanced techniques of consumer sorting demonstrated how human information had become central to the development and reproduction of economic power.[23] For corporations, the internet represented yet another marketplace, one in which they could deploy and refine their techniques of consumer profiling. This commercial surveillance had become so deeply instantiated in the commercial internet that Lyon noted, "younger readers may have to be persuaded that there was once a time when no advertising appeared on the Internet!"[24] Legal scholar Daniel Solove has described how early internet databases were deployed to create a "digital person," which was profiled and sorted into categories, for more efficient deployment of market power in the form of targeted advertising.[25] Some of these surveillance-based sorting categories exploited obvious vulnerabilities in disturbing ways, such as marketing to rape survivors, emotionally-disturbed teenagers, or the parents of deceased children.[26] Such cases are appropriately shocking, but the mere act of *classification* to more effectively drive purchasing habits is itself an exploitation of data-derived vulnerabilities.

As technology and business practices advanced into the digital sphere, companies began to realize that the internet could become so much more

---

20. SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 368 (2018).

21. OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993).

22. Oscar H. Gandy, Jr., *Coming to Terms with the Panoptic Sort*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 132, 151–52 (D. Lyon & E. Zureik eds., 1996).

23. DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 42 (2007).

24. *Id.*

25. SOLOVE, *supra* note 6, at 1–2.

26. *E.g.*, *What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 113th Cong. (2013) (statement of Pamela Dixon, Executive Director, World Privacy Forum), https://www.commerce.senate.gov/services/files/E290BD4E-66E4-42AD-94C5-FCD4F9987781[https://perma.cc/QDP8-7BNW] (rape victims); Olivia Solon, *'This Oversteps a Boundary': Teenagers Perturbed by Facebook Surveillance*, GUARDIAN (May 2, 2017, 11:20 AM), https://www.theguardian.com/technology/2017/may/02/facebook-surveillance-tech-ethics [https://perma.cc/N2L3-CF9S] (teenagers); Ryan Calo, *OfficeMax Letter to 'Daughter Killed in Car Crash' Could Be Privacy's Whale Song*, FORBES (Jan. 19, 2014, 4:09 PM), https://www.forbes.com/sites/ryancalo/2014/01/19/officemax-letter-to-daughter-in-car-crash-could-be-privacys-whale-song/?sh=739ffdd83fb8 [https://perma.cc/WH89-Z2WS].

than just another marketplace; it could become a realm of greater and more persistent surveillance of human beings, unlike anything else ever created.[27] Shoshana Zuboff explains how early engineers at Google noticed that their interactions with customers using their search engine produced significant amounts of information about customer behavior, a phenomenon sometimes referred to as a "data exhaust."[28] The engineers discovered that rather than discarding the data, they could use it to improve the quality of their services to benefit the human customers. Later engineers discovered that this data—what Zuboff terms "behavioral surplus"—has other uses as well, ones that did not necessarily benefit the customers who were generating it.[29] As venture capitalists impatiently sought a return on their investment in Google, and the company anxiously searched for assets to "monetize," Google seized upon "behavioral surplus" as a means to serve targeted advertisements.[30] "Advertising," Zuboff explains, "had always been a guessing game" of hunches, "art, relationships, conventional wisdom, [and] standard practice, but never 'science.' The idea of being able to deliver a particular message to a particular person at just the moment when it might have a high probability of actually influencing their behavior was, and always had been, the holy grail of advertising."[31]

The new ads targeted by "behavioral surplus" were both far more effective at changing behavior and far more lucrative for Google. As a result, Google transformed from a search engine company into the pioneer of surveillance capitalism, claiming "human experience as free raw material for hidden commercial practices of extraction, prediction, and sales . . . [t]he foundational framework of a surveillance economy."[32]

Zuboff's framework of surveillance capitalism has many ramifications for our understanding of the digital economy, but one in particular is critical for the duty of loyalty. Surveillance capitalism represents a shift in the way companies perceive human information produced by digital activities. Previously, such information was used primarily for the consumer's benefit, to improve the quality of services. That changed when it is understood as "behavioral surplus" because it started to be used to predict and increasingly to influence those consumers in ways designed to benefit the company. From this perspective, people are no longer the party to be served, but rather become grist for the mills of behavior and attention. Human customers who trust tech companies become transformed into sources of the raw material

27. NEIL RICHARDS, WHY PRIVACY MATTERS (2021).
28. ZUBOFF, *supra* note 3, at 67–69.
29. *Id.* at 8.
30. *Id.* at 71–75.
31. *Id.* at 77–78.
32. *Id.* at vii.

of behavioral surplus, which is then used to manipulate those same customers, for the benefit of the surveillance capitalist platform and its real customers, the advertisers. Zuboff's account reveals how much of the digital economy, particularly for companies offering "free" services, rests on a business model with significant natural incentives (to say the least) for opportunistic exploitation of human customers.

B. Nudging

If the technical tools of data science represented one way in which companies could exploit consumer vulnerability, the use of new behavioral science tools, developed by psychologists and economists, represented another. Beginning in the late 1960s with the pioneering work of Israeli psychologists Daniel Kahneman and Amos Tversky, the emerging field of "behavioral economics" documented numerous ways in which the human brain diverges from the assumption of rationality at the core of classical microeconomics.[33] The economist Richard Thaler draws a helpful distinction between "econs," the assumed rational actor in economic models that says human beings are motivated by self-interest, and "humans," actual human beings as the experimental evidence reveals them to be.[34] Humans, it turns out, do not always act like the econs the rational actor model assumes. Instead, our brains are, as psychologist Dan Ariely puts it, "predictably irrational."[35] Experimental evidence has revealed humans to be bad at estimating probability, prone to reasoning with emotion over facts, and tending to prefer the status quo over some objectively superior alternatives ("status quo bias").[36] Furthermore, evidence has proved that humans find it hurts more to lose something they already own than the thing is worth ("the endowment effect").[37] These characteristics dictate how humans make decisions and persist systematically across differences in intelligence, wealth, and other factors.[38] They are not defects so much as they are consequences of the way the human brain has evolved to function.[39]

---

33. *See generally* DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011); MICHAEL LEWIS, THE UNDOING PROJECT: A FRIENDSHIP THAT CHANGED OUR MINDS (2016).

34. RICHARD H. THALER, MISBEHAVING: THE MAKING OF BEHAVIORAL ECONOMICS 4–5 (2015).

35. DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS, at xx (2008).

36. Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630, 673–76 (1999).

37. *Id.*

38. For examples of these phenomena, see *id.* at 643–87; *see also* ARIELY, *supra* note 35, at xx.

39. Thaler and Judge Richard Posner, the godfather of the modern law and economics rational actor model in the legal academy, apparently clashed over this very point at an infamous workshop at the University of Chicago Law School in the mid-1990s. *See* THALER, *supra* note 34, at 261.

And critically, they can be demonstrated repeatedly across populations. We humans "systematically behave in nonrational ways."[40]

The findings of behavioral science were popularized by Thaler and Cass Sunstein in their 2008 book *Nudge*.[41] *Nudge* describes how governments, companies, and ordinary people can use techniques derived from cognitive and behavioral science to ensure that they (or others) make better choices.[42] Their key finding is that entities who can control how choices are structured can also control, at least at the margins, what decisions humans make. This is accomplished by harnessing behavioral science to do things like set defaults, which tend to be sticky due to the way humans perceive things like status quo bias and the endowment effect. "Choice architecture," they argued, was tremendously powerful, but in order to be ethical, it needed to be accompanied by the substantive constraint of "liberal paternalism."[43] Choice architects needed to (a) set nudges up in ways that would benefit the humans being nudged and (b) give humans the option to freely choose something other than the default. As a good economist, Thaler recognized that this was a crucial assumption, and he later confessed, "Whenever I'm asked to autograph a copy of 'Nudge,' . . . I sign it, 'Nudge for good.' Unfortunately, that is meant as a plea, not an expectation."[44]

Thaler realized that nudges (like all forms of applied behavioral economics) confer power and are merely tools that can be used for good, for evil, or to advance the goals of whomever wields the tool. Companies realized this as well, and they were spurred on by competitive markets, which created an incentive for them to get consumers to do what they wanted them to do (most frequently, buying lots of their products). Thus, Jon Hanson and Doug Kysar argued in 1999 that not only *could* companies use behavioral science to manipulate consumers by exploiting their known irrationalities but crucially that market incentives *would* effectively require companies to do it.[45] They called this phenomenon "market manipulation," and in a companion article, they provided impressive early empirical evidence that this was exactly what was happening in practice.[46]

Perhaps the best examples of disloyal behavior by trusted companies are so-called "dark patterns" in software user interfaces. Dark patterns are "user

40. Hanson & Kysar, *supra* note 36, at 635.
41. *See* Sunstein & Thaler, *supra* note 10.
42. *Id.* at 4–8.
43. *Id.* at 11–13.
44. Richard H. Thaler, *The Power of Nudges, for Good and Bad*, N.Y. TIMES (Oct. 31, 2015), https://www.nytimes.com/2015/11/01/upshot/the-power-of-nudges-for-good-and-bad.html [https://perma.cc/79EM-BUXX].
45. Hanson & Kysar, *supra* note 36, at 743.
46. Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 HARV. L. REV. 1420, 1505–24 (1999).

interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions."[47] Common examples include unnecessary multiple checkboxes and extra clicks required to unsubscribe from marketing emails; prominently featured "I AGREE" buttons placed next to small, hidden "no thanks" buttons; and options to decline framed in such a way that shames the user into agreeing to certain proposals ("no thanks, I hate free stuff!"), a practice known as "confirmshaming."[48] Then there are the "free" mobile games that offer addictive gameplay at the start, followed by a slow crawl of progression in the game due to attention-sapping advertisements and the need to purchase premium currencies to progress.[49] They rely on the endowment effect of the time already invested in the game to induce these levies on consumer time, money, and attention. In these ways, companies can weaponize the insights of *Nudge* and behavioral science to engage in opportunistic behavior adverse to the interests of trusting human customers. Companies use choice architecture to nudge not for good and not to promote trust but for their own financial interests. This unmasks choice architecture for what it truly is: a cookbook for the control of human choices.

C. Manipulation

By themselves, the tools of surveillance-based sorting and behavioral science are examples of how opportunistic behavior can manifest. But new vistas of opportunity for manipulation become possible when they are put together. Tech companies quickly realized not only that they could reap dividends in the digital environment through market manipulation but that

47. Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 43; *see also* Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, *Dark Patterns: Past, Present, and Future*, ACM QUEUE 67 (Mar.–Apr. 2020); Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites*, 3 PROC. ACM HUM.-COMPUT. INTERACTION CSCW 81:1 (2019); Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, CHI '18: PROC. 2018 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS., Apr 2018; Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba & Alberto Bacchelli, *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, CHI '20: PROC. 2020 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS., Apr 2020; Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger & Lalana Kagal, *Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence*, CHI '20: PROC. 2020 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS., Apr 2020; Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, PROC. ON PRIV. ENHANCING TECHS., Jul. 2016, at 237–54.

48. *See* Harry Brignull, *Types of Dark Pattern*, DARK PATTERNS, https://www.darkpatterns.org/types-of-dark-pattern [https://perma.cc/A6RD-YAFB] (discussing "confirmshaming").

49. *Monetary Dark Patterns*, DARK PATTERN GAMES, https://www.darkpattern.games/pattern/2/monetary-dark-patterns.html [https://perma.cc/CKL2-T5UV].

the power to manipulate was even greater for companies who possessed more human information and could also design every aspect of their interactions with consumers. As Ryan Calo explains, "[S]ociety 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."[50] Calo calls this phenomenon "digital market manipulation," or, more bluntly, "nudging for profit."[51]

Though she does not discuss their work, Zuboff's account illustrates how Hanson and Kysar's and Calo's predictions bore inevitable fruit in the later stages of the development of surveillance capitalism. As the relentless pressures of the market and the demands of advertisers led companies to acquire ever-more detailed and granular data, they refined their methods. First they did this to serve better ads; then to better predict behavior for more effective marketing; and finally to try to control consumer behavior through (1) choice architecture; (2) ever-more granular targeting; and (3) other data-driven, social science-informed methods of persuasion.[52] Ultimately, Zuboff argues, the processes of surveillance capitalism moves through three stages: from extraction of data, to prediction of consumer behavior, and to control.[53]

By simultaneously absorbing the insights of behavioral economics and relaxing the assumption of liberal paternalism, social science can be deployed to control consumer behavior. Think of this not as a benevolently paternalistic nudge of the kind envisioned by Thaler and Sunstein but as an evil nudge. Thus, rather than serving the needs of consumers, those same consumers have become served up for consumption. After all, what better way is there to improve advertising than predicting (and knowing) what a consumer wants, and what better way is there to ensure the effectiveness of an ad than to control consumer behavior? Beyond ever-more-refined mechanisms to produce perfectly timed and perfectly messaged advertising delivery, these techniques have been proven and used for the manipulation of both human customers and their voting practices, as revealed by the Cambridge Analytica scandal, in which the tools of commercial control were applied to political behavior.[54]

---

50. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1006 (2014).
51. *Id.* at 1001.
52. *Cf.* ZUBOFF, *supra* note 3, at 8–12 (explaining the processes of "surveillance capitalism").
53. *Id.* at 18–21.
54. *See, e.g.*, Adam D.I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCIENCES, 8788–90 (2014) (emotional contagion); Robert M. Bond et al., *A 61-Million-Person Experiment in Social Influence and Political Mobilization*, 489 NATURE 295–98 (2012) (political mobilization); Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump*

***

This, then, is the nature of the problem: companies can collect human data and use it to profile, nudge, and manipulate consumers using the tools of behavioral and data science. What is more, not only does privacy law not sufficiently constrain this behavior but corporate law and market forces actively encourage it in ways that are highly profitable for companies at the expense of not just their trusting customers but our democracy itself.

II. THE NEED FOR A DUTY OF LOYALTY IN PRIVACY LAW

At this point you might be wondering why privacy law does not deal with the problem we have just identified. After all, there are many privacy laws, and American law schools train many privacy lawyers to interpret them—whether they are the Federal Trade Commission's prohibitions on unfair and deceptive trade practices;[55] Europe's General Data Protection Regulation (GDPR);[56] or new U.S. state laws, like those enacted in California, Virginia, and Colorado.[57] In this Part, we explain how and why current data privacy law is not up to the task of confronting opportunism.

It is not just one or two statutes in the U.S. patchwork of privacy rules that need to be changed. The entire approach and value system of U.S. data privacy does not even comprehend the problems of opportunism at the scale presented by modern tech companies. Lawmakers have set their sights on giving people as much transparency about companies' data practices and as much control over their personal information as possible.[58] But the kind of control they are seeking is impossible in mediated environments.[59] What is more, giving people control over information will not protect against

Consultants Exploited the Facebook Data of Millions, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/MY9P-MGET] (Cambridge Analytica); Scott Detrow, *What Did Cambridge Analytica Do During the 2016 Election?*, NAT'L PUB. RADIO (Mar. 20, 2018, 7:22 PM), https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election [https://perma.cc/Q26D-UW8T] (same).

55. 15 U.S.C. § 45.

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

57. California Consumer Privacy Act/Privacy Rights Act, CAL. CIV. CODE § 1798.100-1798.199.100 (West 2018); Virginia Consumer Data Protecton Act, VA. CODE ANN. § 59.1-571–59.1-581 (West 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0035; Colorado Privacy Rights Act, COLO. REV. STAT. § 6-1-1301–6-1-110 (WEST 2021), https://legiscan.com/CO/drafts/SB190/2021.

58. *See generally* Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018).

59. *Id.*

manipulation, discrimination, and the erosion of our attention and our public institutions. We need an entirely new framework.

A. Privacy Law Misses Opportunism

Data privacy law, used here to broadly describe both the American and European approaches to regulating how human information is collected, used, and shared, protects against a litany of abuses. But the two major regulatory approaches to information privacy, "consumer protection" and "data protection,"[60] have overlooked how companies who interact with people in online environments exploit their structural and informational superiority over the people trusting them with their data and online experiences.

In the United States, as we have elsewhere described, there are three basic principles of American privacy law. They are (1) Do Not Lie, (2) Do Not Harm, and (3) Follow the Fair Information Practices.[61] The first two of these principles come from consumer protection law,[62] which is the predominant American approach to consumer privacy law. This approach grants "expansively defined individual rights in the context of commercial transactions."[63] As many scholars and practitioners have recognized, the most important privacy rule in practice is Section Five of the Federal Trade Commission Act of 1914, which prohibits unfair or deceptive trade practices in commerce.[64]

The principle of Do Not Lie is embodied in Section Five's prohibition on deceptive trade practices.[65] Although Section Five does not require companies to create privacy policies, most companies in the internet era have posted privacy policies to their web sites as a consequence of market norms and compliance with other state, federal, and international laws.[66] The FTC has aggressively policed deceptive claims in privacy policies to make sure that corporate privacy behavior in practice does not differ from

60. *Cf.* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 165–66, 225–58 (2016).

61. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 15 (2018) (describing American privacy law today as having three basic commands: "follow the Fair Information Practices, do not lie, and do not harm").

62. *Id.*

63. MCGEVERAN, *supra* note 60, at 165.

64. *See* Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (prohibiting "unfair or deceptive acts or practices in or affecting commerce"). *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

65. 15 U.S.C. § 45(a)(1).

66. *See generally* Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044 (2017).

what their privacy policies state.[67] But the Do Not Lie principle in Section Five does not effectively protect against opportunism. Privacy policy mandates require that companies disclose general statements of practice, but they do not have the rigor, for example, of the disclosure requirements in federal securities law. Companies can choose to be vague or confusingly technical when describing opportunistic data practices, or they can hide self-serving revelations under catch-alls like processing to "improve" service or provide "personalized" experiences.[68] Even if privacy policies were sufficiently nuanced and descriptive, no reasonable consumer would have the time required to read all of the privacy policies they encounter. Consequently, most people do not read privacy policies anyway.[69] There is thus no deeper moral principle embedded in the Do Not Lie ethic that would seek to mitigate opportunistic behavior so long as a company's fine print resembles reality.

Section Five also illustrates the second basic principle of American privacy law, Do Not Harm, through its regulation of unfair practices.[70] The idea of harm is central to American privacy law, and it is on the (in)ability to prove harm that the law frequently turns.[71] Section Five's prohibition on unfair trade practices does not provide any legal recourse for many wrongs that flow from opportunistic behavior in a relationship, because such wrongs do not always result in the narrow kind of concrete harm to consumers envisioned by tort and consumer protection regimes. The FTC Act defines an "unfair" practice as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[72] Thus, companies are free under Section Five to cause a substantial injury to consumers, at least as long as the harm

67. *See* Solove & Hartzog, *supra* note 64; HOOFNAGLE, *supra* note 64; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

68. *See, e.g.*, *Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010 [https://perma.cc/KMM7-XQ7V]; *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/5VKX-3DN4].

69. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 553 (2008); Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 6:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/BMX3-9QH4].

70. 15 U.S.C. § 45(m).

71. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021) (tightening the requirement that an injury be "concrete" to satisfy the injury-in-fact requirement in Article III standing doctrine); Danielle Keats Citron & Daniel J. Solove, *Privavcy Harms*, 102 B.U. L. REV. (forthcoming 2022) (manuscript at 3–5); *see generally* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

72. 15 U.S.C. § 45(n).

was reasonably avoidable, beneficial to other consumers, or beneficial to competition.

By fixating on harm and deception, the consumer protection approach fails to properly deal with opportunism. The consumer protection approach misses all kinds of self-dealing behavior because it looks specifically for outright deception or concrete harm, often in the form of financial injury or extreme emotional suffering. But disloyal behavior does not always result in these kinds of extreme harms. For example, nudging does not usually deal with outright falsehoods. Rather, it involves leveraging people's own cognitive and resource limitations against them. While these harms might be consistent with an intuitive understanding of unfairness, the FTC's regulation of unfair practices is limited through legislation and agency restraint. Thus, unfairness requires a showing of harm that is not present when companies use nondeceptive tactics to wheedle and cajole information out of us. However, categorizing people by characteristics for marketing purposes creates all kinds of vulnerabilities. Unfortunately, the structural harm it causes is only a pre-cursor to the kind of harm typically recognized by consumer protection law.

The other dominant approach to privacy protection is the data protection law approach.[73] As William McGeveran has helpfully explained, the data protection model differs from the consumer protection model in four separate respects. First, data protection law stems from the idea that consumers have the right to control how data about them is used, which in Europe is treated as a fundamental human right. This differs from consumer protection law, which looks to protect consumers from injury. Second, data protection law has the opposite default rule from consumer protection. Whereas the consumer protection approach assumes data processing is lawful and restricts it only in cases of harm, data protection assumes processing is restricted and allows it only where (sometimes very broad) exceptions apply. Third, because most data protection regimes derive from codes of fair information practice principles, they frequently give consumers affirmative rights to access, correct, delete, or otherwise participate in deciding how their information is processed. Fourth, data protection approaches tend to be specific and rule-based, while consumer protection obligations tend to be standards-based.[74]

United States data protection law supplies the third basic principle of privacy law—a weak push to "follow the Fair Information Practices." There are some sector-specific data protection regimes, such as those governing consumer credit data, video rental data, and health and financial

73. MCGEVERAN, *supra* note 60, at 165, 257–58.
74. *Id.* at 257–58.

information.[75] But the overarching rule established as a baseline by the FTC is that companies processing consumer data need to apply a watered-down version of the Fair Information Practices known as "notice and choice."[76] In theory, this regime represents the gold standard of informed consent to data processing, in which consumers are made aware of how their data is being used and are given meaningful choices to control how it is processed. However, in reality, things are very different. "Notice" in practice is usually no more than a dense set of legal terms buried in a privacy policy, while "choice" is little more than the choice of whether or not to participate in modern, networked life.[77] This baseline rule fails to protect privacy and is even worse at dealing with opportunism.

Of course, constructive notice plus illusory choice is not the only way to set up a data protection regime. Several U.S. laws provide somewhat greater data protection rights than the low bar of baseline "notice and choice."[78] Moreover, many believe that Europe's General Data Protection Regulation, an EU-wide instantiation of robust data protection rights, represents a superior way of dealing with the problems of data processing. The GDPR, for instance, requires a "lawful basis" for data processing.[79] This can certainly include consent (though GDPR consent is closer to the gold standard of knowing and voluntary than the often fictional consent that suffices under U.S. law).[80] Alternatively, a "lawful basis" can be achieved under other means, including the catch-all "legitimate interest" basis for processing.[81] The legitimate interest standard requires an additional balancing of the need for processing against the data subject's fundamental right of data protection.[82] These rules are backed up by stiff penalties; protective defaults for processing and design; a rigorous set of compliance standards; and robust data subject rights, such as the right to deletion and to stop processing.[83]

---

75. HARTZOG, *supra* note 61, at 15; *see also* Woodrow Hartzog, *The Invaluable, Inadequate Fair Information Practices*, 76 MD. L. REV. 952 (2017).

76. Hartzog & Richards, *supra* note 16, at 1691.

77. *Taking Trust Seriously*, *supra* note 5, at 434; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019).

78. *See, e.g.*, Federal Trade Commission Act, 15 U.S.C. § 1681s; Privacy Act of 1974, 5 U.S.C. § 552a; California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798.100–1798.199.100 (West 2020); Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

79. GDPR, *supra* note 56, at art. 6(1).

80. *See id.* at art. 4(11) (defining consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"); art. 6(1)(a) (allowing consent as a lawful basis for processing); art. 7 (explicating consent as requiring, *inter alia*, clear requests for consent and the ability for consent to be revocable after it has been given).

81. *Id.* at art. 6(1)(f).

82. *Id.*

83. *Id.* at art. 7, 12–23, 77–84.

One might be tempted to think that the GDPR and similar data protection regimes around the world might be enough to keep companies from acting opportunistically. But data protection regimes can actually *facilitate* opportunistic behavior because the GDPR and its ilk are focused on data and not the disparities within information relationships. Data protection models focus on identifiable personal data and how to process it legitimately rather than on power dynamics in relationships. This is a primarily *procedural* focus because it specifies what is needed to process data (whether consent or notification is needed, etc.), rather than placing *substantive* limits on kinds or purposes of processing. As a result, data protection models can miss abuses that do not involve personal data processing, like dark patterns for nudging or the use of knowledge gleaned from aggregated data from other people to manipulate us.

The procedural aspects of the data protection regimes that emphasize informational self-determination do not protect against self-dealing. In fact, the machinery is built in such a way as to encourage it. "Consent" requests are ground zero for disloyal behavior online. They serve as little more than window dressing—a "privacy theater"[84] that gives companies permission to engage in any manner of manipulation to wheedle and extract information and slice and dice the data of our lives in a million different ways. When companies secure people's "consent" against their own interest for dubious practices, they show how watered-down and ineffective this approach to data privacy has become, particularly in the United States.

Even substantive limitations within stronger data protection regimes like the GDPR fail to mitigate opportunism. One common restriction in these regimes is known as the "purpose limitation" or "secondary use limitation," which dictates that companies may not use data they collect for one purpose for a different, secondary purpose.[85] Relatedly, "data minimization" dictates that controllers should identify the minimum amount of personal data needed to fulfill a stated purpose and hold that much information and no more.[86] These are theoretically robust protections, but in practice they can be diluted through vague language and hindered by the focus on how the data will be *put to use*. They also typically have exceptions for consent, and in the United States in particular, consent is often presumed, deeply pathological, and rarely an effective limitation.[87]

---

84. For an early discussion of "privacy theater," see Chris Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191 (2010).

85. *See, e.g.*, GDPR, *supra* note 56, at art. 5(1)(b).

86. *Principle (c): Data Minimisation*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ (last visited Sept. 17, 2021).

87. *See generally* Richards & Hartzog, *supra* note 77.

The mischief of nudging and sorting does not always stem from the purpose for which data is processed. Benign purposes like "personalization" are sometimes useful, but they can easily blur into corrosive targeting practices that unreasonably exclude people from opportunities, extract their attention and financial resources, and expose them to misinformation.[88] Moreover, harmful nudging is usually a byproduct of user interface affordances and constraints.[89] Our personal data usually only indirectly shapes these interfaces.

The GDPR's concept of "legitimate interests" might also in theory help limit opportunistic abuses by data collectors. This concept generally provides that data processing can be justified if:

> [P]rocessing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[90]

The theory here is that determining whether there is a legitimate interest for processing requires a balancing of interests to reduce the risks of processing. In practice, as one industry-supported think tank concludes, "organisations are in the best position to undertake a risk/benefits analysis and to devise appropriate mitigations, and individuals should not be overburdened with making these assessments and informed choices for all digital interactions and processing of their personal data."[91]

Unfortunately, even this concept, which requires a balancing of substantive interests, is porous enough to accommodate many kinds of disloyal behavior.[92] A company privately "balancing" its own interests against those of its human customer would be highly unlikely to put the customer first when its data practices are not being scrutinized. Moreover, such a balancing standard would generally not aid in the interpretation of other duties, set substantive limits on the design of information

88. *See generally* COHEN, *supra* note 3.

89. *See generally* HARTZOG, *supra* note 61.

90. GDPR, *supra* note 56, at art. 6(f)

91. HUNTON & WILLIAMS LLP: CTR. FOR INFO. POL'Y LEADERSHIP, RECOMMENDATIONS FOR IMPLEMENTING TRANSPARENCY, CONSENT AND LEGITIMATE INTEREST UNDER THE GDPR 3 (May 19, 2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/06/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf [https://perma.cc/EF8T-B8NB].

92. HUNTON & WILLIAMS LLP: CTR. FOR INFO. POLICY LEADERSHIP, CIPL EXAMPLES OF LEGITIMATE INTEREST GROUNDS FOR PROCESSING OF PERSONAL DATA (Apr. 27, 2017), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_27_april_2017.pdf [https://perma.cc/QV4Q-8RUV].

technologies, or otherwise limit self-dealing so long as the basis for personal data processing was sound.

In sum, data protection regimes (even robust ones) fail to properly deal with opportunism due to their focus on process over outright substantive prohibitions, on data over relationships, and on informational self-determination over a broader vision for human flourishing. They are fundamentally procedural rules focused on the data, whose key substantive limitation is the consent of the data subject.[93] Particularly in digital environments where interface design is entirely constructed, and when consent can be manufactured or presumed, the limitation of "consent" can be a very weak one indeed.[94]

B. A Duty of Care Is Not Enough

One promising response to tech company opportunism that some lawmakers have proposed would be to impose a *duty of care* on data collectors. These proposals have taken a few different forms, but they share a general idea of extending negligence law principles to companies to ensure that they do not cause unreasonable harm to data subjects.[95]

Duties of care have a lot of appeal. Negligence was, of course, Anglo-American law's great response to the industrial revolution and all the new risks that its technical progress created for ordinary people.[96] Every first-year law student is familiar with these cases, involving train crossings, car accidents, medical malpractice, and dangerous products, and one infamous case of exploding packages on a railway platform.[97] Then there is the famous *Carroll Towing* case, involving a tug boat causing an industrial barge to sink in New York harbor and establishing the classic test for

93. The centrality of consent varies across data protection regimes. Meg Jones and Margot Kaminski have taken great care to demonstrate how concepts of consent and control are not the sole animating values of the GDPR. *See generally* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93 (2020).

94. *Cf.* Lisa M. Austin, *Enough About Me; Why Privacy is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY?: WHAT LAW CAN AND SHOULD DO 158, 158–59 (Austin Sarat ed., 2014) (making a similar point).

95. *See supra* note 7. Almost all bills proposing a duty of loyalty do so in combination with a duty of care.

96. *See* Donald G. Gifford, *Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles, and Accident Compensation*, 11 J. TORT L. 71, 71 (2018) ("Following the Industrial Revolution, for example, machines, no longer humans and animals, powered production. With greater force, locomotives and other machines inflicted far more severe injuries. These dramatic technological changes prompted the replacement of the preexisting strict liability tort standard with the negligence regime.").

97. Palsgraf v. Long Island R.R. Co., 162 N.E. 99 (N.Y. 1928); Boyce v. Brown, 77 P.2d 455 (Ariz. 1938); Cordas v. Peerless Transp. Co., 27 N.Y.S.2d 198, (City Ct. 1941); Martin v. Herzog, 126 N.E. 814 (N.Y. 1920); United Novelty Co. v. Daniels, 42 So. 2d 395 (Miss. 1949).

negligence.[98] Negligence responded well to these cases of physical harm; it also allowed industrial activity to prosper, protecting against significant injuries but giving diffuse or *de minimis* injuries a free pass.

Negligence law adapted well to the problems of the industrial age, and it remains a necessary component of privacy law in the information age. In cases of data breach, for example, where companies have been negligent in their security practices, negligence principles have helped to establish a duty of data security.[99] But negligence in the form of a *duty of data care* has real limitations. Even in the context of data security, where harm is clear, causation remains a problem in many cases. Even when negligent data security is beyond question, courts struggle with connecting a known breach to an actual case of identity theft by an unknown third party hacker.[100] As more of us become victims of data breach, tying an individual breach as the factual and proximate cause of an individual harm will become even more challenging, simply because defendants can argue that someone else's negligent breach could have been the actual cause of the injury.

Negligence has also failed to handle privacy issues well because of its intense focus on harm rather than relationships. A company that causes small injuries to millions of its customers can argue that each injury is *de minimis*, even though its vast market capitalization is the aggregate of billions of even tinier transactions. Although toxic torts have faced down similar issues admirably, the ethereal nature of privacy seems to have stymied courts.[101]

The narrowness of a legally cognizable privacy harm is also an important limitation in privacy litigation. In virtually all of these cases, companies have pushed back heavily on what constitutes a legal harm or injury throughout privacy law, with courts often agreeing to narrow theories of harm.[102]

Recent developments in Article III standing doctrine in privacy cases have turned pushback on privacy harm into a growing jurisdictional bar. In the *Spokeo* decision, for example, the Court required that plaintiffs alleging "intangible" injuries like privacy claims must now as a constitutional matter show the additional requirement of a "concrete" injury in fact (i.e., more than what the Court terms a "bare procedural violation").[103] In order to show that intangible claims are legally "concrete," plaintiffs must now

98. United States v. Carroll Towing, 159 F.2d 169, 173 (2d Cir. 1947).

99. *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1196 (2019).

100. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 751, 762 (2018).

101. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. (forthcoming Mar. 2022) (manuscript at 7, 12–14).

102. *See id.*

103. Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).

demonstrate either that Congress has identified a new harm that meets constitutional requirements (though the correctness of Congress's judgment on this question is itself subject to judicial review) or that "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."[104] This limitation on the theories of harm is a constitutional one, which means that private litigants in private cases must satisfy *Spokeo*'s concreteness test or they will be unable to raise the claim in federal court. As many scholars have documented, the tightening of standing doctrine in recent years has made privacy claims more difficult to prosecute, possibly distorting standing doctrine in the process.[105] And the Court's recent decision in *TransUnion v. Ramirez* seems to have tightened these requirements even further, suggesting that Congress's ability to recognize new legal wrongs is limited and that new causes of action have to have "a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[106] Such a limitation would appear to cast doubt on Congress's ability to craft novel remedies to new kinds of privacy wrongs, at least if the remedy is a private cause of action.[107]

In any event, not even a robust private cause of action can contain the rise of an informational capitalism that is under-regulated. It is a good thing, overall, to require tech companies to be careful and not cause unreasonable harm, but this industrial-age solution alone is woefully insufficient to deal with the problems of data-based opportunism. As Zuboff puts it well: "These developments are all the more dangerous because they cannot be reduced to known harms—monopoly, privacy—and therefore do not easily yield to known forms of combat."[108] A new—or at least a different—tool is needed for the job.

III. A THEORY OF LOYALTY FOR INFORMATION RELATIONSHIPS

Loyalty, like much else in the law, is about power. In relationships of trust, the trusting party makes themselves vulnerable to the power of the entrustee. In the particular case of an information relationship, power is conferred through the exposure of personal information and submission of

104. *Id.* (citation omitted).

105. *See* Citron & Solove, *supra* note 101; *see also* Thomas Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193 (2020); Solove & Citron, *supra* note 100, at 744 (2018); Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 548 (2017); Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 439 (2017).

106. TransUnion L.L.C. v. Ramirez, 141 S. Ct. 2190, 2213 (2021) (quotations omitted).

107. *Ramirez* explains that Congress's ability to vest enforcement authority in federal agencies is unaffected by the limitations in standing doctrine because federal agency enforcement power vests in Article II of the Constitution rather than Article III. *See id.* at 2207.

108. ZUBOFF, *supra* note 3, at 54.

agency. This power is increased when the parties deal with each other in technologically mediated environments such as app interfaces, telephone-answering AI decision trees, or social networks. The power given to entrustees allows them to make decisions that will affect the well-being of the trusting party. Inevitably, profit-seeking entrustees risk acting in their own self-interest in ways that disadvantage trusting parties. This is another example of what we have been calling opportunism.

Loyalty is the antidote to opportunism. Duties of loyalty are meant to protect against precisely this kind of exploitation. Loyalty shifts the legal duty from self-serving to other-serving. It has a morality broader than the profit-maximization of neoliberal capitalism. And it has deep roots in our law.[109] But there is more than just abstract ethics and notions of honor to the duty of loyalty. Loyalty compels firm legal duties and prohibitions that, when breached, give rise to legal liability on grounds of conflicts of interest or of duty.[110]

The core idea animating a duty of loyalty is that trusted parties must make their own interests subservient to those made vulnerable through the extension of trust.[111] This sounds appealing in the abstract, but of course important ambiguities must be resolved if loyalty is to do any major work. What is the purpose of the relationship? In what way is the trusting party vulnerable? What is the purpose or mission of a duty of loyalty—is it about obedience or protection? What are the boundaries of the duty? This Part offers a theory of loyalty for data collectors that seeks to answer these important questions.

A. Existing Loyalty Proposals

The idea of subjecting data collectors to a duty of loyalty is not entirely new. The concept has been circulating for some time in a variety of forms and levels of specificity. At the turn of the millennium, Ian Kerr suggested looking to the law of fiduciaries (and its duties of care and loyalty) to govern Internet Service Providers.[112] Daniel Solove made a similar proposal to

109. Donahue v. Rodd Electrotype Co. of New England, Inc., 328 N.E.2d 505, 515 (Mass. 1975); Edward B. Rock, *Saints and Sinners: How Does Delaware Corporate Law Work?*, 44 UCLA L. REV. 1009, 1101–03 (1997) (suggesting a moral guidance function for loyalty rules); Gregory S. Alexander, *A Cognitive Theory of Fiduciary Relationships*, 85 CORNELL L. REV. 767, 767 (2000).

110. Andrew Gold, *The Fiduciary Duty of Loyalty*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 385, 386.

111. *Id.*

112. Kerr, *supra* note 6; Ian Kerr, *Personal Relationships in the Year 2000: Me and My ISP*, *in* PERSONAL RELATIONSHIPS OF DEPENDENCE AND INTERDEPENDENCE IN LAW 78, 102, 109 (Law Comm'n of Can. ed., 2002) ("The word 'trust' connotes a state of dependence and the correlative duty

govern data brokers and other businesses that collect personal information in his book *The Digital Person*.[113] Jack Balkin prominently proposed treating data collectors as "information fiduciaries" subject to strict duties of care, loyalty, and confidentiality, a call that Jonathan Zittrain subsequently joined.[114] Balkin and Zittrain's proposal is itself the primary target of Lina Khan and David Pozen's critique of information fiduciaries, which expresses skepticism about the concept's efficacy and harmony with other laws.[115] Still, other scholars such as Lindsey Barrett, Lauren Scholz, and Kiel Brennan-Marquez have continued to advocate for and develop the concept in various contexts.[116]

Duties of loyalty have also been proposed and explored by scholars advocating a closer relationship between privacy and trust. While in harmony with the call to treat data collectors as information fiduciaries, these scholars also explore non-fiduciary frameworks and doctrines designed to keep entrusted parties discreet, honest, and protective. Ari Waldman developed a theory of privacy as trust in a monograph and series

---

of loyalty arises from the level of trust and dependence that is evident in the relationship. The type of disclosure that routinely occurs in [people's relationships with ISPs] results in the trusted party's acquiring influence that is equivalent to a discretion or power to affect the trusting party's legal or practical interests. . . . [T]he idea that some ISPs might be held to owe their users a duty of loyalty with respect to the care and control of user information is an increasingly important consideration. In fact, the idea of ISP-as-fiduciary might become even more plausible as network technology (NT) becomes more advanced."); *see also* Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. REV. 635 (2001).

113. SOLOVE, *supra* note 6, at 103 ("I posit that the law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us.").

114. Balkin first developed his idea on his blog in 2014. Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/2A6V-E5D3]. He followed up with a more thorough treatment in scholarly journals. *See* Balkin, *supra* note 6; *see also* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance*, and *New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1160–63 (2018); Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2047–54 (2018); Balkin & Zittrain, *supra* note 6; JACK M. BALKIN, AEGIS SER. PAPER NO. 1814, A HOOVER INSTITUTION ESSAY: FIXING SOCIAL MEDIA'S GRAND BARGAIN 11–15 (2018), https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf [https://perma.cc/ES3X-E7FQ]. Professor Jonathan Zittrain has also prominently advocated for information-fiduciary frameworks. Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/AX6R-P7XG]; Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/9V3H-K4CL]; Jonathan Zittrain, *Mark Zuckerberg Can Still Fix This Mess*, N.Y. TIMES: OPINION (Apr. 7, 2018), https://nyti.ms/2EsJ0La [https://perma.cc/XM4H-HVV6].

115. Khan & Pozen, *supra* note 6, at 498.

116. *See generally* Barrett, *supra* note 6; Scholz, *supra* note 6; Brennan-Marquez, *supra* note 6; Dobkin, *supra* note 6, at 1; Whitt, *supra* note 6.

of articles.[117] We have also explored the relationship between privacy and trust extensively in our previous research, including proposing a duty of loyalty for data collectors.[118]

All of this scholarship is important, but what it lacks with respect to loyalty is *detail*. Many have called for fiduciary, trust, or loyalty obligations for data collectors in general, but significant work remains to explain how the duty of loyalty would apply in practice and how it is separate from and interacts with other obligations, such as duties of care and confidentiality. The literature thus lacks a fully theorized duty of loyalty, something that is essential before fiduciary or non-fiduciary duties can be properly implemented in statutory and case law.

In this Part, we seek to fill that void. We offer a full-blown theory of loyalty for privacy law, including an explanation of loyalty's mission and its substance. A good theory also leads to specific rules and implementations and explains how they serve the goal of loyalty in information relationships. This Part details what we believe to be such a theoretically informed and practically useful approach.

B. The Mission of a Duty of Loyalty for Privacy

What should be the goal of a data collector's loyalty? Other kinds of special legal relationships for power differentials reflect particular concerns that influence what the duty of loyalty in those relationships looks like. For example, the law of trusts looks to wealth preservation and giving effect to donative intent.[119] Corporate fiduciaries are concerned with shareholder wealth maximization.[120] Agency law looks to keep agents obedient to a principal's instructions.[121] Guardianship law is concerned with making decisions on behalf of a vulnerable ward that is also consistent with the ward's instructions, values, and wishes.[122] Each of these contexts shape the

117. *See generally* WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE, *supra* note 6; Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, *supra* note 6, at 560; Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, *supra* note 6; Ari Ezra Waldman, *A Breach of Trust: Fighting Nonconsensual Pornography*, 102 IOWA L. REV. 709 (2017); Ari Ezra Waldman, *Manipulating Trust on Facebook*, 29 LOY. CONSUMER L. REV. 175 (2016).

118. *Taking Trust Seriously*, *supra* note 5; *Privacy's Trust Gap*, *supra* note 5, at 1122–23; Hartzog & Richards, *supra* note 6; Hartzog & Richards, *supra* note 16.

119. *See* Gold, *supra* note 110, at 388 (citing Robert H. Sitkoff, *Fiduciary Principles in Trust Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 41–42); RESTATEMENT (THIRD) OF TRUSTS § 78 (AM. L. INST. 2007)).

120. *Id.* (citing Julian Velasco, *Fiduciary Duties in Corporate Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 61).

121. *Id.* (citing Deborah A. Demott, *Fiduciary Principles in Agency Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 25).

122. *Id.* (citing Nina A. Kohn, *Fiduciary Principles in Surrogate Decision-Making*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 255).

contours of what the duty of loyalty demands. Specifically, factors like the purpose of the relationship, including the reason trust is given; what specifically is entrusted; the goals of the trusting party; and the discretion and power of the entrustee all dictate what it means to be loyal in a given context.

Given data protection law's focus on informational self-determination, loyalty could mean primarily seeking to effectuate the information-related instructions of the trusting party and advancing the goal of informational self-determination. This would be consistent with duties of loyalty in some other contexts.[123] On the other hand, we know from a quarter of a century of experience that it is rare for internet consumers to adequately understand the technologies they are using, the legal terms being offered, or the consequences of many technologically mediated actions.[124]

Two options therefore lie before us.[125] Should loyal data collectors act obediently? Or should they act in the best interests of the trusting parties? Answering this question requires us to unpack each of the models and, in particular, the assumptions about the nature, goals, and inherent vulnerability of the relationship that each model contains.

The first option is the obedience model, which has the virtue of consumer empowerment. It resonates with notions of control and autonomy that have been the core of data protection law since its inception in the 1970s. It also resolves many easy cases. For example, a trusting party's instructions, preferences, and purposes are frequently clear, such as when people press the "delete" button on user interfaces or share their location for the purpose of GPS mapping. Here, it would be disloyal to secretly preserve the "deleted" data for company use because it would be disobedient (i.e., contrary to a trusting party's clear instructions).[126] It would also be disloyal to use location data to send the customer the long way around to please an

123. Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513, 558 (2015) ("One could, for example, adopt an agency model according to which loyalty is tied to obedience or compliance with the instructions of one's principal. On this view, loyalty may be understood as entailing adherence to a beneficiary's instructions or present preferences. Alternatively, loyalty may be a function of the fiduciary's adherence to a beneficiary's specified purposes.").

124. This is the notion of "unwitting consent," which we explore in Richards & Hartzog, *supra* note 16, at 1478–86.

125. Miller & Gold, *supra* note 123, at 561 ("[P]rescriptive accounts of loyalty to persons can involve much more than conduct in the best interests of another. Loyalty may involve obedience to the commands or instructions of others, fidelity to their preferences, or allegiance to their purposes."). We note that there is actually an even more strict standard for loyalty in trust law—the "sole interest" rule, which requires that fiduciaries have a completely undivided loyalty to beneficiaries, enforced by a "not further inquiry" rule. However, we are not yet ready to propose such complete fealty for large companies with billions of users at scale. *See* Robert H. Sitkoff, *Fiduciary Principles in Trust Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 45.

126. *See In re* Snapchat, Inc., 2014 FTC LEXIS 313 (F.T.C. December 23, 2014).

advertiser or improve the algorithm.[127] Such uses conflict with a person's intent in sharing data. In those instances, obedience is probably the right conceptualization of loyalty.

The vice of obedience, though, is that it assumes too much about the ability of ordinary internet consumers to convey their wishes, desires, and intentions. Obedience theories of loyalty tend to be present when the principal is a sophisticated actor with access to good information and nuanced legal advice. This is why obedience is a good fit, for example, in the case of agency law's duty of loyalty. But the sophisticated actors of the agency model fit poorly for the typical internet consumer trying to clear out her inbox or drive her car to a new location. Instead, the model presumes too much about the abilities and resources of internet users, a phenomenon Paul Ohm has called "the Myth of the Superuser."[128] When dealing with ordinary consumers in the privacy context, the obedience approach risks exposing relatively unwitting consumers to avoidable harm. Thus, while a "best interests" approach would still send a consumer on the most direct route, it might cache deleted emails for a short period of time, just in case the consumer (as we have all done) had hit "delete" in error or immediately regrets the decision. Moreover, while privacy-as-control has an undeniable rhetorical appeal, its vices have been well-documented in the literature since important work by Paul Schwartz in the 1990s.[129]

More recently, we have argued elsewhere that privacy-as-choice suffers from three overpowering defects in the contemporary digital environment. First, *control can be overwhelming*, in that vast numbers of choices become vast amounts of "privacy work" delegated to already overworked consumers, resulting in resignation, psychic numbing, and an acceptance of default settings designed to maximize data collection.[130] Second, privacy as *control is insufficient* because it treats privacy as a purely individual good that can be bartered away freely without any concern for the social values that privacy serves.[131] Finally, when it comes to privacy, *control is an*

127. Balkin and Zittrain gave some vivid examples of disloyalty along these lines: "At the very least, digital businesses may not act like con men—inducing trust in end users and then actively working against their interests. Google Maps shouldn't recommend a drive past an IHOP as the 'best route' on your way to a meeting from an airport simply because IHOP gave it $20. And if Mark Zuckerberg supports the Democrat in a particular election, Facebook shouldn't be able to use its data analysis to remind its Democratic users that it's election day—while neglecting to remind, or actively discouraging, people it thinks will vote for Republicans." Balkin & Zittrain, *supra* note 6.

128. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1327–28 (2008).

129. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1658 (1999).

130. RICHARDS, WHY PRIVACY MATTERS, *supra* note 27, at Ch. 3. For "privacy work," see MARWICK, *supra* note 11. For "psychic numbing," see ZUBOFF, *supra* note 3.

131. RICHARDS, WHY PRIVACY MATTERS, *supra* note 27, at Ch. 3.

illusion because choice-architected interfaces and default settings are designed to maximize data collection by default, and also because meaningful privacy choices such as "no surveillance-based advertising" are rarely given to consumers.[132] Because American law lacks substantive rules barring manipulative data practices, this leads us straight back to the insufficient regime of "notice and choice" with which we began.

The second option for a duty of loyalty is a best-interests approach. The virtue of this approach is that it puts the customers' well-being first, even when they do not understand the technology, the legal terms to which they agree, or the full consequences or risks of their actions.[133] This approach would ensure that the protections of loyalty are always on by default for human customers, looking to protect them and put them first. Obedience is often impossible when it comes to the basic design of systems, which must have defaults by their nature. A best interests standard informing default choices would put human values first and ensure that the design of systems in practice lives up to the empowering promises made by the marketing department. It also places the burden of acting safely and appropriately on the data collector, who is in a vastly superior position to understand the risks of data processing and the interface design.

Like obedience, however, a best-interests approach has its own undeniable vices. It eliminates the ability for people to opt out of certain defaults where their preferences diverge from the mainstream with respect to "best interests" or default risk tolerance. Some people, after all, might want "more relevant ads," even where "relevance" is based upon surveillance.[134]

More fundamentally, a "best interests" standard of the sort we see in child custody cases could be seen as infantilizing to users, treating all users of a service to a standard of relative unsophistication that would not apply to all, and undermining the data protection model's goal of empowered informational self-determination. It is also subject to charges of paternalism. But loyalty is not primarily about informational self-determination or even autonomy. Loyalty is about vulnerability, and thus every duty of loyalty has

132. *Id.*

133. *Cf.* Richards & Hartzog, *supra* note 16, at 1478–86 (exploring the idea of "unwitting consent").

134. *America's Views on Surveillance Advertising*, ACCOUNTABLETECH, https://accountabletech.org/research/surveillance-advertising/ [https://perma.cc/4LGL-2VNJ].

some measure of paternalism built into it.[135] As Miller and Gold explain in this context:

> [A] fiduciary should act in what she believes are the beneficiary's best interests, even if the beneficiary might prefer a different course of action. A paternalistic form of fiduciary loyalty is arguably prominent in trust law, in which trustees have independent discretion to make choices that beneficiaries may disagree with. It is also arguably evident in corporate law, which provides that directors may act contrary to their shareholders' known desires when executing their [fiduciary] mandate.[136]

For digital information relationships, conflicts between informed manifested intent and best interests are likely to be rare because a person's specific intent and purpose is typically unclear. People do not think through all the possible hopes, dreams, and purposes for their data. Digital consumers are also vulnerable to a host of dangers, including secret surveillance, data extraction, manipulation, and data breach. Together, these risks have led to the failure of "notice and choice." We might wish that digital consumers might be like the rational creatures that Thaler calls "econs," but in reality, they are humans. They are subject to the predictable irrationality demonstrated by the experimental evidence in behavioral science and able to be manipulated by the power of data science in designed, constructed digital environments. Digital consumers have little choice but to trust companies to not to leverage user interfaces, the design of tools, and their own data against them. They have few meaningful alternatives short of going "off the grid," and so they hope their exposure will not come back to haunt them, however forlorn that hope may turn out to be in reality.

A duty of loyalty would represent a real difference from the stated purpose of most models of data protection law, which is generally to leave the determination of how data is processed to the data subject. In the U.S., this notion has become entangled with the law of online contracts, because so much of the rules that apply between people and online services are dictated by terms of use and privacy policies.[137] This is not just a matter of contract law—these boilerplate documents are still the single most important privacy regulatory instrument for the FTC and state attorneys

---

135. *See* Daniel Markovits, *Sharing Ex Ante and Sharing Ex Post: The Non-Contractual Basis of Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 209, 217 (2014).

136. Miller & Gold, *supra* note 123, at 559.

137. Woodrow Hartzog, *Website Design As Contract*, 60 AM. U. L. REV. 1635, 1641 (2011) ("As websites became ubiquitous, so did terms of use. As a result, an overwhelming amount of online activity is not governed by default law but rather through agreement between the parties.") [hereinafter Hartzog, *Website Design As Contract*]; Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMMC'N L. & POL'Y 405 (2010).

general. Not only have they been deemed largely adequate to fulfill the transparency mandate of privacy and data protection laws but they also are used to obtain people's consent to data practices, the other dominant regulatory apparatus in privacy law. But data privacy law should not be largely an extension of online contracting law, where dense and non-negotiable legalese is used by online services to place the risk of loss on people under the auspices of "consent."[138] Yet we treat most consumers under the fiction that they are sophisticated parties to bilateral arm's-length transactions.

In this respect, a best-interests standard could have some appeal to tech companies, at least those interested in long-term sustainable (and profitable) relationships rather than one-time cash grabs. The digital information relationships that leave us the most vulnerable are not one-time discrete transactions but long-term relationships with providers of email services, cloud services, operating systems, and hardware.[139] They are more like a relationship with a trustee or bailee than a one-time purchase of a hamburger on vacation (we note that even the hamburger transaction is regulated for safety and cleanliness). This is perhaps the largest change from nondigital transactions or the old-school software model of one-time purchases of licenses. Modern information relationships are long-term and characterized by trust through exposure and confidence. Both the trusting party and entrustees should favor a safe and sustainable state of affairs.

We believe that in most circumstances, a duty of loyalty should mean that data collectors are obligated to pursue the "best interests" of the trusting party with respect to what is exposed and entrusted. And while obedience to a trusting party might occasionally be in the trusting party's best interest, an overriding obedience approach to loyalty leaves too much room for mischief and abuse, including the manufacturing of "consent."[140] And what *is* typically entrusted by people when they interact with data collectors? It is not just personal data. People also trust companies with their time, attention, experience, emotions, reputation, interpersonal relationships, vulnerabilities, and financial security. Companies that control people's mediated environments and collect their personal data have substantial

138. *See generally* RADIN, *supra* note 3; KIM, *supra* note 18; Scholz, *supra* note 6; Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587 (2007); Hartzog, *Website Design As Contract*, *supra* note 139, at 1636; Hartzog, *supra* note 139; Richards & Hartzog, *supra* note 16.

139. For insight into the potential distinctions between "discrete" contracts and "relational" or "intertwined" ones, see generally IAN R. MACNEIL, THE NEW SOCIAL CONTRACT: AN INQUIRY INTO MODERN CONTRACTUAL RELATIONS (1980); Ian R. Macneil, *Relational Contract Theory as Sociology: A Reply to Professors Lindenberg and de Vos*, 143 J. INST'L & THEORETICAL ECON. 272, 275–76 (1987).

140. *See generally* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019).

discretion over whether those people will flourish in that environment and whether their welfare will be preserved. Companies can manipulate people's buying habits, emotions, political commitments, and even their voting habits.[141] In short, when people enter into information relationships with companies online, they trust those companies with their *well-being*.

Of course, a duty of loyalty cannot be unlimited. Because it is relational, it should be limited to the scope of the relationship. Thus, subject to the narrow obedience exception, we propose that those bound by a duty of loyalty should be bound to act in the best interests of the trusting party only *to the extent of their exposure*. So, for example, a company that designs dating apps should be bound to seek to maximize user well-being with respect to the choices they make using the service, the relationships they hope to create using the service, and the data that the service collects. But such a company would not be bound to seek to maximize a trusting party's well-being outside the scope of exposure to the service by, say, making sure that all their users brush their teeth every night, select healthy food options on dates, or remember to make their car payments. By contrast, a wellness app could well suggest healthy food choices and give reminders about tooth-brushing but still have little to say about potential dates or car payments. And a financial planning app could remind about car payments, but not need to encourage toothbrushing or a high-fiber diet.

As we explore below, acting loyally in practice will generally mean avoiding conflicts of interest and conflicts of duty. But a duty of loyalty could also serve as a polestar for several different default rules and procedural mechanisms to breathe life and purpose into U.S. data privacy law.

C. The Substance of a Duty of Loyalty for Privacy

Once lawmakers establish that the primary mission of the duty of data loyalty should be to act in the best interests of the trusting party to the extent of their exposure, the next step is to detail the substance and form of how the duty will be manifested in our rules. Robert Sitkoff helpfully 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."[142] However, as he also notes, "the *other* fiduciary duties, which we might call the *subsidiary* or *implementing* fiduciary duties, are

141. *See generally* HARTZOG, *supra* note 61; Luguri & Strahilevitz, *supra* note 47; Zittrain, *supra* note 6.

142. Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 419, 419.

typically structured as *rules* or at least *more specific standards* that speak with greater specificity."[143]

While lawmakers and scholars seem to pay most attention to the rules meant to compel or constrain behavior, a duty of loyalty could also act as an interpretive guide for other rules and duties. Simply put, it could be a sorely needed mechanism for setting default rebuttable presumptions against many kinds of questionable behavior.

1. Rules to Compel or Constrain Behavior

There are two main ways to conceptualize rules meant to effectuate a duty of loyalty: proscriptive and prescriptive.[144] Proscriptive approaches to loyalty focus on the kinds of activities from which loyal fiduciaries are prevented from engaging. By contrast, prescriptive approaches focus on affirmative duties to act in certain ways that demonstrate loyalty.[145] The proscriptive account of loyalty is typified by "no conflict" rules, like not using data about human customers for the company's own purposes or to manipulate those customers.[146] But other rules can also compel or constrain behavior, such as disclosure requirements and the invalidation of attempts to waive certain obligations or liability. We propose a combination of these accounts for privacy law in the form of no conflict rules, attempted waiver prohibitions, and disclosure and nondisclosure obligations.

a. No Conflicted Design or Processing

If a duty of loyalty placed on companies collecting and using human data is to accomplish anything, it should prohibit the conflicted design of digital tools and data processing. Avoiding conflicts is loyalty's core mandate and the logical starting point for lawmakers, judges, industry, and civil society.[147] A general rule against conflicted design and data processing could serve as the foundation for a host of regulatory regimes, self-regulatory efforts, and guidance to the public to encourage and nurture their trust.

Because no-conflict rules are already at the heart of fiduciary obligations of loyalty, lawmakers could borrow from established frameworks when creating rules for data collectors. Thus loyal fiduciaries, generally speaking, must follow two basic no-conflict rules. The first is a "conflict of interest rule": a mandate to avoid conflicts between the fiduciary's duty to act in the

143. *Id.*
144. Miller & Gold, *supra* note 123, at 556–57.
145. *Id.*
146. Gold, *supra* note 110.
147. *Id.*

beneficiary's best interest and the fiduciary's own self-interest. The second is the "conflict of duty rule": a mandate that the fiduciary avoid conflicts between the duty of loyalty to the beneficiary and other duties the fiduciary may have.[148] Rules of this sort do not require any particular course of action on the part of the fiduciary. Instead, (as one account has helpfully explained) they are "thought to establish boundaries within which the fiduciary may reasonably be expected to act loyally, at least to the extent that the rules isolate biasing factors that might induce the fiduciary to subjugate the interests of beneficiaries to the interests of others."[149]

Loyalty can vary according to the kinds of parties involved. For example, in corporate law, loyalty requires fiduciaries to put the interests of the corporation before personal interests that may be at odds with the corporation. One court described this duty as follows: "The concept of loyalty, of constant, unqualified fidelity, has a definite and precise meaning. The fiduciary must subordinate his individual and private interests to his duty to the corporation whenever the two conflict."[150] Some scenarios in which a fiduciary's interests may be at odds with those of the corporation include: sale of property from a fiduciary to the corporation; purchase of property or pursuit of a contract by a fiduciary that may also be in the interests of the corporation to purchase or pursue itself; when a fiduciary is a director and involved in setting executive compensation; and wherever a fiduciary is connected to shareholder litigation, insider litigation, and the protection of control.[151]

In the case of data collectors, loyalty would mean not attempting to (1) collect or process data and (2) design tools and mediated environments that would conflict with the duty to act in the interest of the well-being of the trusting party. This obligation could manifest in several ways. One of the most obvious ways would be strict and robust rules limiting what data can be collected, how long it could be kept, and for what it could be used. In this way, a duty of loyalty could impose data minimization and purpose limitations that are keyed to the objective, stated purpose for which data was collected, such as fraud prevention or direct marketing, offering more contextual specificity than the blunt data minimization principles we see in data protection law. But such a duty could also be shaped by the subjective *motives* of the trustee and the best interests of the trusting party outside of a cost/benefit analysis, like with a "legitimate interest" inquiry. The logic of

148. Paul B. Miller, *A Theory of Fiduciary Liability*, 6 MCGILL L.J. 235, 256–57 (2011).
149. Miller & Gold, *supra* note 123, at 557.
150. Bayer v. Beran, 49 N.Y.S.2d 2, 5 (Sup. Ct. 1944).
151. *See* Julian Velasco, *Fiduciary Principles in Corporate Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 61, 66–68.

a robust data minimization rule is that data that does not exist cannot form the basis of self-dealing activity.

b. Invalidation of Attempted Waivers

One of the core failures of U.S. data privacy law is the ease with which companies can extract waivers for duties. Mountains of otherwise prohibited actions involving data collection, use, and disclosure are routinely validated by the "I agree" button, by dense, confusing terms of service, and by the deployment of choice architecture to manufacture consent at the margins. This parody of knowing and voluntary consent has undermined the entire endeavor of digital consent.

One function of a duty of loyalty could be to invalidate waivers that attempt to relieve entrustees of obligations to avoid conflicted design or processing. In other words, a duty of loyalty could mandate a non-waivable baseline level of care, discretion, honesty, and protection for people. In this way, duties of loyalty would align with Anita Allen's proposal for coercive privacy mandates that prohibit waiver.[152]

The notion that certain attempts to waive the duty of loyalty should be legally invalid is already a key component of many fiduciary relationships, including trusts[153] and fact-based fiduciary relationships.[154] Even in corporate law, when statutes provide for the exculpation of certain fiduciary responsibilities, they usually explicitly exclude the duty of loyalty from waiver provisions.[155] Julian Velasco concludes that this pattern "seem[s] to suggest that the duty of loyalty (and good faith) is not subject to waiver, which would be consistent with the common belief that the duty of loyalty should be mandatory."[156] In trust law, for example, even exculpation clauses in trusts "cannot exculpate *bad faith, reckless indifference* [to the interests

152. ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE?, at xii (2011) ("[I]n an egalitarian liberal democracy, particularly if justified on broadly dignitarian grounds, legal policy makers (1) must create strong privacy rights, of course; but, moreover, (2) must be open, in principle, to coercive privacy mandates that impose unpopular privacies on intended targets and beneficiaries.").

153. *See* Sitkoff, *supra* note 125, at 56.

154. *See, e.g.*, Daniel B. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 3, 18 ("For fact-based fiduciaries, it appears that courts have identified (or at least assumed) there are certain fiduciary principles that are mandatory, that is, that cannot be waived or modified by agreement of the parties."); Gold, *supra* note 110, at 393 ("Fiduciary duties will sometimes trump contract obligations, often on the theory that the contract would be an improper limitation on the fiduciary's responsibilities to look out for her beneficiary's best interests. In that case, loyalty is not only a potential source of liability for the fiduciary, it is a limit on the existence of what would ordinarily be third-party contact rights.") (citing Paramount Communications Inc. v. QVC Network Inc., 637 A.2d 34, 51 (Del. 1993) ("To the extent that a contract, or a provision thereof, purports to require a board to act or not act in such a fashion as to limit the exercise of fiduciary duties, it is invalid and unenforceable.")).

155. *See* Velasco, *supra* note 151, at 61, 73.

156. *Id.*

of the beneficiaries or to the terms and purposes of the trust], or *intentional or willful neglect* by the trustee."[157]

The key here is to ensure that farcical notions of "consent" combined with the misguided trajectory of boilerplate contract law are not used to vitiate the duty of loyalty. Judges can play a role with this, of course, taking a cue from loyalty in other contexts. But even more useful would be a statutory prohibition on waiver. For example, Senator Schatz's "Data Care Act" provides that with respect to its proposed duties of loyalty, "[t]he rights and remedies provided under this Act may not be waived or limited by contract or otherwise."[158]

c. Disclosure and Nondisclosure Requirements

One common aspect of loyalty duties in fiduciary law is mandated disclosure, often conceptualized in ways like the "duty to inform" and the "duty to account,"[159] and other methods of obligatory transparency and notice.[160] While mandated disclosure obligations are often conceptualized as an obligation under the duty of care, when a failure to disclose something conflicts with the best interests of the trusting party (with respect to their exposure), it is probably better understood as disloyal behavior.

In our previous work on trust and privacy law, we have advocated for a "duty of honesty" as an affirmative, super-charged version of the notice and transparency notions built into the fair information practices and data protection regimes around the world.[161] We suggested that "the goal of honesty-based disclosure . . . is broader than just informing. While notice rules are horrible at informing people, they can be very good at generating the skepticism necessary to avoid a misplaced trust."[162] Duties of honesty are more substantive and have a stronger moral underpinning than mere constructive notice requirements. This is because they (1) counsel entrustees to disclose the things thatmatter most to the trusting party, particularly when the disclosed information is something the entrustee would rather not see

157. *See* Sitkoff, *supra* note 125, at 56 (citing RESTATEMENT (THIRD) OF TRUSTS § 96 cmt. C (AM. L. INST. 2012)).

158. Data Care Act of 2019, S. 2961, 116th Cong. § 5 (2019).

159. *See* RESTATEMENT (THIRD) OF TRUSTS § 82 (AM. L. INST. 2007).

160. Gold, *supra* note 110, at 391 ("A duty of disclosure is not always considered to be a loyalty duty, but . . . it is sometimes understood in that way. Duties to share information, and to share it accurately, are central to fiduciary law, and in certain cases they constitute loyalty obligations . . . .").

161. *Taking Trust Seriously*, *supra* note 5, at 463–64; *Privacy's Trust Gap*, *supra* note 5, at 2015; Hartzog & Richards, *supra* note 6; Hartzog & Richards, *supra* note 16.

162. *Taking Trust Seriously*, *supra* note 5, at 463–64 ("Information practices that are secret or shrouded in secrecy are inherently untrustworthy. Faced with such practices, skeptics act more judiciously or refrain entirely from accepting risk, even if they aren't entirely sure of what they are avoiding or how likely an undesired action or effect is.").

the light of day, and also because (2) they place the burden of understanding on the corporate speaker rather than on the human listener.

In this way the duty of loyalty could effectuate what Paul Ohm has termed "forthright code."[163] Under Ohm's proposal:

> Forthrightness would obligate companies to be completely honest, direct, and candid. Importantly, forthrightness would impose an affirmative obligation to warn rather than a passive obligation to inform. A forthright company will anticipate what a consumer does not understand because of cognitive biases, information overload, or other mechanisms that interfere with information comprehension, and will be obligated to communicate important information in a way that overcomes these barriers.[164]

Ohm notes the close relationship between loyalty and forthrightness, explaining how although "[f]orthrightness and loyalty overlap quite a bit[,] . . . my project supplements rather than diverges from loyalty."[165] While Ohm ultimately concludes that loyalty "seems like an incomplete fit for the casual, shifting, memetic, information ecosystem in which we find ourselves these days,"[166] we believe that a duty to be forthright is one of the main ways in which a duty to be loyal could be conceptualized.

In addition to mandated disclosure obligations, the duty of loyalty could dictate nondisclosure rules, as it does in other areas of fiduciary law. For example, agents are not allowed to use or communicate confidential information of the principle for their own (or anyone else's) purposes if disclosure would not be in the best interests of the trusting party.[167] In previous works we have advocated for a "duty of discretion," which would mean in certain contexts a duty of confidentiality.[168] A duty of loyalty would combine with the duty of care to prevent not just reckless and unreasonable disclosures of personal information but also disclosures in conflict with the best interests of the trusting party with respect to their exposure.

---

163. Paul Ohm, *Forthright Code*, 56 HOUS. L. REV. 471, 473 (2018).

164. *Id.*

165. *Id.* at 485. Ohm also noted the overlap between our own conceptualization of honesty and his notion of forthrightness but distinguished the two, saying that forthrightness "suggests a higher obligation to identify and share discreditable information than mere honesty" and that "honesty is such a commonplace word with a broad range of shadings and connotations that I worry that it will be misconstrued or manipulated to mean something less robust than Hartzog and Richards have proposed. Forthrightness, being a narrower and less common word, is less susceptible to this kind of treatment." *Id.* at 487. While we think honesty and forthrightness are more synonymous in this context than Ohm does, that possibly semantic debate is outside the scope of this Article.

166. *Id.* at 485.

167. *See* Deborah DeMott, *Fiduciary Principles in Agency Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 23, 31–32.

168. *Taking Trust Seriously*, *supra* note 5, at 459; *Privacy's Trust Gap*, *supra* note 5, at 1188, 2015; Hartzog & Richards, *supra* note 6, at 585; Hartzog & Richards, *supra* note 16, at 1747.

2. Rebuttable Presumptions of Disloyal Activities

Another central weakness of the U.S. approach to data privacy is that, by default, anything goes.[169] Unlike most other data protection regimes around the globe, the U.S. always allows data processing unless it is specifically prohibited.[170] A duty of loyalty could change that. In addition to substantive prescriptive and proscriptive rules, a duty of loyalty could also be deployed procedurally to shift the default status of certain design choices and data processing activities into a rebuttable presumption of disloyalty.

Under this model, several different practices could be presumptively conflicted and, thus, invalid. However, borrowing from the example of corporate law, these conflicting actions might be allowed upon proof that the behavior was justified. For example, perhaps a data protecton authority or other disinterested ombuds or Internal Rreview Board-style board could approve the actions of the entrustee. Or perhaps the presumption could be left to litigation, where courts can apply the "entire fairness" test, with the burden on the defendant to demonstrate fairness.[171] Under this test, the analysis is a comprehensive inquiry, incorporating multiple considerations such as the costs and benefit to the trusting party, the benefit conferred to the trustee, the expectations and foreseeability of risk, externalities, and structural and relative power differentials, with no one factor being decisive.[172]

Such a model is not foreign to American law; in fact, it is the basic model taken for health privacy under the HIPAA Privacy Rule. Like our loyalty framework, HIPAA is primarily relationship-based rather than data-based, applying only to data disclosed to a "covered entity" as part of a health care transaction.[173] HIPAA also presumes consent for data use that is necessary for the transaction—so called, "treatment, payment, or health care system operations data."[174] Such uses are either in the best interests of the patient (treatment) or necessary for the operation of the health care system that provides such treatment (payment and operations). Any data uses beyond those purposes require an exceptional consent that must satisfy a high bar to be legally valid. HIPAA's main problem is that it does not apply to a broad enough category of relationships. Thus, it does not protect disclosed

169. MCGEVERAN, *supra* note 60, at 257.

170. William McGeveran has noted that the U.S. and E.U. approaches to data privacy "start from converse assumptions about which data practices are permissible." *Id.*

171. Gold, *supra* note 110, at 388.

172. *See id.*

173. *See* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 676–77 (2012).

174. HIPAA Privacy Rules, 45 C.F.R. §§ 164.506, 164.508.

data outside of "covered entities" or their "business associates."[175] Nevertheless, HIPAA represents an excellent example of a loyalty-style model working effectively in American law. We could do worse than to look to it for guidance.

3. Guidance and Support for Other Duties

U.S. data privacy law often feels morally unmoored. As we have seen, the fair information practices of notice, choice, consent, access, etc., which famously undergird the entire data protection endeavor, frequently reduce privacy frameworks into mere procedural exercises. Data privacy laws tend to lack a clear sense of which intrinsic and instrumental values should be guiding the interpretation and implementation of these frameworks.[176] One of the most important ways loyalty could contribute to data privacy law would be to provide interpretive guidance for other data privacy rules. A duty of loyalty could even help guarantee the due performance of every other data privacy rule.[177] Loyalty could be a backstop to help protect against the dilution of all U.S. data privacy rules that govern information relationships. In other words, privacy law would be better as a whole if we asked less "have the procedures for data processing been followed" and asked instead "does this data processing actually promote the best interests of the human user?"

This is how loyalty works elsewhere in fiduciary law. Andrew Gold explains that in jurisdictions that see various duties of care as "non-fiduciary," duties of loyalty "may be understood as prophylactic duties, designed to ensure a proper compliance with other, non-fiduciary duties."[178] The duty of loyalty can thus play "a distinct role in changing a fiduciary's incentives with respect to breaches of other obligations."[179] Most notably, loyalty can be used to bolster the duty of care. The duty of care owed by a fiduciary is different (and more robust in some ways) than the standard duty of care owed in tort law.[180]

---

175. *See* Kirk Nahra, *A Public Service Announcement About the HIPAA Privacy Rule*, IAPP (June 18, 2021), https://iapp.org/news/a/a-public-service-announcement-about-the-hipaa-privacy-rule/ [https://perma.cc/227R-J7S5].

176. *See generally* Hartzog & Richards, *supra* note 16; Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017); *see also* Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIV. L. 250 (2014).

177. *See* MATTHEW CONAGLEN, FIDUCIARY LOYALTY: PROTECTING THE DUE PERFORMANCE OF NON-FIDUCIARY DUTIES 62 (2010).

178. Gold, *supra* note 110, at 392.

179. *Id.*

180. *See* John C.P. Goldberg, *The Fiduciary Duty of Care*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 405, 407–08.

As a check on and boost for other duties, a duty of loyalty could be used to change business models by removing incentives for companies to act, which is seen by many (including us) as a key cog in meaningful reform in data privacy law. For companies, a duty of loyalty could also help companies prioritize who they should be caring for first. In the past few years, many of us have likely heard the saying "if you're not paying for the product, you are the product."[181] The pathologies of informational capitalism drive this result. But a duty of loyalty would resolve the ambiguity of who is supposed to be primarily cared for by those who traffic personal information: people, not ad brokers or governments. Thus, loyalty will help set the priority of duties, in addition to shaping their contours. The question of who to be loyal to can be resolved with a simple maxim: When in doubt, be loyal to those who trusted you with their exposure. This means, for example, putting the interests of human consumers over those of advertising clients.

IV. IMPLEMENTING A DUTY OF LOYALTY IN PRIVACY LAW

How, then, should a duty of loyalty be implemented and what activities, specifically, should it apply to? In this Part we attempt to put some meat on the bones of the theory of loyalty we articulated above. First, we articulate four threshold conditions for a robust duty of loyalty to apply. Second, we explore several different possible frameworks for implementing a duty of loyalty in data privacy law.

A. When the Duty of Loyalty Should Arise

The duty of loyalty should arise whenever a person is susceptible to exploitation within an information relationship where trust was invited and given. Generally speaking, such a conclusion is the culmination of several different factors, including the power one party has over another, the ability for the party to resist that power to avoid harm or improve their situation, the incentives for opportunistic behavior, the communication between the parties, and the degree of exposure and reliance on trustworthy behavior.[182]

---

181. *See* Will Oremus, *Are You Really the Product?*, SLATE (Apr. 28, 2018, 5:55 AM), https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html [https://perma.cc/C8QE-DTR7].

182. *See* Paul B. Miller, *The Identification of Fiduciary Relationships*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 367, 374) (identifying various factors implicating fiduciary responsibility, including "the possession and exercise of legal authority and/or power by one person relative to another; inequality in material position, power, strength or influence between the parties; the dependence and/or vulnerability of one person upon another; a more specific susceptibility to harm, as where one's assets

Drawing from lessons of fiduciary and confidentiality law, we identify four conditions that, when present, should give rise to a duty of loyalty. Loyalty should be required (1) when trust is invited, (2) from people made vulnerable by exposure, (3) when the trustee has control over people's online experiences and data processing, and (4) when people trust data collectors with their exposure.[183]

1. When Trust Is Invited

One of the key components for determining whether a fiduciary owes duties of care and loyalty is whether the alleged fiduciary invited a person to trust them with their assets or well-being in a manner that would make them vulnerable to the actions of the fiduciary.[184]

Companies offering online services are constantly inviting consumers to trust them. They do so explicitly and implicitly through words, design, and context. In previous work, we have called these invitations "trust indicators"; those signals given off by companies through their words and the design of their digital services.[185] Ari Waldman has also noted that invitations of trust are not merely explicit. Such invitations are shaped by the relative experience of the parties, explicit and implicit social cues, and other indicia inviting a voluntary vulnerability through exposure.[186]

Informational capitalism demands your personal data and your attention. Consequently, companies do everything within their power to make you feel safe to expose yourself online. They plaster their websites with privacy and trust seals, aspirational and encouraging language, padlock icons, and enough privacy settings to spend a lifetime fiddling with in order to make

---

or person is placed at risk of conversion or exploitation; the exchange of confidential or private information; a repose of trust and/or confidence; the legal or actual incapacity of a party and/or a complete or situational inability to engage in monitoring, reporting, or other forms of self-protection; the reliance of one person upon another; or, one person's expectation of goodwill, altruism, loyalty or competent or considered advice or judgement from another").

183. Generally speaking, courts find that one ought to be bound by a duty of care and loyalty when there is "(1) [a] dependence or vulnerability by one party on the other, that (2) results in power being conferred on the other, (3) such that the entrusting party is not able to protect itself effectively, . . . and (4) this entrustment has been solicited or accepted by the party on which the fiduciary obligation is imposed." Eileen A. Scallen, *Promises Broken vs. PromisesBetrayed. Metaphor, Analog, and the New Fiduciary Principle*, 1993 U. ILL. L. REV. 897, 922.

184. *See* Kelly, *supra* note 154, at 7.

185. Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 795 (2014); *see generally* HARTZOG, *supra* note 61; *Taking Trust Seriously*, *supra* note 5.

186. WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE, *supra* note 6, at 72.

you feel comfortable exposing yourself.[187] Privacy policies predictably start with comforting language meant to reassure the reader they are safe, like "Here at Tech Company we take your privacy seriously" or "Your privacy is our top priority." Social media companies promise ephemerality (even when it is not true)[188] and make bold (and often false) statements, sometimes explicitly promising that certain services are the "safest place on the Internet."[189]

Because the modern business model for technology companies is to extract as much labor, attention, and data from people as possible, convincing people to expose themselves online is an existential matter for companies. While it can be difficult at times to isolate invitations of trust from puffery and the general functionality of an online service, courts have identified various factors that, when considered in their totality, constitute an invitation of trust.[190] These include the nature of the relationship between the parties, whether particular kinds of exposure were solicited through words or design, the nature of the exposure or sensitivity of the disclosure, the relative vulnerability or sophistication of the parties, the room for negotiation, the nature of the signals given off, and how context shapes their likely interpretation.[191] But most of the time, for most websites, apps, and other digital services, trust will be invited within the meaning of this test.

2. From People Made Vulnerable by Exposure

The degree of a trusting party's vulnerability is the second important consideration when it comes to the existence of fiduciary duties like loyalty. This factor focuses on just how dangerous it can be for people to expose themselves online. The relevant inquiry here is not just how much information a trusting party shares with a company but also the nature of the information revealed and the utility of that data to third parties. The more information that is exposed and the more attractive it is to companies, the more precarious people's situations become. This is particularly true for sensitive information, which can be used to shame, embarrass, harass, blackmail, and manipulate. But even seemingly anodyne information can be used to deny people employment opportunities, increase their insurance,

187. *See generally* HARTZOG, *supra* note 61; Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMP. L. REV. 891 (2009); Hartzog, *Website Design As Contract*, *supra* note 139*;* Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385 (2013).

188. Complaint, *In re* Snapchat, Inc., 2014 FTC LEXIS 313 (Fed. Trade Comm'n, Dec. 23, 2014).

189. Drew Harwell, *Secret-sharing App Whisper Left Users' Locations, Fetishes Exposed on the Web*, WASH. POST (Mar. 10, 2020), https://www.washingtonpost.com/technology/2020/03/10/secret-sharing-app-whisper-left-users-locations-fetishes-exposed-web/.

190. Hartzog, *supra* note 185, at 775–76.

191. *Id.* at 777–94.

disadvantage them in their dealings with others, harm their reputation, and leverage their identity to defraud others.[192] This is to say nothing of the slow-but-steady creep of surveillance that threatens to chill behavior in accretive ways.[193]

A duty of loyalty would be sensitive to people's vulnerabilities due to their exposure. The more vulnerable people become due to invited trusts, the greater loyalty the law would demand from trusted parties. Looking to vulnerabilities focuses on potential outcomes for the weaker party in modern information relationships.

The collection and processing of personal data is just one of many ways people are made vulnerable. For example, when consumers enter a digitally mediated environment, they by definition relinquish a certain amount of agency. The constraints of interacting in an app interface or web page mean that consumers can only choose from the options that are presented to them. They can only click on the buttons, drop down menus, and settings that companies want them to have. They can only view that which is pre-constructed and selected for them. This leaves them susceptible to, among other things, manipulation.[194] People are targeted, nudged, wheedled, cajoled, shamed, denied, confirmed, and worn down until they act in the precise way a company wants. Anyone who has mindlessly clicked on the shiny "I agree" button or relented in the face of countless requests from mobile apps to "turn on notifications" has experienced this kind of mediated interface-driven manipulation.

There is more. When consumers trust their data and experiences to companies, they become largely helpless to the decisions those companies make about them and for them. Companies use artificial intelligence to predict consumers' actions, which shapes what they see, for how long they see it, and who else on the internet sees them. Companies extract human attention and limit our knowledge of the world using ranking algorithms and predictive analytics that offer up only "relevant content." Our individual

192. *See generally* Citron & Solove, *supra* note 102; Solove & Citron, *supra* note 105; Calo, *supra* note 105; Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735 (2015); CITRON, *supra* note 3. *See also* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039 (2018); Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, Sophia Qasir & Thomas B. Norton, *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485 (2015); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

193. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY (2015); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013); Woodrow Hartzog & Evan Selinger, *Surveillance As Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1376–77 (2015); Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153 (2011); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 69 (2013).

194. *See* HARTZOG, *supra* note 61; Calo, *supra* note 50; Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 2 (2019); Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 461–78 (2019).

capacity to contribute to the democratic endeavor of self-governance is to a significant degree in the hands of such "unaccountable, transnational authority."[195] Loyalty, however, can protect us and ensure that we do not trust only at our peril. For if our vulnerability in mediated environments is connected to a duty of loyalty, there is more assurance that the "relevant" content is relevant to us, rather than to companies and their paying advertiser customers.

The key lies in companies' abilities to collect so many kinds of information and shape our experiences. As one of us has written elsewhere: Design is power. Design is political. Design is everywhere.[196] Companies leverage the design of information technologies to extract our consent to information collection and processing, then subsequently collect that information to gain prescient knowledge about what makes us tick, then use that knowledge to extract more data about us and harvest our attention, and then the cycle continues. Loyalty places limits on the power that information and design confer, preventing risks of opportunism and promoting properly placed trust.

3. And When Trust Is Given

In fiduciary law, courts are more likely to recognize a duty of loyalty when trust and confidence are actually placed in the entrusted.[197] Trust can can be manifested explicitly but also implicitly through actions as people acquiesce to the constraints, terms, and environment.[198]

We have little choice these days but to place our well-being in the hands of companies who seek such exposure and have such control over us. Jennifer Cobbe and Elettra Bietti wrote that in the wake of the COVID-19 pandemic:

> Daily life—including friendships, relationships, family connections, education, employment, healthcare, finances and much more—will be mediated by platform companies such as Google and Facebook that see our human interactions and relationships as content to be moderated, and as sources of data to be monetized. Amazon is already becoming a primary source of supplies, delivering food and other goods to our door. We are coming to rely increasingly on platforms for our every social and material need.[199]

195. Cobbe & Bietti, *supra* note 19.
196. *See* HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 61, at 279.
197. *See* Kelly, *supra* note 154, at 7.
198. *See generally* Hartzog, *supra* note 185.
199. Cobbe & Bietti, *supra* note 19.

To pretend that our relationship with companies that offer online services is an arm's-length transaction, as though they were street-corner hot dog vendors, makes a mockery of legal structures put in place precisely in recognition that some relationships are far more dangerous than others. In such situations, only loyalty is specifically tailored to prevent the full range of opportunistic behavior that stems from such a steep power imbalance and deep exposure of ourselves to the whims of those who would otherwise strip us for parts.

B. Possible Loyalty Frameworks

So where, exactly, does the rubber meet the road for a duty of loyalty in privacy law? We believe that loyalty rules could and should manifest in a variety of ways, from general and ad hoc relational duties, to rules designed to discourage disloyal behavior, and to equitable remedies. We argue that loyalty should be implemented or recognized in statutes, administrative action and regulations, the common law, and even in constitutional protections.

We propose that the best way to think about loyalty frameworks is in tiers. First, all major data players should be bound (ideally by statute) by a relational duty of loyalty to those whose data they hold. Courts and regulators could also look to specific promises of loyalty and care regarding people's exposure to impose ad hoc loyalty obligations. This would be the most robust form of a duty of loyalty in privacy law. Second, we propose lawmakers and regulators create rules and frameworks to mitigate, prohibit, or create incentives against disloyal actions in specific contexts. This could be thought of as a loyalty agenda or loyalty rules outside of the confines of relational duties. Finally, we explore remedies for breaches of loyalty and how loyalty might affect the developing law of standing.

1. General and Ad-Hoc Relational Duties

One of the most important traits of U.S. data privacy law and data protection regimes around the world is that they rarely differentiate between large, powerful organizations and small, weaker ones. Section Five of the FTC Act applies more or less equally to Amazon as it does to your neighborhood pizza shop. The same goes for the GDPR in the E.U. Big or small, you are prohibited from lying or harming people and obligated to follow the fair information practices. Universality is certainly useful if you want broad applicability. But there is a world of difference between

Facebook and your local coffee shop. Privacy law is about power,[200] and privacy law should be sensitive to the contexts in which that power is amassed and used.[201]

In other words, the obligations of loyalty owed by companies should be roughly proportional to the amount of power they have over people.[202] This could be measured using several different metrics, including market power, time spent using the service, amount of data collected, the nature of the data collected, degree of vulnerability, and the function of the service offered (e.g., core, multi-purpose, entertainment, etc.). The businesses in the top tier—those with the most power over people using their services due to their exposure and, consequently, the highest risk for opportunism—should be subjected to the most robust version of a duty of loyalty in privacy law. Specifically, they should be bound by a general relational duty of loyalty owed to those who entrust these companies with their data and online experiences. As described above, this would include specific prohibitions on conflicted design and data processing, invalidation of attempted waivers, disclosure requirements, and the full suite of rebuttable presumptions against specific kinds of disloyal activities and guidance for shaping other obligations.

The big five tech companies (Apple, Google, Amazon, Microsoft, and Facebook) would fit in this tier. But so too would many businesses commonly referred to as "platforms," like Uber; social media companies, like Twitter; and large credit and data brokers. But this tier could include more. Regulators might even want to create a bright line associated with large amounts of data collection and the pathologies of informational capitalism. One idea could be to look to whether a company requires a user to create an account and log in to use its service. This would be evidence of looking to create a more lasting information relationship than a single transaction.

Other companies that could be made subject to general relational duties of loyalty would be those deploying artificial intelligence technologies to make significant decisions about people who use their services. Consider the language of a bill introduced in Washington State in 2020, which required that: "[a] person may not use artificial intelligence-enabled profiling to make decisions that produce legal effects or similarly significant

200. RICHARDS, WHY PRIVACY MATTERS, *supra* note 27.

201. *Cf.* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, PRIVACY, AND THE INTEGRITY OF SOCIAL LIFE 6 (2010) (arguing that expectations and thus privacy rules should vary depending upon the social understandings of particular contexts).

202. This is, of course, the entire function of distinguishing fiduciary versus arm's-length relationships. But in the information ecosystem, a little more nuance is necessary given the diversity of relationships and services, the unprecedented power of platforms, and the exceptional nature of modern mediated experiences generally.

effects concerning consumers."[203] The bill clarified that "[d]ecisions that include legal effects or similarly significant effects concerning consumers include, without limitation, denial or degradation of consequential services or support, such as financial or lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water."[204] Tech companies amass power not just through the ability to collect personal data but also because they control the environment in which people expose themselves. General relational duties of loyalty could mitigate some of the most egregious self-dealing and opportunism inherent in modern design of digital tools and data processing.

Beyond general duties of loyalty for certain kinds of relationships, lawmakers and judges should also consider the imposition of duties of loyalty based not on a party's relational status but on the particular facts of a case. Even full fiduciary obligations can be imposed on these grounds.[205] The triggers for such ad hoc responsibilities that are most consistent with existing fiduciary law are the four criteria identified above. These criteria are also consistent with the factors relevant to judges when finding implied obligations of confidentiality.[206]

2. Rules Encouraging Loyal Behavior

In addition to obligating a duty of loyalty within information relationships, lawmakers could also embrace a loyalty agenda. This would mean crating rules and frameworks designed to prospectively encourage fidelity prescriptively and to discourage opportunistic behavior regardless of whether a company owes specific obligations within specific relationships. Such an approach might be particularly useful for frameworks meant to apply to specific industries, such as ad tech, or to mitigate specific practices, such as negative option marketing and billing.[207]

One specific example where loyalty-inspired rules (as opposed to relational duties) might be effective is in the area of abusive design. We have explained elsewhere how "[abusive] design interferes with our ability to understand what we perceive or intentionally exploits our willpower to

---

203. H.R. Res. 2644, 66th Leg., H-3930.2 (Wash. 2020), http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/2644.pdf [https://perma.cc/47ZF-F6FV].

204. *Id.*

205. Kelly, *supra* note 154.

206. *See* Hartzog, *supra* note 185, at 776–77.

207. *See* FTC, NEGATIVE OPTIONS: A REPORT BY THE STAFF OF THE FTC'S DIVISION OF ENFORCEMENT (Jan. 2009), https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf [https://perma.cc/YLC8-QZGL].

resist sharing and data extraction."[208] Sometimes design lies to us outright, like a "click to cancel" button that actually does somethine else. However, abusive design is more subtle; it uses our own internal limitations against us.

The notion of abusive design can be found in consumer protection law, which aims to protect authentic consumer choice. The most prominent prohibition on abusive practices in the United States comes from the relatively new Consumer Financial Protection Bureau (CFPB). The Dodd-Frank Wall Street Reform and Consumer Protection Act authorized the CFPB to prohibit any "abusive" act or practice that:

> (1) *materially interferes* with the ability of a consumer to understand a term or condition of a consumer financial product or service; or
>
> (2) *takes unreasonable advantage* of—
>
> (A) a *lack of understanding* on the part of the consumer of the material risks, costs, or conditions of the product or service;
>
> (B) the *inability of the consumer to protect* the interests of the consumer in selecting or using a consumer financial product or service; or
>
> (C) the reasonable *reliance* by the consumer on a covered person to act in the interests of the consumer.[209]

Rules against abusive trade practices are designed precisely to prevent opportunistic behavior by those with the ability to exploit our entrusted vulnerabilities. The elements of this prohibition essentially mirror the criteria for ad hoc fiduciary relationships. Lawmakers and judges should set standards to prohibit design that unreasonably exploits our cognitive limitations, biases, and predictable errors to undermine autonomous decisionmaking. By doing so, they will be creating rules to discourage disloyal behavior.

---

208. HARTZOG, *supra* note 61.

209. 12 U.S.C.A. § 5531(d) (West 2010) (emphasis added) ("The Bureau shall have no authority under this section to declare an act or practice abusive in connection with the provision of a consumer financial product or service, unless the act or practice–(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of–(A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.").

3. Remedies

Loyalty frameworks would also have real virtues in providing remedies to consumers. A breach of a duty of loyalty would be a *per se* legal injury that could solve the standing problem that has plagued privacy litigation, particularly since the *Spokeo* case. Recall that *Spokeo* and *Ramirez* require a concrete legal injury, such as "an alleged intangible harm [that] has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[210] Breaches of a duty of loyalty have been recognized by English and American courts in the fiduciary context for hundreds of years,[211] so an alleged breach of a duty of loyalty would satisfy the *Spokeo/Ramirez* test under its express terms. Moreover, the injury caused by a breach of the duty of loyalty is the harm to the trust in the relationship rather than a pecuniary or emotional injury. Given the intense scrutiny in standing doctrine over whether certain disclosures cause "concrete" harm, we anticipate that loyalty litigation would have real advantages over tort claims that focus on the more intangible consequences of privacy invasions.[212]

V. POTENTIAL OBJECTIONS

There are, of course, several potential objections to the duty of loyalty in privacy law that we propose in this Article. Many of these objections are based on efficacy concerns. Would such a duty accomplish its ostensible goals given potential legal conflicts and the realities of how power is amassed and used? Others are based upon concerns about the costs such a duty would impose on companies. No proposal is free from externalities and unintended consequences. While these concerns are duly noted, we believe that the costs and risks of a duty of loyalty are morally and pragmatically justified and that the duty can be made to be consistent with potentially adverse frameworks and values. The law has already provided multiple blueprints for success. A duty of loyalty can work for U.S. data privacy law. But it will take political will and a commitment to move beyond the traditional approach of privacy as control over data.

---

210. Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016); *see also* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

211. *See* Joshua Getzler, *Fiduciary Principles in English Common Law*, *in* THE OXFORD HANDBOOK, *supra* note 4, at 471, 471–473.

212. We expand on this point in Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. (forthcoming 2022).

A. Loyalty Is Too Vague

Even with some nuanced and subsidiary duties, a duty of loyalty in privacy law will be to some extent vague or, in the language of the law, indeterminate. Companies will likely object in ways that echo their dissatisfaction with the spaciousness of the FTC's unfairness standard, which broadly applies to all commercial activity that unavoidably harms consumers.[213] But there are three important points to make about the vagueness of a duty of loyalty. The first is that loyalty, like all standards in the law (i.e. negligence) will produce clarity over time. The objections to the indeterminacy of loyalty are virtually identical to those of negligence. Yet with negligence, we consider its indeterminacy—its flexibility—to be as much a strength as a weakness. What companies label as indeterminate, we label as adaptable over time in the face of rapid technological change. Indeterminate standards like those in negligence, the Fourth Amendment, and the FTC's unfairness framework have ensured that it can apply to new technologies like the automobile, handheld cameras, and heat sensors and new phenomena, like negative-option marketing and micro-influencers.

Second, some vagueness can be a virtue, and not just because standards have broad applicability. Indeterminate obligations help mitigate against companies gaming the system. When companies are not told exactly what they need to do to comply, they are likely to err on the side of caution and exercise more restraint than just getting "right up to the creepy line and not cross[ing] it."[214] A judicious level of indeterminacy helps protect against companies adopting a threadbare and disingenuous compliance mentality, whereby nominal checks of a box offer a pretense of loyalty while doing little in practice to discourage opportunism and abuse.[215]

Third, flexible standards can evolve with the times. While some critics of a duty of loyalty might argue that it is too vague,[216] other critics argue that law cannot keep pace with technology.[217] One undeniable virtue of a standards-based approach to law is that the specific can be traded off for

---

213. *See generally* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2237–39 (2015).

214. Nick Saint, *Eric Schmidt: Google's Policy Is to "Get Right Up to the Creepy Line and Not Cross It,"* BUS. INSIDER (Oct. 1, 2010, 1:44 PM), https://www.businessinsider.com/eric-schmidt-googles-policy-is-to-get-right-up-to-the-creepy-line-and-not-cross-it-2010-10 [https://perma.cc/7LB2-24PT].

215. For evidence that such a mentality is endemic in the tech industry, see ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021).

216. *See* Julie E. Cohen, *Scaling Trust and Other Fictions*, LPE PROJECT (May 29, 2019), https://lpeproject.org/blog/scaling-trust-and-other-fictions/ [https://perma.cc/7746-6ZJT]; Pozen & Khan, *supra* note 6; 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/ [https://perma.cc/M8VN-5DED].

217. For a critique of the perceived "pacing problem" in the law, see generally JOSH A. T. FAIRFIELD, RUNAWAY TECHNOLOGY: CAN LAW KEEP UP? (2020).

flexibility and the ability to evolve over time. Thus, it should be no surprise that the two most important privacy rules in the United States are not just flexible standards but very old ones—the 1789 Fourth Amendment standard of "unreasonable searches and seizures" and the 1938 FTC standard of "unfair and deceptive acts or practices"—that predate the computer but which have remained relevant in the age of mobile phones, cloud computing, social networking, and GPS trackers.[218]

Moreover, even indeterminate standards can solidify into rules over time through the natural accretive process of the common law. Robert Sitkoff has argued that this has reduced the "uncertainty and decision costs inherent to the standards-based nature of the primary duties of loyalty and care."[219] One of the main ways to bring clarity to loyalty is through subsidiary duties similar to those we have proposed above. Sitkoff argues further that a layered approach incorporating the wisdom of voluminous and diffuse interpretations of a rule helps provide clarity "by specifying how the duties of loyalty and care should be applied to recurring circumstances."[220] Over time, the natural accretive process of the law might result in subsidiary duties in specific recurring contexts.[221] By allowing the natural accretive process of law to run its course, society can benefit from organically formed and nuanced rules in specific contexts, like guidance on whether and when microtargeting is disloyal or when manipulative interfaces conflict with trusting parties' best interests.

B. The Problems of Conflicting Loyalties

In their critique of the information fiduciaries model and its duty of loyalty, Lina Khan and David Posen raise the issue of crosscutting loyalties—that is, the conflict that can occur when a large company like Facebook owes a duty of loyalty to both people who use Facebook as well as the company's shareholders.[222] The idea is that the obligation to maximize the wealth of the shareholders might conflict with an obligation of fidelity to people who trust the company with their data.[223]

This worry seems misplaced or surmountable, at least with respect to the kind of loyalty duties we propose here. Khan and Pozen note that one argument to resolve multiple loyalties might be to simply subordinate a director's duties to stockholders to their duties to users when the two

218. U.S. CONST. amend. IV; 15 U.S.C. § 45.
219. Sitkoff, *supra* note 142, at 425.
220. *Id.*
221. *Id.*
222. Khan & Pozen, *supra* note 6, at 534.
223. *Id.*

collide.[224] In fact, fiduciary law has adapted to regularly resolve conflicting loyalties.[225] Khan and Pozen themselves note this argument is similar to how "a law firm partner's duties to her fellow partners must sometimes give way to her duties to clients."[226] But you do not even have to leave the law of corporate fiduciaries for a blueprint on how to deal with loyalty owed to more than one party or in pursuit or more than one interest. Andrew Gold explains that corporate fiduciary relationships are often specifically designed to serve multiple people.[227] Even shareholders inevitably have interests that diverge from each other.[228] Gold noted, "In some cases, the response to these challenges is to develop a hierarchy of obligations."[229]

We argue that trusting, vulnerable people should take primacy over shareholders. Sometimes, Gold wrote,

> conflicts among best interests obligations 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. In that case, it may be enough to show due regard to the beneficiaries' respective interests.[230]

Alternately, Gold noted, "one might emphasize the rule of law, or focus on . . . conscientiousness. Quite possibly, the fiduciary should need to demonstrate that she has shown a genuine commitment to the ends of her beneficiary; this is different from acting for a beneficiary's exclusive benefit."[231]

Khan and Pozen make a descriptive point in response to the idea that the law should prioritize a company's loyalty to people who expose themselves over shareholders in the event of a conflict: "it runs counter to the prevailing understanding of Delaware doctrine—which, according to the Chief Justice of the Delaware Supreme Court, 'could not have been more clear' since the mid-1980s 'that directors of a for-profit corporation must at all times pursue the best interests of the corporation's stockholders.'"[232] But a duty of loyalty in privacy law would be cashed out in prescriptions and proscriptions similar to every other law that imposes costs but still allows for-profit

224. *Id.* at 508.

225. *See* Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1898, 1908–11 (2021).

226. Khan & Pozen, *supra* note 6, at 508.

227. Gold, *supra* note 110, at 398.

228. *Id.* Gold noted, "Moreover, each new issuance of stock will result in new fiduciary obligations that potentially are in tension with the obligations owed to the existing shareholders. Bankruptcy law offers an especially salient instance of potentially conflicting duties." *Id.*

229. *Id.*

230. *Id.*

231. *Id.*

232. Khan & Pozen, *supra* note 6, at 508.

corporations to maximize wealth for stockholders. The law of negligence, implied obligations of confidentiality, the GDPR, the FTC's prohibition on unfair and deceptive trade practices, and countless other rules impose costs on companies that cause them to obtain less wealth off the backs of users than they might otherwise get were they free to do anything they wished. And of course, to the extent a duty of loyalty might be imposed through a federal law justified by the Commerce Clause, such a federal obligation would be supreme over conflicting state law rules the same way that the federal minimum wage is.

A duty of loyalty in privacy law would not require companies to serve *every* best interest of their users in all aspects of their lives—only to the extent of their entrusted exposure with respect to the design of their tools and the processing of personal data. And to the extent Delaware law blocks a hierarchy of loyalties where wealth maximization is subservient, we repeat our argument from previous work that privacy law is not just about protecting data. It is also about, among other things, restructuring corporate organization and incentives.[233] Khan and Pozen argue that "information-fiduciary advocates generally appear to endorse a . . . strategy for managing conflicts between stockholders and users, which is to cabin any fiduciary duties afforded to users so that they do not seriously threaten firm value."[234] But our proposal would provide no such shield, even if it required the kind of "heavy-handed government intervention" of which Khan, Pozen, and others seem skeptical.[235] After all, the relentless pursuit of maximizing wealth by taking advantage of people's levels of exposure is exactly what got us into this mess.[236]

C. The Problem Is Broader than Just Data Collectors

One obvious limitation to a relational duty of loyalty is that many actors in our digital ecosystem would not be bound by it. Data brokers, surveillance companies, and a host of others would be free to exploit our

233. *See* Hartzog & Richards, *supra* note 114.

234. Khan & Pozen, *supra* note 6, at 509.

235. *Id.* at 504 (quoting Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/23UM-2GCS]).

236. Khan and Pozen correctly note, "[l]ike other corporations with comparable business models, Facebook therefore has a strong economic incentive to maximize the amount of time users spend on the site and to collect and commodify as much user data as possible. By and large, addictive user behavior is good for business. Divisive and inflammatory content is good for business. Deterioration of privacy and confidentiality norms is good for business. Reforms to make the site less addictive, to deemphasize sensationalistic material, and to enhance personal privacy would arguably be in the best interests of users. Yet each of these reforms would also pose a threat to Facebook's bottom line and therefore to the interests of shareholders." *Id.* at 505–06.

data without having to consider what is best for the data subject. This concern traces all the way back to Warren and Brandeis, who fretted that confidentiality is of limited use against the prying eyes of strangers.[237] But we think there are two factors that mitigate this concern.

First, we are not advocating for a duty of loyalty in privacy law *in place* of a robust data protection regime. We are arguing for a duty of loyalty *in addition* to it. One of the hallmarks of the GDPR is that the obligations regarding collection and processing follow the data downstream.[238] So, while loyalty might only apply within the confines of a relationship, data protection rules apply to everyone that touches the data. In this way, the powerful but incomplete protections of both a data protection and a data loyalty approach can complement each other nicely.

Additionally, a duty of loyalty could be implemented in such a way as to make most of the data players faithful by implementing protection at the source of data collection and requiring that protections follow past initial disclosure. In previous research, we have argued in favor of a "chain link" approach to relational privacy rules.[239] Under this approach, lawmakers would directly or through the use of mandated terms in contracts link the disclosure of personal information to obligations of loyalty to protect information as it is disclosed downstream. To create the chain of protection, contracts would be used to link each new recipient of information to a previous recipient who wished to disclose the information.

> These contracts would contain at least three kinds of terms:
>
> (1) obligations and restrictions on the use of the disclosed information, (2) requirements to bind future recipients to the same obligations and restrictions, and (3) requirements to perpetuate the contractual chain—i.e., to contractually obligate future recipients to continue the chain of contractual obligation if they wish to further disclose the information.[240]

HIPAA and data security law already impose chain-link protections on those who share information with "business associates," and the GDPR requires something similar on EU companies that transfer data to the US or other jurisdictions whose privacy laws are not up to the European standard.[241] If lawmakers so wished, they could emulate this model and

237. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
238. *See* Jones & Kaminski, *supra* note 93, at 96.
239. Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 659 (2012).
240. *Id.* at 683.
241. HIPAA Privacy Rules, 45 C.F.R. §§ 160.310, 164.504(e); GDPR, *supra* note 56, at art. 45.

mandate specific prohibitions and rules in the contracts between entrustees and those with whom they share information.

D. Fiduciary Models Risk Entrenching the Status Quo

Khan and Pozen in particular worry that broadly applicable duties of care, loyalty, and confidentiality, "if pursued with any real vigor, would tend to cannibalize rather than complement procompetition reforms."[242] Their argument seems to paint the regulatory picture as a choice between competing options. From this perspective, regulators who choose to get serious about competition law will lack the political capital for privacy law reform. While this may be possible, we think it is ultimately a false choice. Competition law and privacy law are not in conflict and they are certainly not mutually exclusive. Quite the opposite. Even loyal companies might need to be broken up. Even small companies with little market power can be disloyal.

We have argued elsewhere that we will not have comprehensive privacy reform until we solve corporal/competitive issues, relational issues, data issues, and the externalities imposed by the personal information industrial complex.[243] Even before a duty of loyalty was seriously considered by lawmakers, reform anywhere was hard to come by. Lawmakers are in for a fight no matter which path they take. Competition law itself could use a boost, as privacy law has not been the only regime enfeebled by decades of deregulatory zeal. A more cohesive approach to tech policy reform might be the rising tide that can lift all boats.

More fundamentally, Khan and Pozen argue that duties of loyalty and care that target "con artist[ry]" will invite the dominant tech firms to "shun a small set of behaviors and then claim the mantle of trustworthiness, both narrowing the scope of public debate and normalizing the basic operations of surveillance capitalism."[244] We do not think that is the correct conceptualization of how a duty of loyalty should or would operate, nor is it the likely outcome of a duty of loyalty if paired with a robust and holistic approach to data privacy with strong enforcement mechanisms. As we have argued in this Article, taken seriously, loyalty obligations would reinterpret people as precious and authoritative, not products to be exploited. Such a reorganization of priorities is built to resist the core pathologies of informational capitalism, taking it head-on and bringing it to heel.

We are not asserting that any of the information capitalists are too big to fail. Similarly, we do not believe a duty of loyalty would ratify their business

242. Khan & Pozen, *supra* note 6, at 537.
243. Hartzog & Richards, *supra* note 16, at 1739–40.
244. Khan & Pozen, *supra* note 6, at 540.

model. But critically, neither are we saying we want to burn the entire digital ecosystem to the ground. What we are saying is that if companies want to do business by inviting our exposure, there should be ground rules, and the first and foremost of these should be loyalty. When the law guarantees loyalty, there can be trust, and through trust lies sustainability, something that is good for everyone.

E. The End of Targeted Ads?

It is possible that a duty of loyalty could mean the de facto end of some business models and practices. Lawmakers might significantly affect the future of advertising, particularly ads that are targeted based upon surveillance. Would a loyalty approach spell the end of targeted ads? Under our approach, targeted ads could not continue in their current form but might continue if they are pursued in a transparent and loyal manner. For the last two decades, surveillance-based advertising (whether first- or third-party) has been justified either based on economic necessity or on the basis that "more relevant ads" are "better" ads.[245] As the internet advertising industry is fond of quipping, "who would want less relevant ads?"[246] But this rhetoric intentionally obscures the multiple meanings of "relevance." If "more relevant" is truly in the best interests and wishes of exposed parties, then targeted ads of economic necessity to the company can be loyal. But when "more relevant" comes to mean (as it too often does on the contemporary internet) "more of the things that we think we can sell the consumers to please our advertisers," then it is disloyal. A duty of loyalty to consumers means putting customers first over advertisers. If this means the end of two-sided advertising markets, so be it. If this jeopardizes the current corrosive practices of microtargeting in general, then we will all be better off for it.[247] The internet was justified as a vehicle for human connection, empowerment, and commerce.[248] While advertising may be a necessary evil to achieve some of those purposes, it should not become an end in itself.

---

245. *See generally* ZUBOFF, *supra* note 3.

246. *See, e.g.*, Dawn C. Chmielewski, *Mark Zuckerberg Says "We Didn't Take a Broad Enough View Of Our Responsibility" As He Faces Senate Questions*, DEADLINE (Apr. 10, 2018, 4:09 PM), https://deadline.com/2018/04/mark-zuckerberg-facebook-testimony-senate-hearing-1202361762/ [https://perma.cc/P9FT-F7ME] (quoting Facebook founder Mark Zuckerberg testifying that "Even though some people do not like ads, people do not want ads that are irrelevant. . . . The overwhelming feedback we get from our community [is that] people would rather have relevant content than not.").

247. Representative Eshoo's proposed ban on political microtargeting could be seen as a bright line approach prohibiting disloyal behavior. *See* Press Release, Congresswoman Anna G. Eshoo, Rep. Eshoo Introduces Bill to Ban Microtargeted Political Ads (May 26, 2020), https://eshoo.house.gov/media/press-releases/rep-eshoo-introduces-bill-ban-microtargeted-political-ads [https://perma.cc/T5FL-6ABW].

248. *See generally* TURNER, *supra* note 1.

CONCLUSION

A duty of loyalty for privacy has the potential to change how platforms do business. It could also build trust in our digital society in ways that existing models of privacy protection have failed to achieve. It is worth noting, as we conclude, that though we are privacy scholars, we lack the hubris to suggest that privacy law alone can solve all the problems of our digital transformation. We have argued elsewhere that if we want to build a digital future that is just, fair, and promotes human flourishing, many bodies of law must be brought to bear, and where necessary, transformed.[249] Corporate law, environmental law, civil rights law, consumer protection law, competition law, and First Amendment law, among others, must all be enlisted in the task. But privacy law must play a special role in these efforts for two important reasons. First, privacy and data protection law are the set of tools that the Western world has been using for the last few decades to deal with these problems. Issues of the ethical processing of human data have typically been thought of in terms of privacy/data protection, and this model has done a good job on the whole, though like many academic models it has succeeded better at offering understanding than meaningful reform. Second, regulation along these lines is very much on the current legislative agenda and actually stands a good chance of success. As we noted at the outset, both the Cantwell and Schatz bills call for some version of a duty of loyalty. As we have argued, we think that a duty of loyalty framed along the lines we suggest can do good work. This paper is thus offered both in the spirit of pointing the way for law reform as well as in the broader mode of privacy theory.

If, however, after reading our proposal, you leave feeling that it would dramatically change digital business models, and also issue a stern charge to judges and lawmakers to remain vigilant, then you would be right. A duty of loyalty would be a revolution in privacy law. But we believe it would be a revolution we can live with. It would fit alongside robust duties of care, extant data protection regimes, antitrust law, and other privacy-relevant legal frameworks. It would provide substantial and flexible protection to consumers and also encourage the development of long-term sustainable business relationships that hold out the promise of equally long-term profitability. A sea of change is exactly what is needed to deal with the unprecedented power and incentives for self-dealing in our modern digital world. A duty of loyalty would certainly disrupt the surveillance-based advertising model, but Internet companies have long touted the virtues of disruption. Indeed, the digital ad model itself disrupted advertising by

249. *See* Hartzog & Richards,, *supra* note 16.

newspapers, a disruption that has itself endangered the sustainability of a free press. But, fundamentally, the promise of the Internet with which we began this article was neither surveillance nor was it "more relevant ads." The promise of the internet was human flourishing—putting people first, promoting democracy, and protecting people from exploitation and vulnerability. A duty of loyalty for privacy law would be an important step back in that direction.